AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Central District of California

FILED
CLERK, U.S. DISTRICT COURT
APR 18 2019
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

My Passport WD hard-drive, serial number WXQ1A6803KA0; and Apple MacBook Pro with serial number C02SN0ZRG8WN and model number A1398

Case No. 19-1595

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A-1

located in the Central District of California, there is now concealed:

See Attachment B-1

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 371	Conspiracy
18 USC 666	Federal Program Bribery and Kickbacks
18 USC ~~1341~~, 1343, 1346	Deprivation of Honest Services/Wire Fraud
18 USC 1505, 1510	Obstruction of Justice/Federal Proceeding
18 USC 1956	Money Laundering
18 USC 1951	Extortion

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Andrew R. Civetti, SA FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 4/18/19

Judge's signature

City and state: Los Angeles, CA

Printed name and title

AUSA: Diana Kwok (x6529)

FILED
CLERK, U.S. DISTRICT COURT
APR 18 2019
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of:
Information associated with accounts identified as [redacted] and [redacted] that is within the possession, custody, or control of Oath, Inc., dba America Online ("AOL").

Case No. 19-1597

APPLICATION FOR WARRANT PURSUANT TO 18 U.S.C. § 2703

I, a federal law enforcement officer, request a warrant pursuant to Title 18, United States Code, Section 2703, and state under penalty of perjury that I have reason to believe that within the following data:

See Attachment A-2

There are now concealed or contained the items described below:

See Attachment B-2

The basis for the search is:
☑ Evidence of a crime;
☑ Contraband, fruits of crime, or other items illegally possessed;
☑ Property designed for use, intended for use, or used in committing a crime.

The search is related to a violation of:

Code section(s)	*Offense Description*
18 U.S.C. §371	Conspiracy
18 U.S.C. §666	Federal Program Bribery and Kickbacks
18 U.S.C. ~~§1341~~, 1343, 1346	Deprivation of Honest Services / Wire fraud
18 U.S.C. §1505, 1510	Obstruction of Justice / Federal proceeding
18 U.S.C. §1956	Money Laundering
18 USC §1951	extortion

The application is based on these facts:

See attached Affidavit, which is incorporated herein by reference.

/s/
Applicant's signature
Andrew Civetti, Special Agent
Printed name and title

Sworn to before me and signed in my presence:

Date and Time: 4/18/19 at 4:51pm

City and State: Los Angeles, CA

JACQUELINE CHOOLJIAN
Judge's signature
Hon. Jacqueline Chooljian, U.S. Magistrate Judge
Printed name and title

AUSA Diana Kwok: (213-894-6529)

COPY

FILED
CLERK, U.S. DISTRICT COURT
APR 18 2019
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of:
Information associated with accounts identified as [redacted] and [redacted] that is within the possession, custody, or control of Apple, Inc.

Case No. 19-1598

APPLICATION FOR WARRANT PURSUANT TO 18 U.S.C. § 2703

I, a federal law enforcement officer, request a warrant pursuant to Title 18, United States Code, Section 2703, and state under penalty of perjury that I have reason to believe that within the following data:

See Attachment A-3

There are now concealed or contained the items described below:

See Attachment B-3

The basis for the search is:
☑ Evidence of a crime;
☑ Contraband, fruits of crime, or other items illegally possessed;
☑ Property designed for use, intended for use, or used in committing a crime.

The search is related to a violation of:

Code section(s)	*Offense Description*
18 U.S.C. §371	Conspiracy
18 U.S.C. §666	Federal Program Bribery and Kickbacks
18 U.S.C. §~~1341~~, 1343, 1346	Deprivation of Honest Services / wire fraud
18 U.S.C. §1505, 1510	Obstruction of Justice / Federal Proceeding
18 U.S.C. §1956	Money Laundering
18 USC §1951	Extortion

The application is based on these facts:

See attached Affidavit, which is incorporated herein by reference.

/s/
Applicant's signature
Andrew Civetti, Special Agent FBI
Printed name and title

Sworn to before me and signed in my presence:

Date and Time: 4/18/19 at 4:54pm

JACQUELINE CHOOLJIAN
Judge's signature

City and State: Los Angeles, Ca

Hon. Jacqueline Chooljian, U.S. Magistrate Judge
Printed name and title

AUSA Diana Kwok: (213-894-6529)

Table of Contents

I. INTRODUCTION.....1

II. PURPOSE OF AFFIDAVIT.....1

III. BACKGROUND ON SUBJECTS.....5

IV. SUMMARY OF INVESTIGATION.....9

V. PRIOR APPLICATIONS.....11

VI. STATEMENT OF PROBABLE CAUSE.....11

A. The Underlying Civil Litigation.....11

B. No-Bid LADWP Contracts Awarded to Attorney PARADIS.....17

C. Hush Money to Conceal Collusive Litigation Practices.....20

D. Alleged Falsification of Regulatory Paperwork by LADWP Employees with the Knowledge of Attorney President of LADWP Board.....21

E. Alleged Bid Manipulation Involving Attorney Members of the LADWP Board.....23

F. Other Manipulation of LADWP Contract Processes.....24

G. Obstruction of Justice by WRIGHT.....26

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES.....30

VIII. BACKGROUND ON E-MAIL AND SOCIAL MEDIA ACCOUNTS AND THE PROVIDER.....33

IX. REQUEST FOR NON-DISCLOSURE.....46

X. CONCLUSION.....47

AFFIDAVIT

I, Andrew Civetti, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since September 2015. I am currently assigned to a Public Corruption Squad, where I specialize in the investigation of corrupt public officials, including bribery, fraud against the government, extortion, and money laundering. In addition, I have received training in the investigation of public corruption and other white collar crimes.

2. I am currently one of the agents assigned to an investigation of alleged corrupt activities within the City of Los Angeles (the "City"). The City receives over $10,000 yearly in federal funds.

II. PURPOSE OF AFFIDAVIT

3. I make this affidavit in support of applications for search warrants seeking:

a. To search the following items:

i. My Passport WD hard-drive, serial number WXQ1A6803KA0, which contains the Cellebrite extraction of a cellular telephone, [redacted] utilized by DAVID WRIGHT ("**WRIGHT'S PHONE**");

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

ii. An Apple MacBook Pro with serial number C02SN0ZRG8WN and model number A1398 utilized by DAIVD WRIGHT ("**WRIGHT'S LAPTOP**") (collectively, "the **SUBJECT DEVICES**").[1]

b. Information associated with the following accounts utilized by DAVID WRIGHT:

i. Email account [redacted];

ii. Email account, [redacted];

iii. Apple iCloud account, [redacted];

iv. Apple iCloud account, [redacted]

(collectively, the "**TARGET ACCOUNTS**").[2]

A. **SUBJECT DEVICES** Search Warrant

4. The **SUBJECT DEVICES, described in Attachment A-1**, are stored in FBI Los Angeles evidence. In connection with the investigation into this matter, the requested search warrant seeks authorization to search these items for any data or information that constitutes evidence or fruits of violations of 18 U.S.C. §§ 371 (Conspiracy), 666 (Bribery and Kickbacks Concerning Federal Funds), ~~1341 (Mail Fraud)~~, 1343 (Wire Fraud), and 1346 (Deprivation of Honest Services), 1505 (Obstructing Federal Proceeding), 1510 (Obstruction of Justice), 1951 (Extortion) and 1956 (Money Laundering) (collectively, the

[1] On April 11, 2019, I submitted a request for a search warrant for the **SUBJECT DEVICES** to Magistrate Judge Jacqueline Chooljian (2:19-mj-01470), which was ultimately denied. I have updated this affidavit based on questions from Judge Chooljian and my further review of evidence.

[2] On April 11, 2019, I also submitted a request for a search warrant for the **TARGET ACCOUNTS** to Magistrate Judge Jacqueline Chooljian (2:19-mj-01469). On April 16, 2019, the government filed an application to withdraw that request.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

"Target Offenses") as set forth in Attachment B-1. Attachment A-1 and Attachment B-1 are incorporated herein by reference.

B. **TARGET ACCOUNTS Search Warrants**

5. I also make this affidavit in support of an application for a search warrant for the initial seizure of information associated with the following accounts:

a. [redacted] and [redacted], e-mail accounts stored at premises controlled by Oath, Inc. doing business as America Online ("AOL"), and being used by WRIGHT;

b. [redacted] and [redacted], Apple iCloud accounts stored at premises controlled by Apple, Inc., and being used by WRIGHT.

6. Oath, Inc. ("Provider 1") is a provider of electronic communication and remote computing services, headquartered at 22000 AOL Way, Dulles, Virginia 20166, regardless of where such information is stored, held, or maintained.[3]

---

[3] Because this Court has jurisdiction over the offenses being investigated, it may issue the warrant to compel the PROVIDER pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). See 18 U.S.C. §§ 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction") and 2711 ("the term 'court of competent jurisdiction' includes -- (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that -- (i) has jurisdiction over the offense being investigated; (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title").

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

7. Apple, Inc. ("Provider 2") is a provider of electronic communication and remote computing services that accepts service of legal process at 1 Infinite Loop, M/S 36-SU, Cupertino, California, 95014, regardless of where such information is stored, held, or maintained (collectively, "the PROVIDERS").

8. The information to be searched in the **TARGET ACCOUNTS** is described in Attachments A-2 and A-3. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A) and 2703(d)[4] to require the PROVIDERS to disclose to the government copies of the information (including the content of communications) described in Section II of Attachments B-2 and B-3. Upon receipt of the information described in Section II of Attachments B-2 and B-3, law enforcement agents and/or individuals assisting law enforcement and acting at their direction will review that information to locate the items described in Section III of Attachments B-2 and B-3.

---

[4] The government is seeking non-content records pursuant to 18 U.S.C. § 2703(d). To obtain the basic subscriber information, which do not contain content, the government needs only a subpoena. See 18 U.S.C. § 2703(c)(1), (c)(2). To obtain additional records and other information--but not content--pertaining to subscribers of an electronic communications service or remote computing service, the government must comply with the dictates of section 2703(c)(1)(B), which requires the government to supply specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation in order to obtain an order pursuant to 18 U.S.C. § 2703(d). The requested warrant calls for both records containing content (see Attachment Bs Section II.~~10~~13.a) as well as subscriber records and other records and information that do not contain content (see Attachment Bs Section II.~~10~~13.b).

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Attachments A-2 and A-3 and B-2 and B-3 are incorporated herein by reference.

9. As described more fully below, I respectfully submit there is probable cause to believe that the information stored on the **SUBJECT DEVICES** and associated with the **TARGET ACCOUNTS** constitutes evidence, contraband, fruits, or instrumentalities of criminal violations of the Target Offenses.

10. The facts set forth in this affidavit are based upon my personal observations, my training and experience, information obtained from other agents and witnesses, and information obtained from cooperating subjects, as detailed further below. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. BACKGROUND ON SUBJECTS

8. Based on my knowledge of the investigation, below is general background on certain subjects. Although this investigation currently has other subjects, this affidavit focuses on the subjects most relevant to the requested search warrants.

9. DAVID WRIGHT is the General Manager of the Los Angeles Department of Water and Power ("LADWP"). WRIGHT originally joined LADWP in February 2015 as the Senior Assistant General Manager and then became Chief Operating Officer before being

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

appointed as General Manager in September 2016. According to LADWP's website, WRIGHT spearheaded major LADWP initiatives to restore customer trust in the utility, and to create a clean energy future and a sustainable water supply for Los Angeles.

10. PAUL PARADIS is an attorney and partner at Paradis Law Group, PLLC, operating in New York and Los Angeles. In 2015, PARADIS was appointed as Special Counsel for the City in a civil litigation against PricewaterhouseCoopers ("PwC") regarding an alleged faulty billing system, (Superior Court of California, captioned *City of Los Angeles v. PricewaterhouseCoopers*, Case No. BC574690 ("PwC Case")).

a. On March 15, 2019, I initially interviewed PARADIS, in the presence of his attorney, regarding his involvement in the Target Offenses pursuant to a proffer agreement.[5] I have subsequently interviewed PARADIS on numerous occasions. PARADIS has no criminal record and has agreed to assist the government in exchange for favorable consideration in a potential future prosecution of him related to his conduct in this matter. At my direction, PARADIS has conducted multiple consensual recordings with certain subjects in the investigation, some of which are detailed herein.[6]

[5] Under the terms of the proffer sessions discussed herein, the government is allowed to make derivative use of the information provided to it. The government agrees only not to use the information against the provider of the information in the government's case-in-chief against that person, provided the person is entirely truthful in proffer sessions.

[6] Where possible at this early stage of the investigation, I have attempted to corroborate PARADIS's proffer statements with independent evidence. However, these efforts are presently

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

11. GINA TUFARO is a New York-based attorney and the law partner of PARADIS.

12. MEL LEVINE is a Los Angeles-based attorney and partner at Gibson, Dunn, & Crutcher, LLP. LEVINE is also the President of the LADWP Board of Commissioners ("LADWP Board"). LEVINE is a former United States Congressman from California, having served in the United States House of Representatives from 1983 to 1993.

13. CYNTHIA MCCLAIN-HILL is a Los Angeles-based attorney and the Vice President of the LADWP Board.

14. STEPHEN KWOK is the Chief Information Security Officer of the LADWP Board.

15. DAVID ALEXANDER was previously the Chief Information Security Officer at LADWP. He was removed from that position in approximately March 2019, but remains employed by LADWP.

16. JACK LANDSKRONER is a Cleveland-based attorney and partner at Landskroner, Grieco, Merriman, LLC. LANDSKRONER was a counsel for Antwon Jones in a civil litigation against the City, (Superior Court of California, captioned *Jones v. City of Los Angeles*, Case No. BC577267 ("Jones Case")).

a. On March 14, 2019, I interviewed LANDSKRONER, in the presence of his attorney, regarding his involvement in the Target Offenses pursuant to a proffer agreement. LANDSKRONER

---

complicated by the fact that many of the relevant communications may implicate attorney-client privilege or attorney work product. The FBI and the U.S. Attorney's Office are working to resolve these issues through a combination of filter reviews, requests for waivers, and an anticipated request for a judicial determination on the crime/fraud exception.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

has no criminal record and has agreed to assist the government in exchange for favorable consideration in a future prosecution.

17. PAUL KIESEL is a Beverly Hills-based attorney and partner at Kiesel Law, LLP. Along with PARADIS, KIESEL was retained as local Special Counsel for the City in the PwC litigation.

18. JAMES CLARK is the Deputy Chief for the Los Angeles City Attorney. According to the City Attorney's website, CLARK has more than 38 years of civil litigation experience, was a long-time partner at Gibson, Dunn & Crutcher, LLP, is a fellow of the American College of Trial Lawyers, and has handled a multitude of complex civil litigation matters at every level of the California and Federal Courts.

19. THOMAS PETERS was the former Chief of the Civil Litigation Branch of the LA City Attorney's Office. PETERS resigned from his position on or about March 22, 2019, in the wake of allegations that he received money from plaintiffs' firms who had lawsuits against the City. PETERS oversaw the City's civil litigation in the PwC Case.

20. WILLIAM FUNDERBURK, a Los Angeles-based attorney, is the former Vice-President of the LADWP Board.

21. PAUL BENDER was appointed by the presiding Los Angeles Superior Court judge as the "independent monitor" for the City related to the settlement of the Jones Case.

22. LOS ANGELES DEPARTMENT OF WATER AND POWER is, according to its website, the nation's largest municipal utility, with a $7.5 billion annual budget for water, power and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

combined services. LADWP is responsible for a Power System that provides over 26 million megawatt-hours of electricity per year to over 1.5 million electric services, and a Water System that delivers 160 billion gallons of water per year to 681,000 services in the City. LADWP has a workforce of approximately 10,000 employees.

23. AVENTADOR UTILITY SOLUTIONS, LLC ("AVENTADOR") is a cybersecurity company incorporated by PARADIS on or about March 29, 2017. Around March 2019, AVENTADOR was sold at below-market value to another owner and changed its name to ARDENT CYBER SOLUTIONS, LLC ("ARDENT").

24. THE LOS ANGELES CITY ATTORNEY's OFFICE, according to its website, "plays a leading role in shaping the future of the City by fighting to improve the quality of life in the City's neighborhoods, reducing gang activity, preventing gun violence, standing up for consumers and the elderly, protecting the City's environment. The City Attorney's office writes every municipal law, advises the Mayor, City Council and all city departments and commissions, defends the city in litigation, brings forth lawsuits on behalf of the people and prosecutes misdemeanor crimes such as domestic violence, drunk driving and vandalism."

IV. SUMMARY OF INVESTIGATION

25. The FBI has an ongoing investigation into public corruption at the Los Angeles Department of Water and Power ("LADWP") and the Los Angeles City Attorney's Office ("City Attorney's Office"). The evidence indicates that multiple City

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

officials are involved in several interlocking criminal schemes, including the following:

a. Collusive litigation practices related to lawsuits involving the City Attorney's Office and LADWP, which were fueled in at least one instance by a $2.175 million kickback from plaintiff's attorney JACK LANDSKRONER to attorney PAUL PARADIS, a Special Counsel retained by the City Attorney's Office.

b. Offering of bribes by PARADIS, and acceptance of those bribes by LADWP General Manager DAVID WRIGHT and LADWP Board Vice President WILLIAM FUNDERBURK, in exchange for at least one $30 million no-bid LADWP contract to PARADIS's company.

c. An $800,000 hush-money payment to a prospective whistleblower by Special Counsels PARADIS and PAUL KIESEL in exchange for silence as to collusive and potentially fraudulent litigation practices involving PARADIS, KIESEL, and THOMAS PETERS, then the Chief of Civil Litigation at the City Attorney's Office.

d. LADWP's pattern and practice of falsifying records required by the Federal Energy Regulatory Commission ("FERC"), with the knowledge and approval of WRIGHT, LADWP Board President MEL LEVINE, and other LADWP managers and Board members, in order to conceal and avoid responsibility for cybersecurity vulnerabilities related to the City's power grid, water supply, and other critical infrastructure.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

e. Bid rigging and other manipulation of LADWP contract processes by WRIGHT, LEVINE, other members of LADWP management and the LADWP Board, and members of the City Attorney's Office.

26. These schemes are discussed in order, below.

V. PRIOR APPLICATIONS

27. On April 11, 2019, the Honorable Jacqueline Chooljian denied an application for the **SUBJECT DEVICES**.

28. Other than what has been described herein, to my knowledge the United States has not attempted to obtain the contents of the **TARGET ACCOUNT** by other means.

VI. STATEMENT OF PROBABLE CAUSE

29. As an employee of LADWP, WRIGHT communicated and/or interacted directly and indirectly in his official capacity with and about PARADIS, TUFARO, LEVINE, MCCLAIN-HILL, KWOK, ALEXANDER, LANDSKRONER, KIESEL, CLARK, PETERS, FUNDERBURK, BENDER, AVENTADOR, ARDENT, and CYBERGYM (the "Subjects"), relating to the following schemes. Based on my proffers with PARADIS, WRIGHT was an integral part of the commission of the Target Offenses and has been associated in some capacity with each of the Subjects beginning in at least 2015.

A. The Underlying Civil Litigation[7]

30. In 2013, LADWP implemented a new billing system pursuant to a contract with PwC. Upon implementation of the

[7] The facts outlined in this section are based on my review of public court filings, transcripts of depositions taken in the state court cases, open source research, my interviews with LANDSKRONER and/or PARADIS, and consensually recorded meetings.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

system, widespread billing errors ensued. On December 8, 2014, an overbilled LADWP ratepayer named Antwon Jones retained New York-based attorney PAUL PARADIS to represent him in a lawsuit against LADWP for damages related to overbilling and his treatment by LADWP.

31. On December 18, 2014, PARADIS and Beverly Hills-based attorney PAUL KIESEL, serving as local counsel, met at the City Attorney's Office with then-Chief of Civil Litigation THOMAS PETERS to discuss the case.[8] PETERS also happened to formerly be KIESEL's law partner. At or shortly after that meeting, personnel from the City Attorney's Office retained PARADIS and KIESEL to represent the City and LADWP as Special Counsel in all disputes arising from the overbilling issues.[9] The contract formalizing PARADIS's and KIESEL's retention as Special Counsel for the overbilling matter was issued on April 21, 2015, and approved by the City Council on April 23, 2015. However, the agreement was backdated to January 1, 2015 (and based on deposition testimony, PARADIS's and KIESEL's representation appears to actually have commenced even earlier, in December 2014).

---

[8] PETERS resigned from the City Attorney's Office on or about March 22, 2019, in the wake of allegations that he received referral income from plaintiffs' attorneys who had filed lawsuits against the City.

[9] In a proffer session with the government, PARADIS advised that Chief Deputy City Attorney JAMES CLARK offered them the job at the December 18, 2014 meeting in PETERS's office. According to PARADIS, and to CLARK in his deposition, CLARK had knowledge that PARADIS represented both Jones and the City in connection with LADWP billing litigation.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

32. At that time, the City was exploring both the possibility of suing PwC directly, and the possibility of arranging for a class of ratepayers to sue PwC for damages. The City preferred the latter option. This is because the City believed this option would benefit it politically and financially because it would inoculate the City against lawsuits by ratepayers. For that reason, PETERS directed PARADIS, as Special Counsel for the City, to draft a complaint in a contemplated lawsuit by Jones (PARADIS's client) against PwC. PARADIS did so, and in January 2015, he sent copies of the draft complaint both to his client Jones, and to PETERS at the City Attorney's Office.[10] In part because Jones wanted to sue the City[11] and not PwC, that lawsuit did not materialize, and the City ultimately sued PwC directly in a complaint filed on March 6, 2015 ("*City v. PwC*").

33. In mid-March 2015, Jones directed PARADIS to file a lawsuit against the City (not PwC). PARADIS used his work on the draft complaint for the contemplated *Jones v. PwC* action to

---

[10] In his deposition, Chief Deputy City Attorney CLARK testified that he likely advised City Attorney Michael Feuer of the existence of the draft *Jones v. PwC* complaint. CLARK further testified that the draft *Jones v. LADWP* complaint was also forwarded to the LADWP Board, and that LADWP Board President MEL LEVINE was also involved in decisions relating to the draft complaint.

[11] Based on my investigation and conversation with subjects, my understanding is that Jones desired a lawsuit against the entity he felt had wronged and then mistreated him, which was LADWP, not PWC.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

craft a complaint for a lawsuit by Jones against the City.[12] The civil litigation is being presided over by the Honorable Elihu M. Berle, Supervising Judge of the Civil Division at Superior Court of California, County of Los Angeles. On March 26, 2015, PARADIS introduced Cleveland-based attorney JACK LANDSKRONER to Jones via email, advising Jones that LANDSKRONER was an expert in municipal lawsuits who should join their legal team.[13] Jones retained LANDSKRONER on that date.

34. Chief Deputy City Attorney CLARK later testified that he learned from PARADIS about PARADIS's recommendation of LANDSKRONER to represent Jones in his lawsuit against the City. CLARK further testified that he understood and agreed that LANDSKRONER would be advantageous to the City's goals in resolving the ratepayer lawsuit because LANDSKRONER was "a more reasonable person to deal with" than the attorneys who represented the plaintiffs in the four other class-action lawsuits that had separately been filed.[14] According to CLARK,

---

[12] The timing (but not the fact) of PARADIS's work on the *Jones v. City* complaint appears to be disputed among the parties to the civil litigation.

[13] Jones understood, at that time and throughout the course of his lawsuit against the City, that he was represented by both PARADIS and LANDSKRONER. PARADIS did not at any time advise Jones that he was representing the City on this matter, nor did he seek to withdraw as Jones's counsel during the course of the litigation.

[14] After his deposition, CLARK submitted, through the City's new representative counsel, an "errata" list of several dozen transcribed answers that he wished to substantively change, including multiple answers on this topic. A further deposition has been ordered to explore CLARK's post-deposition request to alter his substantive testimony. In any event, CLARK repeatedly testified to his and the City's perception that the other

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

the City had several goals in resolving the ratepayer claims, including: to refund money that had been wrongfully overpaid due to billing errors; to remediate PwC's CC&B billing system, which the City blamed for the errors; and to obtain a release sufficiently broad to cover all of the diverse claims made against the City by all of the class-action plaintiffs.

35. On April 1, 2015, LANDSKRONER filed a class-action lawsuit against the City with Jones as the lead plaintiff ("*Jones v. City*"). The complaint was signed by LANDSKRONER and Los Angeles-based attorney Michael Libman (serving as local counsel) as attorneys for plaintiff Jones. The complaint contained detailed nonpublic information, such as the numbers of ratepayers receiving certain types of utility services, which PARADIS had obtained from the City in the course of his work as Special Counsel and (presumably) provided to LANDSKRONER.[15] Personnel from the City Attorney's Office, including CLARK, were aware that the Jones complaint was going to be filed and settled before either happened. CLARK testified that he knew by the

---

plaintiffs' counsel were "unreasonable" and voiced a preference for selecting counsel who would be easier to deal with and be "willing to do what DWP wanted." In addition, during CLARK's deposition CLARK testified that he destroyed all of his notes related to the matter just days before the deposition and now claimed not to remember things that were on those notes.

[15] In a proffer session, PARADIS confirmed that he obtained this information from LADWP in his role as Special Counsel. The nonpublic nature of that information and the advantages it conferred to the Jones complaint over the other class-action lawsuits have been noted on the record by counsel for the other plaintiffs.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

latter half of March (before the suit was ever filed) that the City would be settling with Jones.[16]

36. On April 2, 2015, LANDSKRONER sent a settlement proposal to the City. Settlement negotiations quickly ensued, and within months, without any discovery production or any motion practice, LANDSKRONER and the City had reached an agreement. The terms of that agreement, which received final approval from Judge Berle on July 20, 2017, were consistent with those originally desired by the the City Attorney. Specifically, the final settlement called for 100% reimbursement of overcharged ratepayers (as determined by LADWP and the City); a $20,000,000 remediation of the LADWP billing system; appointment of an independent monitor to oversee the remediation process;[17] and a release sufficiently broad to cover the claims alleged by the other class-action plaintiffs. The plaintiffs' attorneys were awarded approximately $19,000,000, of which more than $10,000,000 was paid to LANDSKRONER. LANDSKRONER's fees were based on billing records reflecting work allegedly performed beginning in November 2014, four months *before* he ever met or was retained by his client (and before PARADIS ever

---

[16] In his deposition, CLARK was asked the following: "How much earlier than April 1 did you know that the settlement demand would be forthcoming at some point and that you would be settling with Mr. Jones?" He replied, "Sometime during the latter half of -- the end of March." Following CLARK's deposition, in the above-referenced errata letter, the City's new counsel advised that CLARK wished to change that earlier sworn answer to "I didn't."

[17] According to PARADIS, he has largely controlled PAUL BENDER, the "independent monitor," including drafting many or all of BENDER's reports, at the direction of CLARK and others at the City Attorney's Office and with the oversight of WRIGHT.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

contacted Jones). Libman's fees, which totaled approximately $1,300,000, were based on billing records indicating work beginning in 2013, *before* Jones had even received the inflated LADWP bill leading him to seek an attorney.

37. On November 10, 2017, LANDSKRONER covertly paid $2,175,000 of his earnings from the settlement fees to PARADIS as a "referral fee." LANDSKRONER made this payment using a sham real estate investment company, S.M.A. PROPERTY HOLDINGS, LLC, which PARADIS and LANDSKRONER had set up for that purpose.[18]

B. No-Bid LADWP Contracts Awarded to Attorney PARADIS

38. In 2015 and 2016, during the settlement negotiations, PARADIS's two-member law firm received from LADWP two no-bid contracts totaling over $6,000,000 for project management services relating to remediation of the CC&B billing system.

39. On March 29, 2017, PARADIS registered a company called AVENTADOR UTILITY SOLUTIONS, LLC ("AVENTADOR") for the purpose of pursuing a separate $30 million no-bid contract from LADWP, which ostensibly covered further work to remediate the CC&B billing system.[19] To obtain support for AVENTADOR's single-source bid for this $30 million contract, PARADIS secretly

---

[18] This information was proffered by both PARADIS and LANDSKRONER and corroborated by bank records and other documentation that I have reviewed.

[19] The facts of AVENTADOR's incorporation were provided by PARADIS in a proffer and are reflected in records maintained by the California Secretary of State.

As noted below, the facts indicate that the primary purpose of this contract was different than that reflected in the contract itself and the LADWP Board's public materials about the contract.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

offered the LADWP General Manager, DAVID WRIGHT, a future post-retirement position as CEO of the company with an annual salary of $1 million and various associated benefits and perks.[20] WRIGHT accepted this offer.[21]

40. During the months preceding the Board's vote on the AVENTADOR contract, PARADIS also courted support for winning the $30 million contract from LADWP Board Vice President WILLIAM FUNDERBURK, who, in turn, reportedly solicited financial contributions from PARADIS before the vote on the AVENTADOR contract.[22] Specifically, in October 2016, FUNDERBURK invited PARADIS to an award ceremony at which FUNDERBURK was being honored, telling PARADIS that FUNDERBURK expected PARADIS's full support. On the guidance of WRIGHT, who advised PARADIS that he needed to donate because FUNDERBURK would soon be voting on PARADIS's contract, PARADIS donated $5,000 to the organization hosting FUNDERBURK's award function. Additionally, on May 31, 2017, FUNDERBURK (a practicing attorney) asked PARADIS for

---

[20] WRIGHT has stated that he intends to retire from LADWP in 2020.

[21] In a proffer session, PARADIS described his agreement with WRIGHT as to WRIGHT's future employment with and financial interest in AVENTADOR. WRIGHT confirmed their agreement in a consensually recorded conversation with PARADIS, which I have listened to.

In addition to WRIGHT's financial interest in AVENTADOR, PARADIS and WRIGHT are also planning to engage in another business venture that would solicit lucrative contracts from LADWP. Specifically, PARADIS and WRIGHT have agreed to partner with an Israeli company called CYBERGYM to open cybersecurity training facilities in Los Angeles and elsewhere to serve personnel from LADWP and other utilities. PARADIS's affiliation with this company is overt, but WRIGHT, as current LADWP General Manager, has endeavored to hide his role.

[22] PARADIS proffered the information in this paragraph.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

assistance with legal work on behalf of a class-action defendant that FUNDERBURK was representing. PARADIS agreed to assist because he knew that FUNDERBURK was set to vote on the AVENTADOR contract the following week, and he wanted FUNDERBURK to vote in favor. FUNDERBURK sent PARADIS documents via email, and PARADIS wrote a brief and sent it back to FUNDERBURK. PARADIS never billed FUNDERBURK or his client, nor did FUNDERBURK reimburse PARADIS for his legal services. Between May 31, 2017, and August 6, 2017, PARADIS performed "free" legal work for FUNDERBURK and FUNDERBURK's clients because of FUNDERBURK's influence over the AVENTADOR contract and future potential contracts. Based on my knowledge of the investigation, I believe the "free" legal work to be a financial benefit to FUNDERBURK in exchange for FUNDERBURK's official vote on the $30 million AVENTADOR contract.

41. At the LADWP Board meeting on June 6, 2017, both WRIGHT and LADWP Board President (and Gibson Dunn attorney) MEL LEVINE endorsed the $30 million no-bid contract to AVENTADOR, underscoring that the need for AVENTADOR's billing-system remediation services was so imminent that there was not sufficient time to engage in the standard competitive bidding process usually required for LADWP contracts of this size.[23]

---

[23] In this Board meeting, video footage of which is publicly available on LADWP's website and which I have reviewed, WRIGHT described the urgent need to award this no-bid contract to AVENTADOR based on the negotiated terms of the pending settlement agreement, which required the City to remediate the CC&B billing system. LEVINE enthusiastically concurred, noting that LADWP had no choice but to award the no-bid contract to

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Following the strong recommendations of WRIGHT and LEVINE, all Board members (including FUNDERBURK) voted in favor of the $30 million AVENTADOR contract, and the contract was approved.[24]

C. **Hush Money to Conceal Collusive Litigation Practices**[25]

42. PARADIS has proffered information indicating that in 2017, he and KIESEL paid $800,000 to a former KIESEL employee to buy her silence about purported fraudulent dual representation by KIESEL, PARADIS, and PETERS, who was then Chief of Civil Litigation at the City Attorney's Office. Specifically, in approximately July of 2017, KIESEL fired his secretary, Julissa Salgueriro, who had worked for both KIESEL and PETERS when they were law partners. Thereafter, Salgueriro threatened to publicly reveal that KIESEL and PETERS were secretly engaging in collusive litigation practices in the LADWP litigation as well as one or more other cases unless KIESEL paid Salgueriro $1,000,000. KIESEL initially offered to pay Salgueriro $300,000, but she rejected that offer. In October 2017, Salgueriro told PARADIS in a text message that she had approached CLARK with the information, and that CLARK had ignored her. According to PARADIS, CLARK was angry after

---

AVENTADOR. Based on my review of the evidence, and as discussed further below, I do not believe either representation (by WRIGHT or LEVINE) was fair or accurate description of the choice the LADWP Board had to make when awarding this $30 million dollar contract.

[24] The Los Angeles City Council has the prerogative to review a contract of this size. According to PARADIS, WRIGHT asked certain members of City Council not to review the AVENTADOR contract.

[25] The information in this subsection was proffered by PARADIS (with partial corroboration as described herein).

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Salgueriro reached out, and CLARK told PETERS to take care of the problem. At a hearing on December 4, 2017, Salgueriro approached counsel for PwC, [redacted] of Gibson Dunn, in the presence of KIESEL and PETERS, and offered to provide [redacted] with information that he would find interesting.[26] This action quickly spurred renewed discussions between KIESEL, PARADIS, and Salgueriro, which ultimately resulted in an agreement that KIESEL would pay $800,000 to Salgueriro to buy her silence. PARADIS agreed to pay half, and he wired $400,000 to KIESEL in or around late December of 2017. The agreement was memorialized in a confidential settlement agreement, which was prepared by a private attorney named [redacted].[27]

D. Alleged Falsification of Regulatory Paperwork by LADWP Employees with the Knowledge of Attorney President of LADWP Board

43. The above-described LADWP contract awarded to AVENTADOR purported — according to the terms of the contract itself as well as LADWP Board materials and proceedings relating to the contract — to cover services related to remediation of the CC&B billing system, as required by the negotiated terms of the settlement agreement in the *Jones v. City* lawsuit. However, information suggests that this $30 million single-source contract, which was advertised to the LADWP Board as urgent because it was mandated by the court-ordered settlement

[26] [redacted] confirmed the described incident took place (he was not certain of the hearing date but believed it to be in that general time frame).

[27] The government has requested these materials from PARADIS and anticipates receiving those materials in the near future.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

agreement, was in truth primarily intended to cover services related to assessing and improving cybersecurity for the City's power grid and other critical infrastructure.[28]

44. PARADIS alleges that in order to conceal and avoid responsibility for certain cybersecurity vulnerabilities related to critical infrastructure, LADWP employees falsified mandatory federal regulatory documents,[29] including by regularly self-reporting minor violations in order to avoid the discovery of much more significant violations, which would carry substantial fines (in some cases, millions of dollars). In separate consensually recorded conversations, the current and former Chief Information Security Officers for LADWP (STEPHEN KWOK and DAVID ALEXANDER, respectively) confirmed both LADWP's pattern of self-reporting minor violations to conceal far more significant problems, and the fact that members of LADWP management (including WRIGHT) and the LADWP Board (including LEVINE and CYNTHIA MCCLAIN-HILL) were aware of that fraudulent practice.

---

[28] This includes information proffered by PARADIS. It is corroborated in part by 1) the aforementioned consensually recorded conversations with WRIGHT; 2) separate consensually recorded conversations with an AVENTADOR employee; and 3) an AVENTADOR work plan and other documents reflecting AVENTADOR'S cybersecurity work for the City, which PARADIS provided and I have reviewed.

[29] These include documents mandated by the Federal Energy Regulatory Commission under a compliance regime known as NERC-CIP (North American Electric Reliability Corporation, Critical Infrastructure Protection). The NERC CIP plan is a set of requirements designed to secure the assets required for operating North America's bulk electric system.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

E. Alleged Bid Manipulation Involving Attorney Members of the LADWP Board

45. According to PARADIS, LADWP management and members of the Board (including WRIGHT, LEVINE, and MCLAIN-HILL) are currently working to manipulate LADWP's contracting process in order to ensure that AVENTADOR's successor company ARDENT UTILITY SOLUTIONS, LLC ("ARDENT," which the evidence I have reviewed suggests that PARADIS still controls despite a sham sale in March 2019), is awarded a lucrative contract to continue AVENTADOR's work without the competitive bidding process that is required. According to information proffered by PARADIS, LADWP routinely uses the Southern California Public Power Authority ("SCPPA") to circumvent LADWP's standard competitive bid process, which commonly takes 12-18 months, and to falsely make it appear as though a competitive bid process took place.[30] With respect to the contract by which AVENTADOR's work would be continued, 28 vendors submitted proposals to SCPPA, and SCPPA selected three vendors, including ARDENT, as the final candidates. SCPPA is set to vote on these candidates on April 18, 2019. On April 5, 2019, in a consensually recorded conversation by PARADIS, LEVINE and MCCLAIN-HILL confirmed to PARADIS that ARDENT would be the primary vendor, despite the fact that SCPPA had not yet voted on selecting the vendor(s). WRIGHT's financial interest in the success of AVENTADOR (via his secret deal with PARADIS) appears to explain his efforts to secure this contract for ARDENT, but the motivations of LEVINE,

[30] According to the SCPPA website, WRIGHT is the Secretary of SCPPA and a current member of the SCPPA Board of Directors.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

MCCLAIN-HILL, and other City officials to fix the process in favor of ARDENT are presently unknown.

F. Other Manipulation of LADWP Contract Processes[31]

46. In June 2016, while representing the City in its litigation against PwC, PARADIS proposed debarring[32] PwC. According to PARADIS, in a closed session on June 21, 2016, the LADWP Board voted 4-0 in favor of debarring PwC, with Board President LEVINE recusing himself from the discussion and vote due to a conflict of interest.[33] PARADIS further reported that a press release touting the debarment was drafted and circulated among the staff of the City Attorney's Office. According to PARADIS, LEVINE, City Attorney Michael Feuer, former Chief of Civil Litigation PETERS, LADWP General Counsel Joseph Brajevich, and others thereafter embarked on a furtive and successful campaign to influence the other LADWP Board members to secretly change their votes, which ultimately resulted in the PwC

---

[31] PARADIS proffered the information in this paragraph.

[32] Debarment is the state of being excluded from enjoying certain possessions, rights, privileges, or practices and the act of prevention by legal means. For example, companies can be debarred from contracts due to allegations of fraud, mismanagement, and similar improprieties.

This initiative to debar PwC came in the wake of public allegations that PwC managers overbilled the City and then spent the money on prostitutes, luxury bottle service liquor, and entertainment in Las Vegas. See https://www.latimes.com/local/lanow/la-me-ln-dwp-billing-20160630-snap-story.html.

[33] LEVINE is recused from LADWP Board matters involving PwC because PwC is a prominent and lucrative Gibson Dunn client. (LEVINE presently works at Gibson Dunn and Clark formerly worked at Gibson Dunn.)

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

debarment issue being dropped. The initial 4-0 vote in favor of debarment was not reflected in Board materials.

47. Specifically, PARADIS has proffered the following information: On June 30, 2016, he and his law partner, GINA TUFARO, were called to meet with Feuer in his office. Feuer was angry about the debarment initiative and informed PARADIS that he (Feuer) was the "team captain" and as such was charged with making the decision as to whether to pursue debarment. PARADIS stated that the Board had already voted and debarment was therefore going to happen, and Feuer said words to the effect that, "We'll see about that."[34] At Feuer's direction, PARADIS then made a presentation to LADWP management, including WRIGHT, in favor of debarment, and PETERS gave a contrary presentation against debarment. PARADIS met with LADWP Board Vice President FUNDERBURK, who told PARADIS that both he and another Board member, William Fleming, were committed to debarment and would stand by their votes in favor of debarring PwC. A few days later, FUNDERBURK contacted PARADIS to advise that debarment was probably not going to happen. PARADIS went to WRIGHT, threatened to "blow the whistle" if he didn't learn what was going on, and obtained WRIGHT's permission to review the emails from the LADWP server during the period of the debarment dispute. PARADIS printed a large number of relevant emails

[34] According to PARADIS, Feuer stated that the debarment process was "in shambles," and thus that debarment was not a viable option. However, PARADIS noted that the Board also voted to debar another entity at the same June 21, 2016 meeting, and that this other debarment vote was never challenged.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

reflecting communications about debarment and behind-the-scene efforts by LEVINE, Feuer, Bravjevich, then-LADWP General Manager Marci Edwards, and others to reverse the Board's vote to debar PwC.[35] Debarment of PwC did not ultimately happen, and the minutes from the June 21, 2016 LADWP Board meeting do not reflect the original 4-0 vote in favor of debarment.[36]

G. Obstruction of Justice by WRIGHT

48. On March 28, 2019, PARADIS and WRIGHT exchanged text messages arranging a meeting in Rancho Mirage, California, approximately 120 miles from Los Angeles. PARADIS proffered that he and WRIGHT would previously meet in Rancho Mirage to conceal their meetings when discussing their arrangement and certain Target Offenses.

49. On March 29, 2019, in a consensually recorded call, PARADIS and WRIGHT arranged a meeting on March 30, 2019, at 6:00 AM at PARADIS' residence in Rancho Mirage. WRIGHT said he wanted an early hour meeting because he was worried that people would see PARADIS and WRIGHT together. Specifically, WRIGHT said he was concerned because the Daily Journal and LA Times were reporting on the suspected fraud(s) discussed above.

50. On March 30, 2019, in a consensually recorded meeting, PARADIS and WRIGHT discussed the quid pro quo arrangement and confirmed WRIGHT's financial interest in AVENTADOR. PARADIS

---

[35] PARADIS's criminal defense attorneys have represented that they are working to copy and provide these voluminous materials to the government's filter team for review.

[36] With respect to this item, the Board meeting minutes from June 21, 2016, note: "Discussion held - action taken but not a final action that is reportable."

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

informed WRIGHT that WRIGHT's future employment with AVENTADOR was still in the works. WRIGHT stated that he thought that prospect was dead, but after speaking to PARADIS, he now felt "resurrected." WRIGHT and PARADIS discussed the need to be "on the same page" and what to say if anyone, including specifically the FBI, were to question the fraud and formation of AVENTADOR. WRIGHT was concerned about potential discovery of his text message and email communications between himself, PARADIS, and LEVINE over **WRIGHT's PHONE.**[37] WRIGHT was also concerned about the AVENTADOR laptop computer (**WRIGHT's LAPTOP**) that PARADIS had previously given to him. Following a discussion of their options concerning those communications, WRIGHT requested that PARADIS "get his people" to destroy all evidence of their communications on **WRIGHT'S PHONE** and all information on the **WRIGHT'S LAPTOP.**[38] Specifically, WRIGHT told PARADIS to destroy all his emails from his two AOL email accounts, as well as the corresponding iCloud accounts for them (the **TARGET ACCOUNTS**).

---

[37] PARADIS informed me that he received emails from WRIGHT from both of WRIGHT's AOL email accounts: [redacted]om and [redacted] PARADIS also informed me that on some of these emails, he was cc'd on communications between WRIGHT and the other subjects in this investigation, including, but not limited to, GINA TUFARO, MEL LEVINE, CYNTHIA MCCLAIN-HILL, STEPHEN KWOK, DAVID ALEXANDER, JACK LANDSKRONER, PAUL KIESEL, JAMES CLARK, THOMAS PETERS, WILLIAM FUNDERBURK, PAUL BENDER and others from the Los Angeles City Attorney's Office. While PARADIS has offered to show me some of these emails, I have not reviewed any of them, given that the possibility that some may implicate an attorney-client privilege.

[38] Based on the context of the conversation and my knowledge of this case, I understood this to be a reference to the team of hackers and intelligence agency veterans that PARADIS had recruited and hired to work for AVENTADOR on the above-referenced cybersecurity issues.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

WRIGHT expressly noted that he was paying $0.99 a month for iCloud storage.

51. WRIGHT agreed to provide PARADIS **WRIGHT'S PHONE** and **WRIGHT'S LAPTOP** so that WRIGHT could "wipe" the devices clean of incriminating evidence. In addition, WRIGHT told PARADIS that he already shredded all related documents within WRIGHT's office that involved PARADIS and/or LEVINE, and that he planned to do so again the following week. PARADIS agreed to wipe **WRIGHT's PHONE** and laptop and delete all emails on the PROVIDERS' servers. In addition, WRIGHT and PARADIS discussed utilizing the application Confide to communicate as a means to conceal their communications.[39]

52. On March 31, 2019, in a consensually recorded meeting, WRIGHT provided PARADIS **WRIGHT'S PHONE** and **WRIGHT'S LAPTOP** so that, as he and PARADIS had agreed, PARADIS could wipe the devices to include deleting all text messages and emails. WRIGHT and PARADIS agreed to meet in Santa Monica, California, on April 1, 2019, to return **WRIGHT's PHONE** wiped. PARADIS subsequently provided **WRIGHT's PHONE** and **WRIGHT's LAPTOP** to the FBI to preserve all evidence on the phone and laptop.[40]

53. On April 1, 2019, in a consensually recorded meeting,

---

[39] Confide is an encrypted messaging application that deletes each communication after it is viewed. PARADIS proffered that WRIGHT had previously asked him to use Confide in connection with the Target Offenses.

[40] **WRIGHT's PHONE** was imaged by the FBI but not reviewed by me. This extraction, as well as the laptop, are described in Attachment A-1 and outlined above as the **SUBJECT DEVICES**. The **SUBJECT DEVCIES** were entered into FBI evidence and have not yet been reviewed.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

PARADIS and WRIGHT discussed further concealing their future communication via "burner"[41] phones. PARADIS and WRIGHT agreed to meet on April 3, 2019, at the Disney Concert Hall in Los Angeles, California, for WRIGHT to pick up a burner phone from PARADIS.

54. On April 3, 2019, I conducted surveillance of PARADIS and WRIGHT's meeting at the Disney Concert Hall. PARADIS was seated at a table in the back corner of the café with a brown paper bag that contained a burner phone (provided to him by the FBI) and WRIGHT's phone. WRIGHT approached PARADIS and provided a head nod which PARADIS understood to mean WRIGHT acknowledged PARADIS' presence. PARADIS subsequently left the bag with the two phones on the table and walked into the men's bathroom. WRIGHT then approached the table and removed the bag from the table and exited the concert hall before PARADIS returned back to the table. PARADIS and WRIGHT had no verbal interactions during this exchange. Based on my training and experience, PARADIS and WRIGHT's behavior was consistent with a surreptitious "drop" designed to mask the existence of any meeting or transaction between the two. PARADIS then sent a text message via his own FBI provided burner phone disclosing to WRIGHT's burner phone the number for PARADIS' new burner phone.

55. PARADIS then requested from WRIGHT the usernames and passwords for WRIGHT's email accounts and Apple iCloud accounts

---

[41] A "burner" phone is typically a difficult to trace phone that provides little to no paper trail back to its user.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

that WRIGHT requested be wiped. WRIGHT subsequently provided the information for his accounts [redacted], [redacted],[42] and iCloud accounts [redacted] and [redacted]. These accounts were the email accounts and Apple iCloud accounts associated with WRIGHT's phone and email accounts, that WRIGHT requested be wiped because they contained communications with PARADIS, LEVINE, and others related to certain Target Offenses. PARADIS subsequently provided this account information to the FBI.

56. WRIGHT provided PARADIS the devices and account information freely and with the request and expectation that PARADIS wipe and delete all information on the devices/accounts as a means to destroy evidence related to the Target Offenses. Therefore, the government does not believe WRIGHT maintains an expectation of privacy in the referenced devices/accounts. Nevertheless, in the abundance of caution, the government seeks these warrants to establish that there is probable cause to search the extractions/downloads of the devices/accounts for evidence of the Target Offense and more specifically outlined in Attachments B-1 through B-3.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

57. As used herein, the term "digital device" includes the **SUBJECT DEVICES**.

---

[42] On April 3, 2019, WRIGHT inadvertently provided an incorrect email address as [redacted] when it actually was [redacted]. On April 11, 2019, PARADIS confirmed the email address in a text message utilizing the burner phones. WRIGHT responded, "I don't think [redacted] is mine. Just [redacted]."

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

58. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

59. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

60. Other than what has been described herein, to my knowledge, the United States has not attempted to review this data by other means.

VIII. BACKGROUND ON E-MAIL AND SOCIAL MEDIA ACCOUNTS AND THE PROVIDER

61. In my training and experience, and discussions with senior agents, I have learned that providers of e-mail and/or social media services offer a variety of online services to the public. Providers, like the PROVIDERS, allow subscribers to obtain accounts like the **TARGET ACCOUNTS**. Subscribers obtain an account by registering with the PROVIDERS. During the registration process, the PROVIDERS ask subscribers to provide basic personal information. Therefore, the computers of the PROVIDERS are likely to contain stored electronic communications and information concerning subscribers and their use of the PROVIDERS' services, such as account access information, e-mail or message transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the **TARGET ACCOUNTS**.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

62. In my training and experience, and discussions with senior agents, e-mail and social media providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail or social media account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the **TARGET ACCOUNTS.**

63. In my training and experience, and discussions with senior agents, providers of e-mail and social media often maintain, have access to, and store information related to the location of the users of accounts they service. That information may be obtained by the PROVIDERS in a number of ways. For example, a user may access the PROVIDERS services by running an application on the user's phone or mobile device, which application has access to the location information residing on the phone or mobile device, such as Global Positioning System (GPS) information. It may also be accessible through "check-in" features that some providers offer that allows users to transmit or display their location to their "friends" or "acquaintances" via the provider.

64. In my training and experience, and discussions with senior agents, e-mail and social media providers typically

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail and social media providers often have records of the Internet Protocol ("IP") address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the **TARGET ACCOUNTS**.

65. In my training and experience, and discussions with senior agents, e-mail and social media account users will sometimes communicate directly with the service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers of e-mails and social media services typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

because the information can be used to identify the user(s) of the **TARGET ACCOUNTS.**

66. I know from my training and experience, and discussions with senior agents, that the complete contents of an account may be important to establishing the actual user who has dominion and control of that account at a given time. Accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. Given the ease with which accounts may be created under aliases, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of an account, investigators often have to rely on circumstantial evidence to show that an individual was the actual user of a particular account. Only by piecing together information contained in the contents of an account may an investigator establish who the actual user of an account was. Often those pieces will come from a time period before the account was used in the criminal activity. Limiting the scope of the search would, in some instances, prevent the government from identifying the true user of the account and, in other instances, may not provide a defendant with sufficient information to identify other users of the account. Therefore, the contents of a given account, including the e-mail addresses or account identifiers and messages sent to that account, often provides important evidence regarding the actual user's dominion and control of that account. For the purpose of searching for content demonstrating the actual user(s) of the **TARGET ACCOUNTS,**

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

I am requesting a warrant requiring the PROVIDERS to turn over all information associated with the **TARGET ACCOUNTS** with the date restriction included in Attachments B-2 and B-3 for review by the search team.

67. Relatedly, the government must be allowed to determine whether other individuals had access to the **TARGET ACCOUNTS**. If the government were constrained to review only a small subsection of an account, that small subsection might give the misleading impression that only a single user had access to the account.

68. I also know based on my training and experience, and discussions with senior agents, that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as "lol" to express "laugh out loud"), or codewords (which require entire strings or series of conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of a message or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and paren :) to convey a smile or agreement) to discuss matters. "Keyword searches" would not account for any of these possibilities, so actual review of the contents of an account by law enforcement personnel with information regarding the identified criminal

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

activity, subject to the search procedures set forth in Attachments B-2 and B-3, is necessary to find all relevant evidence within the account.

69. As set forth in Attachments B-2 and B-3, I am requesting a warrant that permits the search team to keep the original production from the PROVIDERS under seal until the investigation is completed and, if a case is brought, that case is completed through disposition, trial, appeal, or collateral proceeding.

a. I make that request because I believe it might be impossible for the PROVIDER to authenticate information taken from the **TARGET ACCOUNTS** as its business record without the original production to examine. Even if the PROVIDERS kept an original copy at the time of production (against which it could compare the results of the search at the time of trial), the government cannot compel the PROVIDERS to keep a copy for the entire pendency of the investigation and/or case. If the original production is destroyed, it may be impossible for the PROVIDERS to examine a particular document found by the search team and confirm that it was a business record of the PROVIDERS' taken from the **TARGET ACCOUNTS.**

b. I also know from my training and experience, and discussions with senior agents, that many accounts are purged as part of the ordinary course of business by providers. For example, if an account is not accessed within a specified time period, it -- and its contents -- may be deleted. As a consequence, there is a risk that the only record of the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

contents of an account might be the production that a provider makes to the government, for example, if a defendant is incarcerated and does not (perhaps cannot) access his or her account. Preserving evidence, therefore, would ensure that the government can satisfy its Brady obligations and give the defendant access to evidence that might be used in his or her defense.

A. Services Provided by Apple, Inc.

70. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

71. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices. iCloud can also be used to back up various settings and history of a user's activity, such as searches and web history.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

remotely identify and track the location of, display a message on, and wipe the contents of those devices.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

72. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

73. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

74. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

75. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

76. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

77. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

78. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

79. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

80. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

81. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime),

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

82. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

83. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

IX. REQUEST FOR NON-DISCLOSURE

84. Pursuant to 18 U.S.C. § 2705(b), I request that the Court enter an order commanding the PROVIDERS not to notify any person, including the subscriber(s) of the **TARGET ACCOUNTS**, of the existence of the warrant until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date the PROVIDERS comply with the warrant or such later date as may be set by the Court upon application for an extension by the United States. There is reason to believe that

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

such notification will result in (1) flight from prosecution; (2) destruction of or tampering with evidence; (3) intimidation of potential witnesses; and (4) otherwise seriously jeopardizing the investigation. The current investigation set forth above is not public, and I know, based on my training and experience, that those involved in criminal activity often will destroy digital evidence if they learn of an investigation. In addition, if the PROVIDERS or other person notifies the targets of the investigation that a warrant has been issued for the **TARGET ACCOUNTS**, the subjects might further mask their activity and seriously jeopardize the investigation.

\\

\\

\\

\\

\\

X. CONCLUSION

85. Based on the foregoing, I request that the Court issue the requested search warrants.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

/s/

ANDREW CIVETTI, Special Agent
Federal Bureau of
Investigation

Subscribed to and sworn before
me on April 18, 2019.

JACQUELINE CHOOLJIAN

HONORABLE
UNITED STATES MAGISTRATE JUDGE

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

ATTACHMENT A-1

PROPERTY TO BE SEARCHED

a) A My Passport WD hard drive, serial number WXQ1A6803KA0, which contains the Cellebrite extraction of a cellular telephone, [redacted] used by DAVID WRIGHT;

b) An Apple MacBook Pro with serial number C02SN0ZRG8WN and model number A1398.

ATTACHMENT A-2

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the account identified as [redacted]om and [redacted] and being used by DAVID WRIGHT, that is within the possession, custody, or control of Oath, Inc. dba America Online ("AOL"), a company that accepts service of legal process at its headquarters located at a provider of electronic communication and remote computing services, headquartered at 22000 AOL Way, Dulles, Virginia 20166, regardless of where such information is stored, held, or maintained.

ATTACHMENT A-3

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the accounts identified as [redacted] and [redacted] and being used by DAVID WRIGHT, that is within the possession, custody, or control of Apple, Inc., a provider of electronic communication and remote computing services that accepts service of legal process at 1 Infinite Loop, M/S 36-SU, Cupertino, California, 95014, regardless of where such information is stored, held, or maintained.

ATTACHMENT B-1

A. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 666 (Bribery and Kickbacks Concerning Federal Funds), 1341 (Mail Fraud), 1343 (Wire Fraud), and 1346 (Deprivation of Honest Services), 1505 (Obstruction of Federal Proceeding), 1510 (Obstruction of Justice), 1951 (Extortion) and 1956 (Money Laundering) (collectively the "Target Offenses"), namely:

a. Evidence of who accessed or used the digital device on or after February 1, 2015, including records about their identities and whereabouts.

b. Communications or agreements on or after February 1, 2015, referencing: PAUL PARADIS, GINA TUFARO, MEL LEVINE, CYNTHIA MCCLAIN-HILL, STEPHEN KWOK, DAVID ALEXANDER, JACK LANDSKRONER, PAUL KIESEL, JAMES CLARK, THOMAS PETERS, WILLIAM FUNDERBURK, PAUL BENDER, AVENTADOR UTILITY SOLUTIONS, LLC, ARDENT CYBER SOLUTIONS, LLC, and CYBERGYM (the "Subjects").

c. Records, documents, programs, applications, or materials from on or after February 1, 2015, referencing:

i. DAVID WRIGHT's bank accounts, credit card accounts, other financial accounts, and wire transfer records;

ii. DAVID WRIGHT's calendar or date book, including calendars or date books stored on digital devices;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

iii. Los Angeles Department of Water and Power contracts, proposed contracts, and contracting processes, including but not limited to any manipulations of contracting processes, the use of other entities to circumvent the requirement for open-bid contracts, and procedures and actions regarding debarment of vendors;

iv. Any private business ventures in which a Los Angeles City ("City") official had a financial interest, including but not limited to AVENTADOR UTILITY SOLUTIONS, LLC, CYBERGYM, and ARDENT UTILITY SOLUTIONS, LLC;

v. Any lawsuit where the City of Los Angeles ("the City") was a party to the lawsuit and appears to have had a legal, representational, and/or financial interest in both sides of the lawsuit.

vi. Financial payments, gifts, services, or other benefits given or offered to officials at LADWP or the City Attorney's Office or their staff or family members, or solicited by officials at LADWP or the City Attorney's Office or their staff or family members;

vii. Records, data, or other information required by or submitted to the Federal Energy Regulatory Commission ("FERC") or the North American Electric Reliability Corporation, Critical Infrastructure Protection ("NERC-CIP"); and

viii. Cybersecurity vulnerabilities within the LADWP, including the City's power grid, water supply, and other critical infrastructure.

d. Any SUBJECT DEVICE which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Target Offenses, and forensic copies thereof.

e. With respect to any SUBJECT DEVICE used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations;

ii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

iii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications or other text or written communications sent to or received from any digital device;

iv. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents,

browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

v. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

vi. evidence of the attachment of other devices;

vii. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

viii. evidence of the times the device was used;

ix. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

x. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

xi. records of or information about Internet Protocol addresses used by the device;

xii. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

B. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

6. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications, work product, or other potentially privileged communications:

7. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will review only digital device data which has been released by the Privilege Review Team.

8. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

9. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will

conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

10. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

11. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

12. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

13. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered,

including how it was immediately apparent contraband or evidence of a crime.

14. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

15. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

16. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

17. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

18. After the completion of the search of the digital devices, the government shall not access digital data falling

outside the scope of the items to be seized absent further order of the Court.

19. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary

to access the digital device or data stored on the digital device.

20. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

C. SEARCH PROCEDURE FOR DIGITAL DEVICES

21. In searching the SUBJECT DEVICES or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any SUBJECT DEVICE capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each SUBJECT DEVICE where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICE(S) as soon as is practicable but not to exceed 180 days from the date of issuance of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each SUBJECT DEVICE capable of containing any of the items to be seized to the search protocols to determine whether the SUBJECT DEVICE and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques [, including to search for known images of child pornography.]

e. If the search team, while searching a SUBJECT DEVICE, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that SUBJECT DEVICE pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence

of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

f. If the search determines that a SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the SUBJECT DEVICE and delete or destroy all forensic copies thereof.

g. If the search determines that a SUBJECT DEVICE does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a SUBJECT DEVICE if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the SUBJECT DEVICE(S), the government shall not access digital data falling

outside the scope of the items to be seized absent further order of the Court.

k. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

ATTACHMENT B-2

EMAIL ITEMS TO BE SEIZED

I. SEARCH PROCEDURE INCLUDING PRIVILEGE REVIEW PROCEDURE

1. The search warrant will be presented to personnel of Oath, Inc. dba America Online ("AOL") (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide the Section II information in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.13.a. below), law enforcement agents and/or other individuals assisting law enforcement agents who are not participating in the investigation of the case and who are assigned as the "Privilege Review Team" will review the content records, according to the procedures set forth herein, to determine whether or not any of the content records appears to contain or refer to communications between an attorney, or to contain the work product of an attorney, or between a spouse and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

any person ("potentially privileged information"). The "Search Team" (law enforcement personnel conducting the investigation and search and other individuals assisting law enforcement personnel in the search) will review only content records which have been released by the Privilege Review Team. With respect to the non-content information produced by the PROVIDER (see Section II.13.b. below), no privilege review need be performed and the Search Team may review immediately.

5. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for in the content records, to include specific words like names of any identified attorneys or law firms and names of any identified spouses] or their email addresses, and generic words such as "privileged" and "work product". The Privilege Review Team will conduct an initial review of all of the content records by using the privilege key words, and by using search protocols specifically chosen to identify content records containing potentially privileged information. Content records that are not identified by this initial review as potentially privileged may be given to the Search Team.

6. Content records that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Content records determined by this review not to be potentially privileged may be given to the Search Team. Content records determined by this review to be potentially privileged will be given to the United States Attorney's Office

for further review by a Privilege Review Team Assistant United States Attorney ("PRTAUSA"). Content records identified by the PRTAUSA after review as not potentially privileged may be given to the Search Team. If, after review, the PRTAUSA determines it to be appropriate, the PRTAUSA may apply to the court for a finding with respect to particular content records that no privilege, or an exception to the privilege, applies. Content records that are the subject of such a finding may be given to the Search Team. Content records identified by the PRTAUSA after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

7. The Search Team will search only the content records that the Privilege Review Team provides to the Search Team at any step listed above in order to locate, extract and seize content records that are within the scope of the search warrant (see Section III below). The Search Team does not have to wait until the entire privilege review is concluded to begin its review for content records within the scope of the search warrant. The Privilege Review Team may also conduct the search for content records within the scope of the search warrant if that is more efficient. The search may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

8. If, while reviewing content records or non-content information, either the Privilege Review Team or the Search Team

encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

9. The Privilege Review Team and the Search Team will complete the search of non-content information and both stages of the search of the content records discussed herein as soon as is practicable but not to exceed 180 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the records beyond this 180-day period without first obtaining an extension of time order from the Court.

10. Once the Privilege Review Team and the Search Team have completed their review of the non-content information and the content records and the Search Team has created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the Search Team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, neither the Privilege Review Team nor the Search Team will access the data from the sealed original production which fell outside the scope of the items to be seized or was determined to be privileged absent further order of the Court.

11. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

12. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDERS

13. To the extent that the information described in Attachment A-2, is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each **TARGET ACCOUNT** listed in Attachment A-2:

a. All contents of all wire and electronic communications associated with [redacted]m and [redacted] limited to that which occurred on or after February 1, 2015, [1] including:

i. All e-mails, communications, or messages of any kind associated with the **TARGET ACCOUNTS**, including stored or preserved copies of messages sent to and from the account,

[1] To the extent it is not reasonably feasible for the PROVIDER to restrict any categories of records based on this date restriction (for example, because a date filter is not available for such data), the PROVIDER shall disclose those records in its possession at the time the warrant is served upon it.

deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information associated with each e-mail or message, and any related documents or attachments.

ii. All records (including content records and the stored application data) pertaining to any Oath, Inc. service associated with the **TARGET ACCOUNTS**;

iii. All records (including content records and the stored application data) associated with the **TARGET ACCOUNTS** pertaining to Location History, including custom maps, changes and edits to public places, starred places, private labels of locations, and saved locations.

iv. All records or other information stored by subscriber(s) of the **TARGET ACCOUNTS**, including address books, contact and buddy lists, calendar data, pictures or photos, videos, notes, texts, links, user profiles, account settings, access logs, and files.

v. All records pertaining to communications between the PROVIDER and any person regarding the **TARGET ACCOUNTS**, including contacts with support services and records of actions taken.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), any alternate names, other account names or e-mail addresses associated with the account, linked

accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, and including any changes made to any subscriber information or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred, for the **TARGET ACCOUNTS.**

ii. All user connection logs and transactional information of all activity relating to the **TARGET ACCOUNTS** described above, including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations, , and including specifically the specific product name or service to which the connection was made.

iii. Any information showing the location of the user of a **TARGET ACCOUNTS**, including while sending or receiving a message using a **TARGET ACCOUNTS** or accessing or logged into a **TARGET ACCOUNTS.**

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

14. For each **TARGET ACCOUNT** listed in Attachment A-2, the search team may seize:

a. All information described above that constitutes evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 666 (Bribery and Kickbacks Concerning Federal Funds), ~~1341~~ Wire fraud, 1343, and 1346 (Deprivation of Honest Services), 1505 Obstructing federal proceedings, 1510 (Obstruction of Justice), 1951 (Extortion) and 1956 (Money Laundering) (the "Target Offenses"), involving DAVID WRIGHT, PAUL PARADIS, GINA TUFARO, MEL LEVINE, CYNTHIA MCCLAIN-HILL, STEPHEN KWOK, DAVID ALEXANDER, JACK LANDSKRONER, PAUL KIESEL, JAMES CLARK, THOMAS PETERS, WILLIAM FUNDERBURK, PAUL BENDER, AVENTADOR UTILITY SOLUTIONS, LLC, ARDENT CYBER SOLUTIONS, LLC, and CYBERGYM (the "Subjects") namely:

i. Information relating to who created, accessed, or used the **TARGET ACCOUNTS**, including records about their identities and whereabouts.

ii. Communications or agreements referencing PAUL PARADIS, GINA TUFARO, MEL LEVINE, CYNTHIA MCCLAIN-HILL, STEPHEN KWOK, DAVID ALEXANDER, JACK LANDSKRONER, PAUL KIESEL, JAMES CLARK, THOMAS PETERS, WILLIAM FUNDERBURK, PAUL BENDER, AVENTADOR UTILITY SOLUTIONS, LLC, ARDENT CYBER SOLUTIONS, LLC, and CYBERGYM;

iii. Records, documents, programs, applications, or materials referencing:

1. DAVID WRIGHT's bank accounts, credit card accounts, other financial accounts, and wire transfer records;

2. DAVID WRIGHT's calendar or date book, including calendars or date books stored on digital devices;

3. Los Angeles Department of Water and Power contracts, proposed contracts, and contracting processes, including but not limited to any manipulations of contracting processes, the use of other entities to circumvent the requirement for open-bid contracts, and procedures and actions regarding debarment of vendors;

4. Any private business ventures in which a Los Angeles City ("City") official had a financial interest, including but not limited to AVENTADOR UTILITY SOLUTIONS, LLC, CYBERGYM, and ARDENT UTILITY SOLUTIONS, LLC;

5. Any lawsuit where the City of Los Angeles ("the City") is a party to the lawsuit and appears to have a legal, representation, and/or financial interest in both sides of the lawsuit;

6. Financial payments, gifts, services, or other benefits given or offered to officials at LADWP or the City Attorney's Office or their staff or family members, or solicited by officials at LADWP or the City Attorney's Office or their staff or family members;

7. Records, data, or other information required by or submitted to the Federal Energy Regulatory Commission ("FERC") or the North American Electric Reliability Corporation, Critical Infrastructure Protection ("NERC-CIP");

8. Cybersecurity vulnerabilities within the Los Angeles Department of Water and Power, including the City's power grid, water supply, and other critical infrastructure; and

iv. All records and information described above in Section II.13.b.

IV. PROVIDER PROCEDURES

15. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. The PROVIDER shall send such information to:

16. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

17. IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 2705(b), that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A-2, of the existence of the warrant, until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date the PROVIDER complies with this warrant or such later date as may be set by the Court upon application for an extension by the United States. Upon expiration of this order, at least ten business days prior to disclosing the existence of the warrant, the PROVIDER shall notify the agent identified in paragraph 15 above of its intent to so notify.

ATTACHMENT B-3

EMAIL ITEMS TO BE SEIZED

I. SEARCH PROCEDURE INCLUDING PRIVILEGE REVIEW PROCEDURE

1. The search warrant will be presented to personnel of Apple Inc. (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide the Section II information in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.13.a. below), law enforcement agents and/or other individuals assisting law enforcement agents who are not participating in the investigation of the case and who are assigned as the "Privilege Review Team" will review the content records, according to the procedures set forth herein, to determine whether or not any of the content records appears to contain or refer to communications between an attorney, or to contain the work product of an attorney, or between a spouse and any person ("potentially privileged information"). The "Search

Team" (law enforcement personnel conducting the investigation and search and other individuals assisting law enforcement personnel in the search) will review only content records which have been released by the Privilege Review Team. With respect to the non-content information produced by the PROVIDER (see Section II.13.b. below), no privilege review need be performed and the Search Team may review immediately.

5. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for in the content records, to include specific words like names of any identified attorneys or law firms and names of any identified spouses] or their email addresses, and generic words such as "privileged" and "work product". The Privilege Review Team will conduct an initial review of all of the content records by using the privilege key words, and by using search protocols specifically chosen to identify content records containing potentially privileged information. Content records that are not identified by this initial review as potentially privileged may be given to the Search Team.

6. Content records that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Content records determined by this review not to be potentially privileged may be given to the Search Team. Content records determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a Privilege Review Team Assistant United

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

States Attorney ("PRTAUSA"). Content records identified by the PRTAUSA after review as not potentially privileged may be given to the Search Team. If, after review, the PRTAUSA determines it to be appropriate, the PRTAUSA may apply to the court for a finding with respect to particular content records that no privilege, or an exception to the privilege, applies. Content records that are the subject of such a finding may be given to the Search Team. Content records identified by the PRTAUSA after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

7. The Search Team will search only the content records that the Privilege Review Team provides to the Search Team at any step listed above in order to locate, extract and seize content records that are within the scope of the search warrant (see Section III below). The Search Team does not have to wait until the entire privilege review is concluded to begin its review for content records within the scope of the search warrant. The Privilege Review Team may also conduct the search for content records within the scope of the search warrant if that is more efficient. The search may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

8. If, while reviewing content records or non-content information, either the Privilege Review Team or the Search Team encounters immediately apparent contraband or other evidence of

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a crime outside the scope of the items to be seized, the team shall immediately discontinue its search pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

9. The Privilege Review Team and the Search Team will complete the search of non-content information and both stages of the search of the content records discussed herein as soon as is practicable but not to exceed 180 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the records beyond this 180-day period without first obtaining an extension of time order from the Court.

10. Once the Privilege Review Team and the Search Team have completed their review of the non-content information and the content records and the Search Team has created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the Search Team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, neither the Privilege Review Team nor the Search Team will access the data from the sealed original production which fell outside the scope of the items to be seized or was determined to be privileged absent further order of the Court.

11. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

12. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDERS

13. To the extent that the information described in Attachment A-3, is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each **TARGET ACCOUNT** listed in Attachment A-3:

a. All contents of all wire and electronic communications associated with [redacted]m and [redacted], limited to that which occurred on or after February 1, 2015, [1] including:

i. All e-mails, communications, or messages of any kind associated with the **TARGET ACCOUNTS**, including stored or preserved copies of messages sent to and from the account, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information

[1] To the extent it is not reasonably feasible for the PROVIDER to restrict any categories of records based on this date restriction (for example, because a date filter is not available for such data), the PROVIDER shall disclose those records in its possession at the time the warrant is served upon it.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

associated with each e-mail or message, and any related documents or attachments.

ii. All records (including content records and the stored application data) associated with the **TARGET ACCOUNT** pertaining to Location History and maps, including custom maps, changes and edits to public places, starred places, private labels of locations, and saved locations.

iii. All records or other information stored by subscriber(s) of the **TARGET ACCOUNT**, including address books, contact and buddy lists, calendar data, pictures or photos, videos, notes, texts, links, user profiles, account settings, access logs, and files.

iv. All records pertaining to communications between the PROVIDER and any person regarding the **TARGET ACCOUNT**, including contacts with support services and records of actions taken.

v. All stored files and other records stored on iCloud for each **TARGET ACCOUNT**, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks.

vi. All files, keys, or other information necessary to decrypt any data produced in an encrypted form,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), any alternate names, other account names or e-mail addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, and including any changes made to any subscriber information or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred, for the **TARGET ACCOUNT**.

ii. All activity, connection, and transactional logs for all activity relating to each **TARGET ACCOUNT** described above in Section II.13.a. (all log files, dates, times, durations, data transfer volumes, methods of connection, authentication logs, IP addresses, ports, routing information, dial-ups, and locations), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

(including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers).

i. Any information showing the location of the user of a **TARGET ACCOUNT**, including while sending or receiving a message using a **TARGET ACCOUNT** or accessing or logged into a **TARGET ACCOUNT**.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

14. For each **TARGET ACCOUNT** listed in Attachment A-2, the search team may seize:

a. All information described above that constitutes evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 666 (Bribery and Kickbacks Concerning Federal Funds), 1341, 1343, and 1346 (Deprivation of Honest Services), 1505, 1510 (Obstruction of Justice), 1951 (Extortion) and 1956 (Money Laundering) (the "Target Offenses"), involving DAVID WRIGHT, PAUL PARADIS, GINA TUFARO, MEL LEVINE, CYNTHIA MCCLAIN-HILL, STEPHEN KWOK, DAVID ALEXANDER, JACK LANDSKRONER, PAUL KIESEL, JAMES CLARK, THOMAS PETERS, WILLIAM FUNDERBURK, PAUL BENDER, AVENTADOR UTILITY SOLUTIONS, LLC, ARDENT CYBER SOLUTIONS, LLC, and CYBERGYM (the "Subjects") namely:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

i. Information relating to who created, accessed, or used the **TARGET ACCOUNTS**, including records about their identities and whereabouts.

ii. Communications or agreements referencing PAUL PARADIS, GINA TUFARO, MEL LEVINE, CYNTHIA MCCLAIN-HILL, STEPHEN KWOK, DAVID ALEXANDER, JACK LANDSKRONER, PAUL KIESEL, JAMES CLARK, THOMAS PETERS, WILLIAM FUNDERBURK, PAUL BENDER, AVENTADOR UTILITY SOLUTIONS, LLC, ARDENT CYBER SOLUTIONS, LLC, and CYBERGYM

iii. Records, documents, programs, applications, or materials referencing:

1. DAVID WRIGHT's bank accounts, credit card accounts, other financial accounts, and wire transfer records;

2. DAVID WRIGHT's calendar or date book, including calendars or date books stored on digital devices;

3. Los Angeles Department of Water and Power contracts, proposed contracts, and contracting processes, including but not limited to any manipulations of contracting processes, the use of other entities to circumvent the requirement for open-bid contracts, and procedures and actions regarding debarment of vendors;

4. Any private business ventures in which a Los Angeles City ("City") official had a financial interest, including but not limited to AVENTADOR UTILITY SOLUTIONS, LLC, CYBERGYM, and ARDENT UTILITY SOLUTIONS, LLC;

5. Any lawsuit where the City of Los Angeles ("the City") is a party to the lawsuit and appears to have a

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

legal, representation, and/or financial interest in both sides of the lawsuit;

6. Financial payments, gifts, services, or other benefits given or offered to officials at LADWP or the City Attorney's Office or their staff or family members, or solicited by officials at LADWP or the City Attorney's Office or their staff or family members;

7. Records, data, or other information required by or submitted to the Federal Energy Regulatory Commission ("FERC") or the North American Electric Reliability Corporation, Critical Infrastructure Protection ("NERC-CIP");

8. Cybersecurity vulnerabilities within the Los Angeles Department of Water and Power, including the City's power grid, water supply, and other critical infrastructure; and

iv. All records and information described above in Section II.13.b.

IV. PROVIDER PROCEDURES

15. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. The PROVIDER shall send such information to:

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

16. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

17. IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 2705(b), that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A-3, of the existence of the warrant, until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date the PROVIDER complies with this warrant or such later date as may be set by the Court upon application for an extension by the United States. Upon expiration of this order, at least ten business days prior to disclosing the existence of the warrant, the PROVIDER shall notify the agent identified in paragraph 15 above of its intent to so notify.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AO 93 (Rev. 11/13) Search and Seizure Warrant (USAO CDCA Rev. 04/17)

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* My Passport WD hard-drive, serial number WXQ1A6803KA0; and Apple MacBook Pro with serial number C02SN0ZRG8WN and model number A1398	)	Case No. 19-1595

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-1

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B-1

Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for____days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 4/18/19 at 4:53 p.m.

City and state: Los Angeles, CA

AUSA: Diana Kwok (x6529)

Judge's signature

Printed name and title

JACQUELINE CHOOLJIAN
UNITED STATES MAGISTRATE JUDGE

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-1

PROPERTY TO BE SEARCHED

a) A My Passport WD hard drive, serial number WXQ1A6803KA0, which contains the Cellebrite extraction of a cellular telephone, [redacted] used by DAVID WRIGHT;

b) An Apple MacBook Pro with serial number C02SN0ZRG8WN and model number A1398.

ATTACHMENT B-1

A. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 666 (Bribery and Kickbacks Concerning Federal Funds), 1341 (Mail Fraud), 1343 (Wire Fraud), and 1346 (Deprivation of Honest Services), 1505 (Obstruction of Federal Proceeding), 1510 (Obstruction of Justice), 1951 (Extortion) and 1956 (Money Laundering) (collectively the "Target Offenses"), namely:

a. Evidence of who accessed or used the digital device on or after February 1, 2015, including records about their identities and whereabouts.

b. Communications or agreements on or after February 1, 2015, referencing: PAUL PARADIS, GINA TUFARO, MEL LEVINE, CYNTHIA MCCLAIN-HILL, STEPHEN KWOK, DAVID ALEXANDER, JACK LANDSKRONER, PAUL KIESEL, JAMES CLARK, THOMAS PETERS, WILLIAM FUNDERBURK, PAUL BENDER, AVENTADOR UTILITY SOLUTIONS, LLC, ARDENT CYBER SOLUTIONS, LLC, and CYBERGYM (the "Subjects").

c. Records, documents, programs, applications, or materials from on or after February 1, 2015, referencing:

i. DAVID WRIGHT's bank accounts, credit card accounts, other financial accounts, and wire transfer records;

ii. DAVID WRIGHT's calendar or date book, including calendars or date books stored on digital devices;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

iii. Los Angeles Department of Water and Power contracts, proposed contracts, and contracting processes, including but not limited to any manipulations of contracting processes, the use of other entities to circumvent the requirement for open-bid contracts, and procedures and actions regarding debarment of vendors;

iv. Any private business ventures in which a Los Angeles City ("City") official had a financial interest, including but not limited to AVENTADOR UTILITY SOLUTIONS, LLC, CYBERGYM, and ARDENT UTILITY SOLUTIONS, LLC;

v. Any lawsuit where the City of Los Angeles ("the City") was a party to the lawsuit and appears to have had a legal, representational, and/or financial interest in both sides of the lawsuit.

vi. Financial payments, gifts, services, or other benefits given or offered to officials at LADWP or the City Attorney's Office or their staff or family members, or solicited by officials at LADWP or the City Attorney's Office or their staff or family members;

vii. Records, data, or other information required by or submitted to the Federal Energy Regulatory Commission ("FERC") or the North American Electric Reliability Corporation, Critical Infrastructure Protection ("NERC-CIP"); and

viii. Cybersecurity vulnerabilities within the LADWP, including the City's power grid, water supply, and other critical infrastructure.

d. Any SUBJECT DEVICE which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Target Offenses, and forensic copies thereof.

e. With respect to any SUBJECT DEVICE used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations;

ii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

iii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications or other text or written communications sent to or received from any digital device;

iv. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents,

browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

v. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

vi. evidence of the attachment of other devices;

vii. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

viii. evidence of the times the device was used;

ix. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

x. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

xi. records of or information about Internet Protocol addresses used by the device;

xii. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

B. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

6. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications, work product, or other potentially privileged communications:

7. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will review only digital device data which has been released by the Privilege Review Team.

8. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

9. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will

conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

10. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

11. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

12. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

13. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered,

including how it was immediately apparent contraband or evidence of a crime.

14. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

15. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

16. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

17. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

18. After the completion of the search of the digital devices, the government shall not access digital data falling

outside the scope of the items to be seized absent further order of the Court.

19. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary

to access the digital device or data stored on the digital device.

20. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

C. SEARCH PROCEDURE FOR DIGITAL DEVICES

21. In searching the SUBJECT DEVICES or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any SUBJECT DEVICE capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each SUBJECT DEVICE where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICE(S) as soon as is practicable but not to exceed 180 days from the date of issuance of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each SUBJECT DEVICE capable of containing any of the items to be seized to the search protocols to determine whether the SUBJECT DEVICE and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques [, including to search for known images of child pornography.]

e. If the search team, while searching a SUBJECT DEVICE, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that SUBJECT DEVICE pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence

of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

f. If the search determines that a SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the SUBJECT DEVICE and delete or destroy all forensic copies thereof.

g. If the search determines that a SUBJECT DEVICE does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a SUBJECT DEVICE if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the SUBJECT DEVICE(S), the government shall not access digital data falling

outside the scope of the items to be seized absent further order of the Court.

k. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of: Information associated with accounts identified as [redacted]com and [redacted] that is within the possession, custody, or control of Oath, Inc. dba America Online ("AOL")	)	Case No. 19-1597

WARRANT PURSUANT TO 18 U.S.C. § 2703

To: Any Authorized Law Enforcement Officer

An application by a federal law enforcement officer requests the production and search of the following data:

See Attachment A-2

The data to be produced and searched, described above, are believed to contain the following:

See Attachment B-2

I find that the affidavit, or any recorded testimony, establishes probable cause to produce and search the data described in Attachment A-2, and to seize the data described in Attachment B-2. Such affidavit is incorporated herein by reference.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE HEREBY COMMANDED to serve this warrant on Oath, Inc. dba America Online ("AOL") in the daytime, between the hours of 6:00 a.m. and 10:00 p.m., within 14 days from the date of its issuance.

OATH, INC. DBA AMERICA ONLINE ("AOL") IS HEREBY COMMANDED to produce the information described in Attachment A-2 within 10 calendar days of the date of service of this order. **OATH, INC. DBA AMERICA ONLINE ("AOL") IS FURTHER COMMANDED** to comply with the further orders set forth in Attachment B-2, and, pursuant to 18 U.S.C. § 2705(b), shall not notify any person, including the subscriber(s) of the account/s identified in Attachment A-2, of the existence of this warrant.

The officer executing this warrant, or an officer present during the execution, shall prepare an inventory as required by law, and shall promptly return this warrant and the inventory to the United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE FURTHER COMMANDED to perform the search of the data provided by Oath, Inc. dba America Online ("AOL") pursuant to the procedures set forth in Attachment B-2.

Date and time issued: 4/18/19 at 7:51 p.m.

Judge's signature

City and State: Los Angeles, CA

The Hon. Jacqueline Chooljian, U.S. Magistrate Judge

Printed name and title

AUSA Diana Kwok: 213-894-6529

Return	
Case No:	*Date and time warrant served on provider:*
Inventory made in the presence of:	
Inventory of data seized: [Please provide a description of the information produced.]	
Certification	
I declare under penalty of perjury that I am an officer involved in the execution of this warrant, and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office. Date: _____	_____ *Executing officer's signature* _____ *Printed name and title*

ATTACHMENT A-2

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the account identified as [redacted] and [redacted] and being used by DAVID WRIGHT, that is within the possession, custody, or control of Oath, Inc. dba America Online ("AOL"), a company that accepts service of legal process at its headquarters located at a provider of electronic communication and remote computing services, headquartered at 22000 AOL Way, Dulles, Virginia 20166, regardless of where such information is stored, held, or maintained.

ATTACHMENT B-2

EMAIL ITEMS TO BE SEIZED

I. SEARCH PROCEDURE INCLUDING PRIVILEGE REVIEW PROCEDURE

1. The search warrant will be presented to personnel of Oath, Inc. dba America Online ("AOL") (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide the Section II information in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.13.a. below), law enforcement agents and/or other individuals assisting law enforcement agents who are not participating in the investigation of the case and who are assigned as the "Privilege Review Team" will review the content records, according to the procedures set forth herein, to determine whether or not any of the content records appears to contain or refer to communications between an attorney, or to contain the work product of an attorney, or between a spouse and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

any person ("potentially privileged information"). The "Search Team" (law enforcement personnel conducting the investigation and search and other individuals assisting law enforcement personnel in the search) will review only content records which have been released by the Privilege Review Team. With respect to the non-content information produced by the PROVIDER (see Section II.13.b. below), no privilege review need be performed and the Search Team may review immediately.

5. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for in the content records, to include specific words like names of any identified attorneys or law firms and names of any identified spouses] or their email addresses, and generic words such as "privileged" and "work product". The Privilege Review Team will conduct an initial review of all of the content records by using the privilege key words, and by using search protocols specifically chosen to identify content records containing potentially privileged information. Content records that are not identified by this initial review as potentially privileged may be given to the Search Team.

6. Content records that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Content records determined by this review not to be potentially privileged may be given to the Search Team. Content records determined by this review to be potentially privileged will be given to the United States Attorney's Office

for further review by a Privilege Review Team Assistant United States Attorney ("PRTAUSA"). Content records identified by the PRTAUSA after review as not potentially privileged may be given to the Search Team. If, after review, the PRTAUSA determines it to be appropriate, the PRTAUSA may apply to the court for a finding with respect to particular content records that no privilege, or an exception to the privilege, applies. Content records that are the subject of such a finding may be given to the Search Team. Content records identified by the PRTAUSA after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

7. The Search Team will search only the content records that the Privilege Review Team provides to the Search Team at any step listed above in order to locate, extract and seize content records that are within the scope of the search warrant (see Section III below). The Search Team does not have to wait until the entire privilege review is concluded to begin its review for content records within the scope of the search warrant. The Privilege Review Team may also conduct the search for content records within the scope of the search warrant if that is more efficient. The search may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

8. If, while reviewing content records or non-content information, either the Privilege Review Team or the Search Team

encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

9. The Privilege Review Team and the Search Team will complete the search of non-content information and both stages of the search of the content records discussed herein as soon as is practicable but not to exceed 180 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the records beyond this 180-day period without first obtaining an extension of time order from the Court.

10. Once the Privilege Review Team and the Search Team have completed their review of the non-content information and the content records and the Search Team has created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the Search Team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, neither the Privilege Review Team nor the Search Team will access the data from the sealed original production which fell outside the scope of the items to be seized or was determined to be privileged absent further order of the Court.

11. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

12. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDERS

13. To the extent that the information described in Attachment A-2, is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each **TARGET ACCOUNT** listed in Attachment A-2:

a. All contents of all wire and electronic communications associated with [redacted] and [redacted] limited to that which occurred on or after February 1, 2015, [1] including:

i. All e-mails, communications, or messages of any kind associated with the **TARGET ACCOUNTS**, including stored or preserved copies of messages sent to and from the account,

[1] To the extent it is not reasonably feasible for the PROVIDER to restrict any categories of records based on this date restriction (for example, because a date filter is not available for such data), the PROVIDER shall disclose those records in its possession at the time the warrant is served upon it.

deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information associated with each e-mail or message, and any related documents or attachments.

ii. All records (including content records and the stored application data) pertaining to any Oath, Inc. service associated with the **TARGET ACCOUNTS;**

iii. All records (including content records and the stored application data) associated with the **TARGET ACCOUNTS** pertaining to Location History, including custom maps, changes and edits to public places, starred places, private labels of locations, and saved locations.

iv. All records or other information stored by subscriber(s) of the **TARGET ACCOUNTS**, including address books, contact and buddy lists, calendar data, pictures or photos, videos, notes, texts, links, user profiles, account settings, access logs, and files.

v. All records pertaining to communications between the PROVIDER and any person regarding the **TARGET ACCOUNTS**, including contacts with support services and records of actions taken.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), any alternate names, other account names or e-mail addresses associated with the account, linked

accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, and including any changes made to any subscriber information or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred, for the **TARGET ACCOUNTS**.

ii. All user connection logs and transactional information of all activity relating to the **TARGET ACCOUNTS** described above, including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations, , and including specifically the specific product name or service to which the connection was made.

iii. Any information showing the location of the user of a **TARGET ACCOUNTS**, including while sending or receiving a message using a **TARGET ACCOUNTS** or accessing or logged into a **TARGET ACCOUNTS**.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

14. For each **TARGET ACCOUNT** listed in Attachment A-2, the search team may seize:

a. All information described above that constitutes evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 666 (Bribery and Kickbacks Concerning Federal Funds), ~~1341~~ (wire fraud) 1343, and 1346 (Deprivation of Honest Services), 1505 (obstruction of federal proceeding), 1510 (Obstruction of Justice), 1951 (Extortion) and 1956 (Money Laundering) (the "Target Offenses"), involving DAVID WRIGHT, PAUL PARADIS, GINA TUFARO, MEL LEVINE, CYNTHIA MCCLAIN-HILL, STEPHEN KWOK, DAVID ALEXANDER, JACK LANDSKRONER, PAUL KIESEL, JAMES CLARK, THOMAS PETERS, WILLIAM FUNDERBURK, PAUL BENDER, AVENTADOR UTILITY SOLUTIONS, LLC, ARDENT CYBER SOLUTIONS, LLC, and CYBERGYM (the "Subjects") namely:

i. Information relating to who created, accessed, or used the **TARGET ACCOUNTS**, including records about their identities and whereabouts.

ii. Communications or agreements referencing PAUL PARADIS, GINA TUFARO, MEL LEVINE, CYNTHIA MCCLAIN-HILL, STEPHEN KWOK, DAVID ALEXANDER, JACK LANDSKRONER, PAUL KIESEL, JAMES CLARK, THOMAS PETERS, WILLIAM FUNDERBURK, PAUL BENDER, AVENTADOR UTILITY SOLUTIONS, LLC, ARDENT CYBER SOLUTIONS, LLC, and CYBERGYM;

iii. Records, documents, programs, applications, or materials referencing:

1. DAVID WRIGHT's bank accounts, credit card accounts, other financial accounts, and wire transfer records;

2. DAVID WRIGHT's calendar or date book, including calendars or date books stored on digital devices;

3. Los Angeles Department of Water and Power contracts, proposed contracts, and contracting processes, including but not limited to any manipulations of contracting processes, the use of other entities to circumvent the requirement for open-bid contracts, and procedures and actions regarding debarment of vendors;

4. Any private business ventures in which a Los Angeles City ("City") official had a financial interest, including but not limited to AVENTADOR UTILITY SOLUTIONS, LLC, CYBERGYM, and ARDENT UTILITY SOLUTIONS, LLC;

5. Any lawsuit where the City of Los Angeles ("the City") is a party to the lawsuit and appears to have a legal, representation, and/or financial interest in both sides of the lawsuit;

6. Financial payments, gifts, services, or other benefits given or offered to officials at LADWP or the City Attorney's Office or their staff or family members, or solicited by officials at LADWP or the City Attorney's Office or their staff or family members;

7. Records, data, or other information required by or submitted to the Federal Energy Regulatory Commission ("FERC") or the North American Electric Reliability Corporation, Critical Infrastructure Protection ("NERC-CIP");

8. Cybersecurity vulnerabilities within the Los Angeles Department of Water and Power, including the City's power grid, water supply, and other critical infrastructure; and

iv. All records and information described above in Section II.13.b.

IV. PROVIDER PROCEDURES

15. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. The PROVIDER shall send such information to:

[redacted]

16. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

17. IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 2705(b), that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A-2, of the existence of the warrant, until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date the PROVIDER complies with this warrant or such later date as may be set by the Court upon application for an extension by the United States. Upon expiration of this order, at least ten business days prior to disclosing the existence of the warrant, the PROVIDER shall notify the agent identified in paragraph 15 above of its intent to so notify.

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of: Information associated with accounts identified as [redacted] and [redacted] that is within the possession, custody, or control of Apple, Inc.

Case No. 19-1598

WARRANT PURSUANT TO 18 U.S.C. § 2703

To: Any Authorized Law Enforcement Officer

An application by a federal law enforcement officer requests the production and search of the following data:

See Attachment A-3

The data to be produced and searched, described above, are believed to contain the following:

See Attachment B-3

I find that the affidavit, or any recorded testimony, establishes probable cause to produce and search the data described in Attachment A-3, and to seize the data described in Attachment B-3. Such affidavit is incorporated herein by reference.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE HEREBY COMMANDED to serve this warrant on Apple, Inc. in the daytime, between the hours of 6:00 a.m. and 10:00 p.m., within 14 days from the date of its issuance.

APPLE, INC. IS HEREBY COMMANDED to produce the information described in Attachment A-3 within 10 calendar days of the date of service of this order. **APPLE, INC. IS FURTHER COMMANDED** to comply with the further orders set forth in Attachment B-3, and, pursuant to 18 U.S.C. § 2705(b), shall not notify any person, including the subscriber(s) of the account/s identified in Attachment A-3, of the existence of this warrant.

The officer executing this warrant, or an officer present during the execution, shall prepare an inventory as required by law, and shall promptly return this warrant and the inventory to the United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE FURTHER COMMANDED to perform the search of the data provided by Apple, Inc. pursuant to the procedures set forth in Attachment B-3.

Date and time issued: 4/18/19 at 7:34 p.m.

Judge's signature

City and State: Los Angeles, CA

The Hon. Jacqueline Chooljian, U.S. Magistrate Judge

Printed name and title

AUSA Diana Kwok: 213-894-6529

Return	
Case No:	*Date and time warrant served on provider:*
Inventory made in the presence of:	
Inventory of data seized: [Please provide a description of the information produced.]	

Certification
I declare under penalty of perjury that I am an officer involved in the execution of this warrant, and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office. Date: _____ _____ *Executing officer's signature* _____ *Printed name and title*

ATTACHMENT A-3

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the accounts identified as [redacted] and [redacted] and being used by DAVID WRIGHT, that is within the possession, custody, or control of Apple, Inc., a provider of electronic communication and remote computing services that accepts service of legal process at 1 Infinite Loop, M/S 36-SU, Cupertino, California, 95014, regardless of where such information is stored, held, or maintained.

ATTACHMENT B-3

EMAIL ITEMS TO BE SEIZED

I. SEARCH PROCEDURE INCLUDING PRIVILEGE REVIEW PROCEDURE

1. The search warrant will be presented to personnel of Apple Inc. (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide the Section II information in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.13.a. below), law enforcement agents and/or other individuals assisting law enforcement agents who are not participating in the investigation of the case and who are assigned as the "Privilege Review Team" will review the content records, according to the procedures set forth herein, to determine whether or not any of the content records appears to contain or refer to communications between an attorney, or to contain the work product of an attorney, or between a spouse and any person ("potentially privileged information"). The "Search

Team" (law enforcement personnel conducting the investigation and search and other individuals assisting law enforcement personnel in the search) will review only content records which have been released by the Privilege Review Team. With respect to the non-content information produced by the PROVIDER (see Section II.13.b. below), no privilege review need be performed and the Search Team may review immediately.

5. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for in the content records, to include specific words like names of any identified attorneys or law firms and names of any identified spouses] or their email addresses, and generic words such as "privileged" and "work product". The Privilege Review Team will conduct an initial review of all of the content records by using the privilege key words, and by using search protocols specifically chosen to identify content records containing potentially privileged information. Content records that are not identified by this initial review as potentially privileged may be given to the Search Team.

6. Content records that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Content records determined by this review not to be potentially privileged may be given to the Search Team. Content records determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a Privilege Review Team Assistant United

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

States Attorney ("PRTAUSA"). Content records identified by the PRTAUSA after review as not potentially privileged may be given to the Search Team. If, after review, the PRTAUSA determines it to be appropriate, the PRTAUSA may apply to the court for a finding with respect to particular content records that no privilege, or an exception to the privilege, applies. Content records that are the subject of such a finding may be given to the Search Team. Content records identified by the PRTAUSA after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

7. The Search Team will search only the content records that the Privilege Review Team provides to the Search Team at any step listed above in order to locate, extract and seize content records that are within the scope of the search warrant (see Section III below). The Search Team does not have to wait until the entire privilege review is concluded to begin its review for content records within the scope of the search warrant. The Privilege Review Team may also conduct the search for content records within the scope of the search warrant if that is more efficient. The search may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

8. If, while reviewing content records or non-content information, either the Privilege Review Team or the Search Team encounters immediately apparent contraband or other evidence of

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a crime outside the scope of the items to be seized, the team shall immediately discontinue its search pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

9. The Privilege Review Team and the Search Team will complete the search of non-content information and both stages of the search of the content records discussed herein as soon as is practicable but not to exceed 180 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the records beyond this 180-day period without first obtaining an extension of time order from the Court.

10. Once the Privilege Review Team and the Search Team have completed their review of the non-content information and the content records and the Search Team has created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the Search Team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, neither the Privilege Review Team nor the Search Team will access the data from the sealed original production which fell outside the scope of the items to be seized or was determined to be privileged absent further order of the Court.

11. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

12. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDERS

13. To the extent that the information described in Attachment A-3, is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each **TARGET ACCOUNT** listed in Attachment A-3:

a. All contents of all wire and electronic communications associated with [redacted] and [redacted], limited to that which occurred on or after February 1, 2015, [1] including:

i. All e-mails, communications, or messages of any kind associated with the **TARGET ACCOUNTS**, including stored or preserved copies of messages sent to and from the account, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information

[1] To the extent it is not reasonably feasible for the PROVIDER to restrict any categories of records based on this date restriction (for example, because a date filter is not available for such data), the PROVIDER shall disclose those records in its possession at the time the warrant is served upon it.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

associated with each e-mail or message, and any related documents or attachments.

ii. All records (including content records and the stored application data) associated with the **TARGET ACCOUNT** pertaining to Location History and maps, including custom maps, changes and edits to public places, starred places, private labels of locations, and saved locations.

iii. All records or other information stored by subscriber(s) of the **TARGET ACCOUNT**, including address books, contact and buddy lists, calendar data, pictures or photos, videos, notes, texts, links, user profiles, account settings, access logs, and files.

iv. All records pertaining to communications between the PROVIDER and any person regarding the **TARGET ACCOUNT**, including contacts with support services and records of actions taken.

v. All stored files and other records stored on iCloud for each **TARGET ACCOUNT**, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks.

vi. All files, keys, or other information necessary to decrypt any data produced in an encrypted form,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), any alternate names, other account names or e-mail addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, and including any changes made to any subscriber information or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred, for the **TARGET ACCOUNT**.

ii. All activity, connection, and transactional logs for all activity relating to each **TARGET ACCOUNT** described above in Section II.13.a. (all log files, dates, times, durations, data transfer volumes, methods of connection, authentication logs, IP addresses, ports, routing information, dial-ups, and locations), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

(including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers).

i. Any information showing the location of the user of a **TARGET ACCOUNT**, including while sending or receiving a message using a **TARGET ACCOUNT** or accessing or logged into a **TARGET ACCOUNT**.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

14. For each **TARGET ACCOUNT** listed in Attachment A-2, the search team may seize:

a. All information described above that constitutes evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 666 (Bribery and Kickbacks Concerning Federal Funds), 1341, 1343, and 1346 (Deprivation of Honest Services), 1505, 1510 (Obstruction of Justice), 1951 (Extortion) and 1956 (Money Laundering) (the "Target Offenses"), involving DAVID WRIGHT, PAUL PARADIS, GINA TUFARO, MEL LEVINE, CYNTHIA MCCLAIN-HILL, STEPHEN KWOK, DAVID ALEXANDER, JACK LANDSKRONER, PAUL KIESEL, JAMES CLARK, THOMAS PETERS, WILLIAM FUNDERBURK, PAUL BENDER, AVENTADOR UTILITY SOLUTIONS, LLC, ARDENT CYBER SOLUTIONS, LLC, and CYBERGYM (the "Subjects") namely:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

i. Information relating to who created, accessed, or used the **TARGET ACCOUNTS**, including records about their identities and whereabouts.

ii. Communications or agreements referencing PAUL PARADIS, GINA TUFARO, MEL LEVINE, CYNTHIA MCCLAIN-HILL, STEPHEN KWOK, DAVID ALEXANDER, JACK LANDSKRONER, PAUL KIESEL, JAMES CLARK, THOMAS PETERS, WILLIAM FUNDERBURK, PAUL BENDER, AVENTADOR UTILITY SOLUTIONS, LLC, ARDENT CYBER SOLUTIONS, LLC, and CYBERGYM

iii. Records, documents, programs, applications, or materials referencing:

1. DAVID WRIGHT's bank accounts, credit card accounts, other financial accounts, and wire transfer records;

2. DAVID WRIGHT's calendar or date book, including calendars or date books stored on digital devices;

3. Los Angeles Department of Water and Power contracts, proposed contracts, and contracting processes, including but not limited to any manipulations of contracting processes, the use of other entities to circumvent the requirement for open-bid contracts, and procedures and actions regarding debarment of vendors;

4. Any private business ventures in which a Los Angeles City ("City") official had a financial interest, including but not limited to AVENTADOR UTILITY SOLUTIONS, LLC, CYBERGYM, and ARDENT UTILITY SOLUTIONS, LLC;

5. Any lawsuit where the City of Los Angeles ("the City") is a party to the lawsuit and appears to have a

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

legal, representation, and/or financial interest in both sides of the lawsuit;

6. Financial payments, gifts, services, or other benefits given or offered to officials at LADWP or the City Attorney's Office or their staff or family members, or solicited by officials at LADWP or the City Attorney's Office or their staff or family members;

7. Records, data, or other information required by or submitted to the Federal Energy Regulatory Commission ("FERC") or the North American Electric Reliability Corporation, Critical Infrastructure Protection ("NERC-CIP");

8. Cybersecurity vulnerabilities within the Los Angeles Department of Water and Power, including the City's power grid, water supply, and other critical infrastructure; and

iv. All records and information described above in Section II.13.b.

IV. PROVIDER PROCEDURES

15. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. The PROVIDER shall send such information to:

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

16. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

17. IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 2705(b), that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A-3, of the existence of the warrant, until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date the PROVIDER complies with this warrant or such later date as may be set by the Court upon application for an extension by the United States. Upon expiration of this order, at least ten business days prior to disclosing the existence of the warrant, the PROVIDER shall notify the agent identified in paragraph 15 above of its intent to so notify.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Central District of California

COPY

FILED
CLERK, U.S. DISTRICT COURT
JUN - 4 2019
CENTRAL DISTRICT OF CALIFORNIA
BY

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	Case No. 2:19-MJ-02347
111 N. Hope Street #1603, Los Angeles, California	

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC § 371	Conspiracy
18 USC § 666	Federal Program Bribery and Kickbacks
18 USC § 1341	Mail Fraud
18 USC § 1343	Wire Fraud
18 USC § 1346	Deprivation of Honest Services

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of_____days (*give exact ending date if more than 30 days*:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/
Applicant's signature

Printed name and title

Sworn to before me and signed in my presence.

Date: 6/4/19

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

PATRICK J. WALSH
Printed name and title

AUSA: Melissa Mills x0627

ATTACHMENT A-4

PROPERTY TO BE SEARCHED

The premises to be searched is the 15th Floor of the John Ferraro Building located at 111 N. Hope Street, Los Angeles, California, which is DAVID WRIGHT's employment ("**WRIGHT's OFFICE**"). Specifically, **WRIGHT's OFFICE** includes the office suite and conference room known as Room 1550. **WRIGHT's OFFICE** building is pictured below:

ATTACHMENT B-4

I. ITEMS TO BE SEIZED

1. Evidence of the criminal schemes and evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 666 (Bribery and Kickbacks Concerning Federal Funds), 1341 (Mail Fraud), 1343 (Wire Fraud), and 1346 (Deprivation of Honest Services), 1505 (Obstruction of Federal Proceeding), 1510 (Obstruction of Justice), 1951 (Extortion), and 1956 (Money Laundering) (collectively, the "Target Offenses"), occurring after February 1, 2015, namely:

a. Communications or agreements referencing: the Subjects identified in Section 3 of the Affidavit (the "Subjects");

b. Records, documents, programs, applications, or materials referencing:

xxv. DAVID WRIGHT's bank accounts, credit card accounts, other financial accounts, and wire transfer records;

xxvi. DAVID WRIGHT's calendar or date book, including calendars or date books stored on digital devices;

xxvii. Los Angeles Department of Water and Power contracts, proposed contracts, and contracting processes, including but not limited to any manipulations of contracting processes, the use of other entities to circumvent the requirement for open-bid contracts, and procedures and actions regarding debarment of vendors;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

xxviii. Any private business ventures in which a City official had a financial interest, including but not limited to AVENTADOR UTILITY SOLUTIONS, LLC, CYBERGYM, and ARDENT UTILITY SOLUTIONS, LLC;

xxix. Any lawsuit where the City was a party to the lawsuit and appears to have had a legal, representational, and/or financial interest in both sides of the lawsuit.

xxx. Financial payments, gifts, services, or other benefits given or offered to officials at LADWP or the City Attorney's Office or their staff or family members, or solicited by officials at LADWP or the City Attorney's Office or their staff or family members;

xxxi. Records, data, or other information required by or submitted to the Federal Energy Regulatory Commission ("FERC") or the North American Electric Reliability Corporation, Critical Infrastructure Protection ("NERC-CIP"); and

c. Cybersecurity vulnerabilities within the LADWP, including the City's power grid, water supply, and other critical infrastructure.

2. Law enforcement personnel are authorized to seize the cellular telephones with telephone numbers [redacted] ("**WRIGHT's PHONE**") and [redacted] ("**WRIGHT's BURNER PHONE**"), and any cellular phone in the possession of DAVID WRIGHT ("**TAREGT PHONES**" or the "digital devices").

3. During the execution of this search warrant, law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of DAVID WRIGHT onto the Touch ID sensor of the **TARGET PHONES**, or hold the **TARGET PHONES** in front of WRIGHT's face to activate the Face ID sensor, in order to gain access to the contents of any such device as authorized by this warrant. The government may not use more force than is reasonable to obtain this access.

4. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the Electronically Stored Information ("ESI") and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review and seize the ESI contained on the **TARGET PHONES** for evidence of the criminal schemes and evidence, contraband, fruits, and instrumentalities of Target Offenses, occurring after February 1, 2015, namely:

a. Items (a) through (c) above.

b. Evidence of who accessed or used the digital device, including records about their identities and whereabouts.

xxxii.

g. Any **TARGET PHONES** which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Target Offenses, and forensic copies thereof.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000137
Page 137 of 1425

c. With respect to any **TARGET PHONES** used to facilitate the Target Offenses or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations;

ii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

iii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications or other text or written communications sent to or received from any digital device;

iv. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

v. evidence of the presence or absence of software that would allow others to control the device, such as

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

vi. evidence of the attachment of other devices;

vii. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

viii. evidence of the times the device was used;

ix. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

x. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

xi. records of or information about Internet Protocol addresses used by the device;

xii. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

5. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000139
Page 139 of 1425

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

6. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications, work product, or other potentially privileged communications:

7. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will review only digital device data which has been released by the Privilege Review Team.

8. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

9. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000140
Page 140 of 1425

potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

10. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

11. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data

that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

12. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

13. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

14. If the search determines that a digital device does not contain any data falling within the list of items to be

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000142
Page 142 of 1425

seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

15. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

16. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

17. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

18. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

19. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

20. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

III. SEARCH PROCEDURE FOR DIGITAL DEVICES

21. In searching the **TARGET PHONES** or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any **TARGET PHONES** capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each **TARGET PHONES** where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the **TARGET PHONES** as soon as is practicable but not to exceed 180 days from the date of issuance of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each **TARGET PHONES** capable of containing any of the items to be seized to the search protocols to determine whether the **TARGET PHONES** and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques [, including to search for known images of child pornography.]

e. If the search team, while searching a **TARGET PHONES**, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that **TARGET PHONES** pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

f. If the search determines that a **TARGET PHONES** does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

the **TARGET PHONES** and delete or destroy all forensic copies thereof.

g. If the search determines that a **TARGET PHONES** does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the **TARGET PHONES** is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a **TARGET PHONES** if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the **TARGET PHONES**(S), the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

k. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

do not apply to any search of digital devices pursuant to any other court order.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Table of Contents

I. INTRODUCTION.....1

II. PURPOSE OF AFFIDAVIT.....1

III. BACKGROUND ON SUBJECTS.....4

IV. SUMMARY OF INVESTIGATION.....10

1. The Criminal Schemes.....10

V. STATEMENT OF PROBABLE CAUSE.....11

A. The Underlying Civil Litigation.....12

1. Collusive Litigation Practices between the Los Angeles City Attorney's Office, PARADIS, PAUL KIESEL, and JACK LANDSKRONER.....12

2. Hush Money to Conceal Collusive Litigation Practices.....18

B. No-Bid LADWP Contracts Awarded to Attorney PARADIS and Quid Pro Quo Established with City Official (WRIGHT).....19

1. 2015 and 2016 No-Bid Contract for $6,000,000.....19

2. 2017 No-Bid Contract for $30,000,000.....20

3. WRIGHT Advocated For and Praised AVENTADOR in an Effort to Gain Support for Future Contracts.....25

C. Alleged Falsification of Regulatory Paperwork by LADWP Employees.....29

1. Underreporting and Failure to Report Cybersecurity Issues.....29

D. Alleged Circumvention of LADWP's Contracting Process.....31

1. WRIGHT and LEVINE Discussed the Necessity of Cyber Services for LADWP.....31

2. Manipulation of the SCCPA Bidding Process..33

E. Alleged Conspiracy and Falsification of Records by Attorney Members of the LADWP Board, LADWP Attorneys, and Members of the City Attorney's Office.....36

1. The City's Debarment of PwC.....36

F. Obstruction of Justice by WRIGHT.....40

1. WRIGHT's Request That PARADIS Destroy Evidence in His Email Accounts and on His Laptop and Cell Phone.....40

2. **WRIGHT** Maintains Evidence of the Criminal Schemes in **WRIGHT's PALM SPRINGS RESIDENCE**.45

3. PARADIS Continues to Meet with WRIGHT to Discuss the Criminal Schemes and Target Offenses.....46

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES.....51

VII. CONCLUSION.....54

AFFIDAVIT

I, Andrew Civetti, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since September 2015. I am currently assigned to a Public Corruption Squad, where I specialize in the investigation of corrupt public officials, including bribery, fraud against the government, extortion, and money laundering. In addition, I have received training in the investigation of public corruption and other white collar crimes.

2. I am currently one of the agents assigned to an investigation of alleged corrupt activities within the City of Los Angeles (the "City"). I am aware that the City receives in excess of $10,000 annually in federal funds through various programs.

II. PURPOSE OF AFFIDAVIT

3. I make this affidavit in support of applications for four search warrants, described in more detail below, for:

a. the search for cellular telephones located in (1) **DAVID WRIGHT's PALM SPRINGS RESIDENCE** or alternatively on the (2) person of WRIGHT;

b. the search of (3) **DAVID WRIGHT's RIVERSIDE RESIDENCE** and (4) **DAVID WRIGHT's OFFICE.**

A. Cellular Telephone Search Warrants

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

4. This affidavit is made in support of applications to search for cellular telephones located in the following residences, or alternatively on the persons of WRIGHT (the "**TARGET PHONES**"):

a. [redacted], Palm Springs, California described in more detail in Attachment A-1 ("**WRIGHT's PALM SPRINGS RESIDENCE**");

b. DAVID WRIGHT, described in more detail in Attachment A-2;

5. In connection with the investigation into this matter, the requested search warrants seek authorization to search **WRIGHT's PALM SPRINGS RESIDENCE**, or alternatively the person of WRIGHT, for the **TARGET PHONES** described in Attachments B-1 and B-2, and any data on the **TARGET PHONES** that constitutes evidence of the criminal schemes identified below and evidence or fruits of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1341 (Mail Fraud); 1343 (Wire Fraud); and 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering) (collectively, the "Target Offenses"), and any **TARGET PHONE** that is itself an instrumentality of the criminal schemes and Target Offenses, as also set forth in Attachment B-1 and B-2. Attachments A-1 and A-2 and B-1 and B-2 incorporated herein by reference.

B. Premises Search Warrants

6. This affidavit is made in support of applications for two warrants to search the following premises for evidence related to the criminal schemes and Target Offenses:

a. [redacted], Riverside, California, described in more detail in Attachment A-3 ("**WRIGHT's RIVERSIDE RESIDENCE**");

b. 111 N. Hope Street #1603, Los Angeles, California, described in more detail in Attachment A-4("**WRIGHT's OFFICE**").

7. In connection with the investigation into this matter, the requested search warrants seek authorization to search **WRIGHT's RIVERSIDE RESIDENCE** and **WRIGHT's OFFICE**, for the items to be seized described in Attachments B-3 and B-4, respectively, that constitute evidence of the criminal schemes and evidence or fruits of violations of the Target Offenses. Attachments A-3 and A-4, and B-3 and B-4 are incorporated herein by reference.

8. The facts set forth in this affidavit are based upon my personal observations, my training and experience, information obtained from other agents and witnesses, consensually recorded conversations, and information obtained from the prior related search warrants, as detailed further below. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all

conversations and statements described in this affidavit are related in substance and in part only.

III. BACKGROUND ON SUBJECTS

9. Based on my knowledge of the investigation, below is general background on certain subjects. Although this investigation currently has other subjects, this affidavit focuses on the subjects most relevant to the requested search warrants.

10. DAVID WRIGHT is the General Manager of the Los Angeles Department of Water and Power ("LADWP"). WRIGHT originally joined LADWP in February 2015 as the Senior Assistant General Manager and then became Chief Operating Officer before being appointed as General Manager in September 2016. According to LADWP's website, WRIGHT spearheaded major LADWP initiatives to restore customer trust in the utility, and to create a clean energy future and a sustainable water supply for Los Angeles.

a. Based on my review of seized communications[1] and recorded conversations, I know WRIGHT to use the cellular

[1] On April 18, 2019, the Honorable Magistrate Judge Jacqueline Chooljian authorized a search warrant for **WRIGHT's PHONE**, WRIGHT's laptop, two of WRIGHT's email addresses, and two of WRIGHT's Apple iCloud accounts (the "April 2019 search warrants"). The April 2019 search warrants and their supporting affidavit, are incorporated herein by reference, and a copy can be made available for the Court. To the best of my knowledge, WRIGHT is not aware that the FBI executed the April 2019 search warrants. The context surrounding the execution of the April 2019 search warrants is discussed in detail below. I know that WRIGHT has continued to use **WRIGHT's PHONE** in connection with certain Target Offenses since the execution of the April 2019 search warrants, as also detailed below.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

telephone [redacted] ("**WRIGHT's PHONE**")[2] and [redacted] ("**WRIGHT's BURNER PHONE**").[3]

b. Based on California Department of Motor Vehicles ("DMV") records, open source information, financial records and/or my own surveillance, I know WRIGHT to utilize [redacted], Palm Springs, California ("**WRIGHT's PALM SPRINGS**") and [redacted], Riverside, California ("**WRIGHT's RIVERSIDE RESIDENCE**").

c. Based on my review of LADWP's website and information I received in interviews, I know WRIGHT to utilize the 15th Floor and specifically room 1550 of the John Ferraro Building located at 111 N. Hope Street, Los Angeles, California ("**WRIGHT's OFFICE**").

11. MELTON EDISES LEVINE is a Los Angeles-based attorney and partner at Gibson, Dunn, & Crutcher, LLP. LEVINE is also the President of the LADWP Board of Commissioners ("LADWP Board"). LEVINE is a former United States Congressman from California, having served in the United States House of Representatives from 1983 to 1993.

---

[2] Unless otherwise noted, communications with WRIGHT described herein were conducted utilizing **WRIGHT's PHONE**.

[3] The FBI surreptitiously provided WRIGHT a "burner" phone through PARADIS at WRIGHT's request to PARADIS to conceal their communications.

a. Based on my review of seized communications[4] and information received in interviews, I know LEVINE to use the cellular telephone [redacted] ("LEVINE's Phone").[5]

b. Based on open source information, and information I received in interviews, I know LEVINE to reside at [redacted], Pacific Palisades, California ("LEVINE's Residence").

12. PAUL PARADIS is an attorney and partner at Paradis Law Group, PLLC, operating in New York and Los Angeles. In 2015, PARADIS was appointed as Special Counsel for the City in a civil litigation against PricewaterhouseCoopers ("PwC") regarding an alleged faulty billing system, (Superior Court of California, captioned *City of Los Angeles v. PricewaterhouseCoopers*, Case No. BC574690 ("PwC Case")).

a. On March 15, 2019, I initially interviewed PARADIS, in the presence of his attorney, regarding his involvement in the Target Offenses pursuant to a proffer agreement.[6] I have subsequently interviewed PARADIS on numerous

---

[6] Under the terms of the proffer sessions discussed herein, the government is allowed to make derivative use of the information provided to it. The government agrees only not to use the information against the provider of the information in the government's case-in-chief against that person, provided the person is entirely truthful in proffer sessions.

[6] Under the terms of the proffer sessions discussed herein, the government is allowed to make derivative use of the information provided to it. The government agrees only not to use the information against the provider of the information in the government's case-in-chief against that person, provided the person is entirely truthful in proffer sessions.

[6] Under the terms of the proffer sessions discussed herein, the government is allowed to make derivative use of the

occasions.[7] PARADIS has no criminal record and has agreed to assist the government in exchange for favorable consideration in a potential future prosecution of him related to his conduct in this matter. At my direction, PARADIS has conducted multiple consensual recordings with certain subjects, including WRIGHT and LEVINE, in the investigation, some of which are detailed herein.[8]

13. AVENTADOR UTILITY SOLUTIONS, LLC ("AVENTADOR") is a cybersecurity company incorporated by PARADIS on or about March 29, 2017. Around March 2019, AVENTADOR was sold at below-market value to another owner and changed its name to ARDENT CYBER SOLUTIONS, LLC ("ARDENT").

14. GINA TUFARO is a New York-based attorney and the law partner of PARADIS.

---

information provided to it. The government agrees only not to use the information against the provider of the information in the government's case-in-chief against that person, provided the person is entirely truthful in proffer sessions.

[7] Where possible at this early stage of the investigation, I have attempted to corroborate PARADIS's proffer statements with independent evidence. However, these efforts are presently complicated by the fact that many of the relevant communications may implicate attorney-client privilege or attorney work product. The FBI and the U.S. Attorney's Office are working to resolve these issues through a combination of filter reviews, requests for waivers, and an anticipated request for a judicial determination on the crime/fraud exception.

[8] As of June 4, 2019, PARADIS has conducted at least fifty hours' worth of recordings with numerous relevant persons in the investigation. I received debriefings from PARADIS regarding each of these recordings; however, due to the high volume, I have not yet listened to each part of every recording. Except where explicitly noted, any citation to a recording in this affidavit means I have reviewed that recording and/or reviewed a detailed summary thereof prepared by other FBI personnel who have reviewed it.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

15. CYNTHIA MCCLAIN-HILL is a Los Angeles-based attorney and the Vice President of the LADWP Board.

16. STEPHEN KWOK is the Chief Information Security Officer ("CISO") of the LADWP Board.

17. DAVID ALEXANDER was previously the CISO at LADWP. He was removed from that position in approximately March 2019, but remains employed by LADWP.

18. JACK LANDSKRONER is a Cleveland-based attorney and partner at Landskroner, Grieco, Merriman, LLC. LANDSKRONER was a counsel for Antwon Jones in a civil litigation against the City, (Superior Court of California, captioned *Jones v. City of Los Angeles*, Case No. BC577267 ("Jones Case")).

a. On March 14, 2019, I interviewed LANDSKRONER, in the presence of his attorney, regarding his involvement in the Target Offenses pursuant to a proffer agreement. LANDSKRONER has no criminal record and has agreed to assist the government in exchange for favorable consideration in a future prosecution of him related to his conduct in this matter.

19. PAUL KIESEL is a Beverly Hills-based attorney and partner at Kiesel Law, LLP. Along with PARADIS, KIESEL was retained as local Special Counsel for the City in the PwC litigation.

20. JAMES CLARK is the Deputy Chief for the Los Angeles City Attorney. According to the City Attorney's website, CLARK has more than 38 years of civil litigation experience, was a long-time partner at Gibson, Dunn & Crutcher, LLP, is a fellow of the American College of Trial Lawyers, and has handled a

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

multitude of complex civil litigation matters at every level of the California and Federal Courts.

21. THOMAS PETERS was the former Chief of the Civil Litigation Branch of the LA City Attorney's Office. PETERS resigned from his position on or about March 22, 2019, in the wake of allegations that he received money from plaintiffs' firms who had lawsuits against the City. PETERS oversaw the City's civil litigation in the PwC Case.

22. WILLIAM FUNDERBURK, a Los Angeles-based attorney, is the former Vice-President of the LADWP Board.

23. PAUL BENDER was appointed by the presiding Los Angeles Superior Court judge as the "independent monitor" for the City related to the settlement of the Jones Case.

24. LOS ANGELES DEPARTMENT OF WATER AND POWER ("LADWP") is, according to its website, the nation's largest municipal utility, with a $7.5 billion annual budget for water, power and combined services. LADWP is responsible for a Power System that provides over 26 million megawatt-hours of electricity per year to over 1.5 million electric services, and a Water System that delivers 160 billion gallons of water per year to 681,000 services in the City. LADWP has a workforce of approximately 10,000 employees.

25. THE LOS ANGELES CITY ATTORNEY'S OFFICE, according to its website, "writes every municipal law, advises the Mayor, City Council and all city departments and commissions, defends the city in litigation, brings forth lawsuits on behalf of the people and prosecutes misdemeanor crimes[.]"

26. CYBERGYM, according to its website, "is a joint venture of the Israel Electric Corporation, a 7.7 billion USD company that faces countless cyberattacks on a daily basis, and Cyber Control, Israel's leading cybersecurity consultancy established by ex-NISA operatives and security experts. CYBERGYM conducts cyber-warfare readiness training for governmental and private enterprises. It focuses on the weakest link in any emergency response system - the people who run it."

IV. SUMMARY OF INVESTIGATION

1. The Criminal Schemes

27. The FBI has an ongoing investigation into public corruption at the Los Angeles Department of Water and Power ("LADWP") and the Los Angeles City Attorney's Office ("City Attorney's Office"). The evidence indicates that multiple City officials are involved in several interlocking criminal schemes that implicate the Target Offenses, including the following:

a. Collusive litigation practices related to lawsuits involving the City Attorney's Office and LADWP, which were fueled in at least one instance by a $2.175 million kickback from plaintiff's attorney JACK LANDSKRONER to attorney PAUL PARADIS, a Special Counsel retained by the City Attorney's Office.

b. An $800,000 hush-money payment to a prospective whistleblower by Special Counsels PARADIS and PAUL KIESEL in exchange for silence as to collusive and potentially fraudulent litigation practices involving PARADIS, KIESEL, and THOMAS

PETERS, then the Chief of Civil Litigation at the City Attorney's Office.

c. Offering of bribes by PARADIS, and acceptance of those bribes by LADWP General Manager DAVID WRIGHT and LADWP Board Vice President WILLIAM FUNDERBURK, in exchange for at least one $30 million no-bid[9] LADWP contract to PARADIS's company.

d. LADWP's pattern and practice of falsifying records required by the Federal Energy Regulatory Commission ("FERC"), with the knowledge and approval of WRIGHT, LADWP Board President LEVINE, and other LADWP managers and Board members, in order to conceal and avoid responsibility for cybersecurity vulnerabilities related to the City's power grid, water supply, and other critical infrastructure.

e. Manipulation of LADWP contract processes by WRIGHT, LEVINE, other members of LADWP management and the LADWP Board, and members of the City Attorney's Office.

f. Conspiracy and falsification of records by the President of the LADWP, other members of the LADWP Board, LADWP managers, and members of the City Attorney's Office.

V. STATEMENT OF PROBABLE CAUSE

28. As officials of LADWP, WRIGHT and LEVINE communicated and/or interacted directly and indirectly in their official

[9] A "no-bid" contract or "sole source contract" is a contract awarded without competitive bidding. Based on my training and experience, a government entity's award of large and lucrative "no bid" contracts can be (but is not always) an indication that improper and possibly illegal deals were made to secure that contract, or that the vendor was selected for reasons beyond its suitability for the job.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

capacity with and/or about PARADIS, TUFARO, MCCLAIN-HILL, KWOK, ALEXANDER, LANDSKRONER, KIESEL, CLARK, PETERS, FUNDERBURK, BENDER, AVENTADOR, ARDENT, and CYBERGYM (collectively, the "Subjects"), relating to the schemes described herein. Based on my proffers with PARADIS, both WRIGHT and LEVINE were an integral part of the commission of the criminal schemes and/or Target Offenses and have been associated in some capacity with each of the Subjects beginning in at least 2015.

A. The Underlying Civil Litigation[10]

1. Collusive Litigation Practices between the Los Angeles City Attorney's Office, PARADIS, PAUL KIESEL, and JACK LANDSKRONER

29. In 2013, LADWP implemented a new billing system pursuant to a contract with PwC. Upon implementation of the system, widespread billing errors ensued. On December 8, 2014, an overbilled LADWP ratepayer named Antwon Jones retained New York-based attorney PAUL PARADIS to represent him in a lawsuit against LADWP for damages related to overbilling and his treatment of by LADWP.[11]

---

[10] The facts outlined in this section are based on my review of public court filings, transcripts of depositions taken in the state court cases, open source research, my interviews with LANDSKRONER and/or PARADIS, and consensually recorded meetings.

[11] PARADIS maintains that Jones retained him to sue PwC. However, Jones has testified that his intent at all times was to sue the City (not PwC), which he eventually did.

I am aware of no wrongdoing by Jones. In early 2015, four other class action lawsuits were filed against LADWP and the City of Los Angeles alleging damages related to overbilling. These lawsuits were filed by other attorneys not referenced herein; I am aware of no wrongdoing by those attorneys or plaintiffs.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

30. On December 18, 2014, PARADIS and Beverly Hills-based attorney PAUL KIESEL, serving as local counsel, met at the City Attorney's Office with then-Chief of Civil Litigation THOMAS PETERS to discuss the case.[12] PETERS was KIESEL's former law partner. At or shortly after that meeting, personnel from the City Attorney's Office retained PARADIS and KIESEL to represent the City and LADWP as Special Counsel in all disputes arising from the overbilling issues.[13] The contract formalizing PARADIS's and KIESEL's retention as Special Counsel for the overbilling matter was issued on or about April 21, 2015, and approved by the City Council on or about April 23, 2015. However, the agreement was backdated to January 1, 2015 (and based on deposition testimony, PARADIS's and KIESEL's representation appears to have effectively commenced even earlier, in December 2014).

31. At that time, the City was exploring both the possibility of suing PwC directly, and the possibility of arranging for a class of ratepayers to sue PwC for damages. The City preferred the latter option. This is because the City believed this option would benefit it politically and

---

[12] PETERS resigned from the City Attorney's Office on or about March 22, 2019, in the wake of allegations that he received referral income from plaintiffs' attorneys who had filed lawsuits against the City.

[13] In a proffer session with the government, PARADIS advised that Chief Deputy City Attorney JAMES CLARK offered them the job at the December 18, 2014 meeting in PETERS's office. According to PARADIS, and to CLARK in his deposition, CLARK had knowledge that PARADIS represented both Jones and the City in connection with LADWP billing litigation.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000163
Page 163 of 1425

financially because it would inoculate the City against lawsuits by ratepayers. For that reason, PETERS directed PARADIS, as Special Counsel for the City, to draft a complaint in a contemplated lawsuit by Jones (PARADIS's client) against PwC. PARADIS did so, and in January 2015, he sent copies of the draft complaint both to his client Jones, and to PETERS at the City Attorney's Office.[14] In part because Jones wanted to sue the City[15] and not PwC, that lawsuit did not materialize, and the City ultimately sued PwC directly in a complaint filed on March 6, 2015 ("*City v. PwC*").

32. In mid-March 2015, Jones directed PARADIS to file a lawsuit against the City (not PwC). PARADIS used his work on the draft complaint for the contemplated *Jones v. PwC* action to craft a complaint for a lawsuit by Jones against the City.[16] The civil litigation is presided over by the Honorable Elihu M. Berle, Supervising Judge of the Civil Division at Superior Court of California, County of Los Angeles. On March 26, 2015, PARADIS introduced Cleveland-based attorney JACK LANDSKRONER to

---

[14] In his deposition, Chief Deputy City Attorney CLARK testified that he likely advised City Attorney Michael Feuer of the existence of the draft *Jones v. PwC* complaint. CLARK further testified that the draft complaint was also forwarded to the LADWP Board, and that LADWP Board President LEVINE was also involved in decisions relating to the draft complaint.

[15] Based on my investigation and conversation with subjects, my understanding is that Jones desired a lawsuit against the entity he felt had wronged and then mistreated him, which was LADWP, not PWC.

[16] The timing (but not the fact) of PARADIS's work on the *Jones v. City* complaint appears to be disputed among the parties to the civil litigation.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000164
Page 164 of 1425

Jones via email, advising Jones that LANDSKRONER was an expert in municipal lawsuits who should join their legal team.[17] Jones retained LANDSKRONER on that date.

33. Chief Deputy City Attorney CLARK later testified that he learned from PARADIS about PARADIS's recommendation of LANDSKRONER to represent Jones in his lawsuit against the City. CLARK further testified that he understood and agreed that LANDSKRONER would be advantageous to the City's goals in resolving the ratepayer lawsuit because LANDSKRONER was "a more reasonable person to deal with" than the attorneys who represented the plaintiffs in the four other class-action lawsuits that had separately been filed.[18] According to CLARK, the City had several goals in resolving the ratepayer claims, including: to refund money that had been wrongfully overpaid due to billing errors; to remediate PwC's CC&B billing system, which

---

[17] Jones understood, at that time and throughout the course of his lawsuit against the City, that he was represented by both PARADIS and LANDSKRONER. PARADIS did not at any time advise Jones that he was representing the City on this matter, nor did he seek to withdraw as Jones's counsel during the course of the litigation.

[18] After his deposition, CLARK submitted, through the City's new representative counsel, an "errata" list of several dozen transcribed answers that he wished to substantively change, including multiple answers on this topic. CLARK was subsequently deposed again to explore the bases for these actions; however, the City designated this proceeding as "confidential" pursuant to the governing protective order. The City's designation was challenged, and on June 3, 2019, it was ordered to be made available. The government is working to obtain a complete copy of the most recent deposition. As of the evening of June 3, 2019, I have received part of this deposition, but I have not yet reviewed its contents. During CLARK's deposition, CLARK testified that he destroyed all of his notes related to the matter just days before the deposition.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000165
Page 165 of 1425

the City blamed for the errors; and to obtain a release sufficiently broad to cover all of the diverse claims made against the City by all of the class-action plaintiffs.

34. On April 1, 2015, LANDSKRONER filed a class-action lawsuit against the City with Jones as the lead plaintiff ("*Jones v. City*"). The complaint was signed by LANDSKRONER and Los Angeles-based attorney Michael Libman (serving as local counsel) as attorneys for plaintiff Jones. The complaint contained detailed nonpublic information, such as the numbers of ratepayers receiving certain types of utility services, which PARADIS had obtained from the City in the course of his work as Special Counsel and (presumably) provided to LANDSKRONER.[19] Personnel from the City Attorney's Office, including CLARK, were aware that the Jones complaint was going to be filed and settled before either happened. CLARK testified that he knew by the latter half of March (before the suit was ever filed) that the City would be settling with Jones.[20]

35. On April 2, 2015, LANDSKRONER sent a settlement proposal to the City. Settlement negotiations quickly ensued,

---

[19] In a proffer session, PARADIS confirmed that he obtained this information from LADWP in his role as Special Counsel. The nonpublic nature of that information and the advantages it conferred to the Jones complaint over the other class-action lawsuits have been noted on the record by counsel for the other plaintiffs.

[20] In his deposition, CLARK was asked the following: "How much earlier than April 1 did you know that the settlement demand would be forthcoming at some point and that you would be settling with Mr. Jones?" He replied, "Sometime during the latter half of -- the end of March." Following CLARK's deposition, in the above-referenced errata letter, the City's new counsel advised that CLARK wished to change that earlier sworn answer to "I didn't."

and within months, without any discovery production or any motion practice, LANDSKRONER and the City had reached an agreement. The terms of that agreement, which received final approval from Judge Berle on July 20, 2017, were consistent with those originally desired by the City Attorney. Specifically, the final settlement called for 100% reimbursement of overcharged ratepayers (as determined by LADWP and the City); a $20,000,000 remediation of the LADWP billing system; appointment of an independent monitor to oversee the remediation process;[21] and a release sufficiently broad to cover the claims alleged by the other class-action plaintiffs. The plaintiffs' attorneys were awarded approximately $19,000,000, of which more than $10,000,000 was paid to LANDSKRONER. LANDSKRONER's fees were based on billing records reflecting work allegedly performed beginning in November 2014, four months *before* he ever met or was retained by his client (and before PARADIS ever contacted Jones). Libman's fees, which totaled approximately $1,300,000, were based on billing records indicating work beginning in 2013, *before* Jones had even received the inflated LADWP bill leading him to seek an attorney.

36. On November 10, 2017, LANDSKRONER covertly paid $2,175,000 of his earnings from the settlement fees to PARADIS as a "referral fee." LANDSKRONER made this payment using a sham

---

[21] According to PARADIS, he has largely controlled PAUL BENDER, the "independent monitor," including drafting many or all of BENDER's reports, at the direction of CLARK and others at the City Attorney's Office and with the oversight of WRIGHT.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

real estate investment company, S.M.A. PROPERTY HOLDINGS, LLC, which PARADIS and LANDSKRONER had set up for that purpose.[22]

2. Hush Money to Conceal Collusive Litigation Practices[23]

37. PARADIS has proffered information indicating that in 2017, he and KIESEL paid $800,000 to a former KIESEL employee to buy her silence about purported fraudulent dual representation by KIESEL, PARADIS, and PETERS, who was then Chief of Civil Litigation at the City Attorney's Office.

38. Specifically, in approximately July of 2017, KIESEL fired his secretary, Julissa Salgueriro, who had worked for both KIESEL and PETERS when they were law partners. Thereafter, Salgueriro threatened to publicly reveal that KIESEL and PETERS were secretly engaging in collusive litigation practices in the LADWP litigation as well as one or more other cases unless KIESEL paid Salgueriro $1,000,000. KIESEL initially offered to pay Salgueriro $300,000, but she rejected that offer.

39. In October 2017, Salgueriro told PARADIS in a text message that she had approached CLARK with the information, and that CLARK had ignored her. According to PARADIS, CLARK was angry after Salgueiro reached out, and CLARK told PETERS to take

[22] This information was proffered by both PARADIS and LANDSKRONER and corroborated by bank records and other documentation that I have reviewed.

[23] The information in this subsection was proffered by PARADIS and was partially corroborated by communications between and among PARADIS, KIESEL, and Salgueriro, and others, and by the settlement agreement entered into by these parties (following a privilege review by filter attorneys, the prosecution team reviewed unprivileged portions of these materials).

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

care of the problem. At a hearing on December 4, 2017, Salgueiro approached counsel for PwC, [redacted] of Gibson Dunn, in the presence of KIESEL and PETERS, and offered to provide [redacted] with information that he would find interesting.[24] This action quickly spurred renewed discussions between KIESEL, PARADIS, and Salgueiro, which ultimately resulted in an agreement that KIESEL would pay $800,000 to Salgueiro to buy her silence. PARADIS agreed to pay half, and he wired $400,000 to KIESEL in or around late December of 2017. The agreement was memorialized in a confidential settlement agreement, which was prepared by a private attorney named [redacted]. The settlement agreement, which I have reviewed, stated that Salgueiro had "alleged legal claims and alleged violations of the law" by Kiesel's law firm, which Kiesel's law firm denied. It further stated that Kiesel's law firm alleged that Salgueiro had taken certain records from the firm, and that Salgueiro denied any impropriety in connection with those records.[25]

B. No-Bid LADWP Contracts Awarded to Attorney PARADIS and Quid Pro Quo Established with City Official (WRIGHT)

1. 2015 and 2016 No-Bid Contract for $6,000,000

40. In 2015 and 2016, during the settlement negotiations, PARADIS's two-member law firm received from LADWP two no-bid contracts totaling over $6,000,000 for project management

[24] [redacted] has confirmed that the described incident took place (he was not certain of the hearing date but believed it to be in that general time frame).

[25] The FBI has not yet interviewed Salgueiro regarding these topics.

services relating to remediation of the CC&B billing system. According to PARADIS, he did not pay any bribes or kickbacks to obtain either the no-bid contract or the extension thereof.

2. 2017 No-Bid Contract for $30,000,000

41. On March 29, 2017, PARADIS registered a company called AVENTADOR UTILITY SOLUTIONS, LLC ("AVENTADOR") for the purpose of pursuing a separate $30 million no-bid contract from LADWP, which ostensibly covered further work to remediate the CC&B system.[26] To obtain support for AVENTADOR's single-source bid for this $30 million contract, PARADIS secretly offered the LADWP General Manager, DAVID WRIGHT, a future post-retirement position as CEO of AVENTADOR, with an annual salary of $1 million and various associated benefits and perks.[27] WRIGHT

---

[26] The facts of AVENTADOR's incorporation were provided by PARADIS in a proffer and are reflected in records maintained by the California Secretary of State.

As noted below, the facts indicate that the primary purpose of this contract was different than that reflected in the contract itself and the LADWP Board's public materials about the contract.

[27] In a consensually recorded conversation, WRIGHT previously stated that he intended to retire from LADWP in 2020. In subsequent consensually recorded conversations, WRIGHT advised that he had prepared a resignation letter and informed the Mayor's Office that he would retire in October 2019. WRIGHT is seeking an arrangement with the City that would permit him, upon retirement, to be hired as a contractor to report to an offsite location (not requiring him to actually produce work) and provide transitional services to the yet to be determined LADPW General Manager.

In a consensually recorded conversation, WRIGHT referred to PARADIS as his "ATM" and requested that PARADIS begin paying WRIGHT in August 2019, despite WRIGHT's intention not to retire from the City until October 2019.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

secretly accepted this offer.[28] Based on my training, experience, and knowledge of this investigation, I believe this secret arrangement to constitute bribery of a public official because it established a quid pro quo, namely, PARADIS's receipt of a lucrative City contract in exchange for WRIGHT's lucrative future salary.

42. According to PARADIS, during the months preceding the LADWP Board's vote on the $30 million no-bid contract, PARADIS also courted support from LADWP Board Vice President, attorney WILLIAM FUNDERBURK, who, in turn, solicited financial benefits from PARADIS before the vote.[29] I believe this arrangement to similarly constitute a quid pro quo relationship between PARADIS and FUNDERBURK.

43. Specifically, on May 31, 2017, FUNDERBURK asked PARADIS to provide legal services on behalf of a class-action

---

[28] In a proffer session, PARADIS described his agreement with WRIGHT as to WRIGHT's future employment with and financial interest in AVENTADOR. WRIGHT confirmed their agreement in multiple consensually recorded conversations with PARADIS.

In addition to WRIGHT's financial interest in AVENTADOR, PARADIS and WRIGHT are planning to engage in another business venture that would solicit lucrative contracts from LADWP. Specifically, PARADIS and WRIGHT have agreed to partner with an Israeli company called CYBERGYM to open cybersecurity training facilities in Los Angeles and elsewhere to serve personnel from LADWP and other utility companies. PARADIS's affiliation with this company is overt, but WRIGHT, as current LADWP General Manager, has endeavored to hide his role.

PARADIS, WRIGHT, and LEVINE all traveled to Israel to meet with individuals related to CYBERGYM and the partnership with LADWP. WRIGHT and LEVINE coordinated the logistics of these trips utilizing the **TARGET PHONES**.

[29] PARADIS proffered the information herein regarding benefits that he provided to FUNDERBURK in exchange for FUNDERBURK's support of his contract.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

defendant that FUNDERBURK was representing. PARADIS agreed to assist because he knew that FUNDERBURK was set to vote on the $30 million no-bid contract the following week, and he wanted FUNDERBURK to vote in his favor. FUNDERBURK e-mailed PARADIS the necessary documents, and PARADIS wrote a brief and sent it back to FUNDERBURK. PARADIS never billed FUNDERBURK or FUNDERBURK's client, nor did FUNDERBURK ever reimburse PARADIS for his legal services. Between May 31, 2017, and August 6, 2017, PARADIS performed "free" legal work for FUNDERBURK and FUNDERBURK's client because of FUNDERBURK's influence over the $30 million no-bid contract and potential future contracts.

44. Additionally, in October 2016, during PARADIS's initial preparations to seek the contract the following year, FUNDERBURK invited PARADIS to an award ceremony at which FUNDERBURK was being honored, telling PARADIS that FUNDERBURK expected PARADIS's full support. On the guidance of WRIGHT, who advised PARADIS that he needed to donate because FUNDERBURK would soon be voting on PARADIS's contract, PARADIS donated $5,000 to the organization hosting FUNDERBURK's award function.

45. On June 4, 2017, two days before the LADWP Board approved the AVENTADOR contract, WRIGHT sent a text message to LEVINE with FUNDERBURK's contact information. LEVINE responded, "Left a detailed vm [voicemail]. Will call again." That same day, LEVINE left a voicemail for WRIGHT that said, "I just reached BILL [FUNDERBURK], **I do not believe BILL [FUNDERBURK] will end up being a problem;** however, the issue is diligence. He said why don't we have like a committee, an oversight committee

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to monitor the progress. I think that is probably a good idea, but I told him I want to run that idea by you and not sign off on anything. I was going to go with you, period. But, that sounded like a reasonable suggestion, so I wanted to hear your thoughts about it."[30] Based on my training, experience, and knowledge of the investigation, I believe that LEVINE referencing that "BILL will not end up being a problem" to mean that LEVINE and WRIGHT, utilizing the **TARGET PHONES**, were coordinating efforts to ensure the $30 million AVENTADOR contract was approved. FUNDERBURK, being the Vice-President, needed to "not be a problem" leading into the LADWP Board meeting.

46. At the LADWP Board meeting on June 6, 2017,[31] both WRIGHT and LADWP Board President (and Gibson Dunn attorney) LEVINE strongly argued in favor of awarding the $30 million no-bid contract to AVENTADOR, underscoring that the need for AVENTADOR's billing-system remediation services was so imminent that there was not sufficient time to engage in the standard competitive bidding process usually required for LADWP contracts of that size.[32] In addition, LADWP Ratepayer Advocate, Frederick

---

[30] This voice-mail was seized pursuant to the April 18, 2019 authorized by the Honorable Magistrate Judge Jacqueline Choolijan.

[31] This meeting was audio/video recorded by the City and I have reviewed this recording.

[32] In this Board meeting, video footage of which is publicly available on LADWP's website, WRIGHT described the urgent need to award this no-bid contract to AVENTADOR based on the negotiated terms of the pending settlement agreement, which required the City to remediate the CC&B system. LEVINE

Pickel, was asked if he had any questions or input, to which Pickel replied with an inquiry about how oversight would be provided. WRIGHT suggested that a subcommittee be formed to evaluate the work being completed, and LEVINE and FUNDERBURK were selected to perform that role. According to the above-described June 4, 2017 voicemail message from LEVINE to WRIGHT, which I have reviewed, these comments appeared to be staged. Following the enthusiastic recommendations of WRIGHT and LEVINE, all the Board members (including FUNDERBURK) voted in favor of awarding the $30 million contract to AVENTADOR.[33] Based on the context of the communications, the recording of the meeting, the interviews I conducted, and my knowledge of the investigation, I believe WRIGHT and LEVINE utilized the **TARGET PHONES** to coordinate together and/or with FUNDERBURK for the AVENTADOR contract approval. This is relevant evidence because of WRIGHT's quid pro quo relationship with PARADIS, and I am seeking to determine who else (a) was aware of their illicit relationship and (b) was set to financially benefit from the AVENTADOR contract approval.

---

enthusiastically concurred, noting that LADWP had no choice but to award the no-bid contract to AVENTADOR. As discussed further below, the representations made by WRIGHT and LEVINE do not appear to be a fair or accurate description of the choice the LADWP Board had to make when awarding this $30 million dollar contract and instead appear to be pre-textual reasons to get the contract approved expeditiously and with little scrutiny.

[33] The Los Angeles City Council has the prerogative to review a contract of this size. According to PARADIS, WRIGHT asked certain members of City Council not to review the AVENTADOR contract.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

3. WRIGHT Advocated For and Praised AVENTADOR in an Effort to Gain Support for Future Contracts

47. On May 12, 2018, in a text message, WRIGHT told LEVINE, "MEL[TON LEVINE], here's a short message I sent [redacted] LADWP Chief Operating Officer] that's entirely plausible from meetings that we attended over the entire trip.[34] Just wanted you to know… We provide rebates for facility energy management systems. Some of the light bulbs that could work with them have light sensors or motion sensors in them. Hackers could go through the light bulbs to hack their facility's entire IT systems. Now think if that energy management system services a hospital. It could actually kill patients! And on top of how horrible that is, we would likely be pulled into the lawsuit." LEVINE replied, "Yikes!!!!!" Based on my training, experience, and knowledge of the investigation, I believe WRIGHT informed LEVINE about his message to [redacted] in an effort to plant seeds related to the need for cyber security. I believe that although the cyber vulnerabilities and necessity for cyber security measures may indeed exist, WRIGHT was such an advocate for cyber awareness and security services at least in part because of his illicit quid pro quo relationship with PARADIS, namely, WRIGHT's self-interest in his future lucrative employment with AVENTADOR.

48. On August 17, 2018, WRIGHT sent a text message to LEVINE and LADWP Board Commissioner Christina Noonan, "we have experienced a phishing attack that has resulted in hackers

[34] Based on the timing of the text message and my knowledge of the investigation, I believe that this was a reference to the May 2018 Israel trip attended by PARADIS, WRIGHT, and LEVINE, along with other LADWP officials.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

obtaining staff credentials and gaining access into our systems. We don't know yet to what extent. AVENTADOR staff have been working 24/7 to contain the situation. Nothing on our systems has been compromised or information released that we are aware of. But his [PARADIS's] dozen staff are mostly from the NSA or DOE and are **the best in the nation.** I will fill you in as we know more." Noonan replied, "Just checking in on this situation. Is AVENTADOR pre-approved under our cyber insurance policy? Any of this 24/7 cost will need to go against our deductible. Also, **I suggest communication relating to this matter, particularly with AVENTADOR, go through our legal counsel so that the Department secures attorney/client privilege which will be beneficial.** All of this presumes we have noticed our insurance carriers." Based on my knowledge of the investigation, I believe that WRIGHT glorified the team as being "the best in the nation" to further praise ADVENTADOR, a company in which WRIGHT secretly had a strong financial interest. In addition, I believe Noonan's comments that communication regarding AVENTADOR should be cloaked in attorney/client privilege to be consistent with LADWP's pattern of behavior to conceal aspects of the AVENTADOR contract.

49. Later that day, WRIGHT provided an update regarding the situation and stated, "We have 10 former staff from the NSA and DOE working 24/7 throughout the weekend and next week on the most highly exposed areas of our SCADA operating systems. (Our contractor, AVENTADOR owned by PAUL PARDIS, hired almost all of the DOE's cyber team over the last six months to work for him,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

so we have the some of the best experts related to these hacking efforts in the world working on this.). Biggest worry is that several months of planned system fixes now have to be expedited into just a few weeks. We can tell the hackers keep trying to attack us but we are on it. (As perspective, **if we called the Federal government for help, they would contact the DOE who would have assigned the staff AVENTADOR already hired to come out to help us**.)." LEVINE replied, "Wow. Thanks Dave. Hang in there. If you want to talk over the weekend or Monday let us know." Based on my knowledge of the investigation, I believe WRIGHT was again advocating for LADWP's continued reliance on AVENTADOR and excusing the need to contact the Federal government regarding the issues. WRIGHT's effusive adulation portrays AVENTADOR and PARADIS as saviors to the City, a depiction that appears unwarranted by the facts and in any event omits WRIGHT's covert financial entanglement with AVENTADOR.[35] In addition, I have reviewed text messages between PARADIS, WRIGHT, and LEVINE in which PARADIS echoes WRIGHT's sentiments

---

[35] In October 2016, AVENTADOR performed penetration testing at the Los Angeles International Airport ("LAX") to test cyber vulnerabilities. The FBI received notice from LAX regarding the intrusion. Cyber agents with the FBI subsequently conducted an investigation that lead to the execution of a search warrant for [redacted], an AVENTADOR employee. [redacted] stated that he was authorized to conduct the penetration test and that AVENTADOR had a contact with the City. Representatives from AVENTADOR (now ARDENT) have yet to produce said contract. Based on my interviews with PARADIS, no such contract existed regarding penetration testing at LAX; however, PARADIS maintains that the testing was verbally authorized by City officials. Based on my discussions with FBI cyber agents, AVENTADOR's work was in fact "amateur."

about AVENTADOR's expertise and necessity, yet omits reference to WRIGHT's financial interest in AVENTADOR's hiring.

50. On August 23, 2018, WRIGHT sent a text message to LEVINE, "no need to call back unless you want more info. Cyber attack has been contained. Mayor briefed by PAUL [PARADIS] and I. It was sophisticated. But PAUL's [PARADIS] **elite team of experts** handled it and prioritized fixes. **Staff is now becoming very accepting of AVENTADOR staff** and excited about getting some training from the experts. PAUL [PARADIS] is charging us for this time, but not overcharging. We are so messed up here that **I will likely suggest a two year extension and an increase to his contract.** But that's six months away. I want to brief the board again at the next meeting." LEVINE replied, "Thanks DAVE [WRIGHT]. Just received. Great news. Please get back to me today if possible with the names of the Israeli companies we are considering using so I can promptly get back to the guy st [at] DHS Rep. Schiff put us together with. Thanks." WRIGHT then responded, "PAUL [PARADIS] is sending via text. **We don't want to do via LADWP email.**" PARADIS then sent a text message to WRIGHT and LEVINE with the Israeli companies' information and stated, "I sent this as a text rather than email for security and public record disclosure reasons." LEVINE then responded, "Great. Thanks. This is what I need and a good way to send. Will get back to you after I hear back." Based on the context of the communication, it appears as though WRIGHT was once again praising AVENTADOR heavily and laying the groundwork to advocate for an extension for AVENTADOR while utilizing personal email,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

which would not be subject to City monitoring. To my knowledge, WRIGHT does not have any formal cyber training or knowledge to be able to distinguish the experts in the field nor be able to provide the LADWP Board a true and accurate assessment of AVENTADOR's work, qualifications, or necessity. I believe that WRIGHT praised and advocated for AVENTADOR so heavily based on his quid pro quo relationship with PARADIS, namely, his financial stake in AVENTADOR contracts.

C. Alleged Falsification of Regulatory Paperwork by LADWP Employees

1. Underreporting and Failure to Report Cybersecurity Issues

51. The above-described LADWP contract awarded to AVENTADOR purported — according to its own terms and to the related LADWP Board materials and proceedings — to cover services related to remediation of the CC&B system, as required by the terms of the settlement agreement in *Jones v. City*. However, evidence suggests that this $30 million single-source contract, which General Manager WRIGHT and Board President LEVINE advertised to the LADWP Board as urgent because it was mandated by the court-ordered settlement agreement, was in truth to address an entirely unrelated matter, that is, it was primarily intended to cover services related to assessing and improving cybersecurity for the City's power grid and other critical infrastructure.[36]

[36] The information in this section was proffered by PARADIS and has been corroborated in part by: 1) the aforementioned consensually recorded conversations with WRIGHT; 2) separate

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

52. PARADIS alleges that in order to conceal and avoid responsibility for certain cybersecurity vulnerabilities related to critical infrastructure, LADWP employees falsified mandatory federal regulatory documents[37], including by regularly self-reporting minor violations in order to avoid the discovery of much more significant violations, which would carry substantial fines (in some cases, millions of dollars). Based on my interviews with PARADIS and my knowledge of the investigation, including review of recordings on this topic, City officials stated that they were under the impression that if they self-reported certain violations, federal regulatory agencies would be less likely to inquire into or investigate other possible violations.

53. In separate consensually recorded conversations with both the current and former Chief Information Security Officers for LADWP (STEPHEN KWOK and DAVID ALEXANDER, respectively), PARADIS confirmed both LADWP's pattern of self-reporting of minor violations to conceal far more significant problems and the fact that members of LADWP management (including WRIGHT) and the LADWP Board (including LEVINE and CYNTHIA MCCLAIN-HILL) were aware of that unethical and potentially illegal practice.

---

consensually recorded conversations with an AVENTADOR employee; and 3) an AVENTADOR work plan and other documents reflecting AVENTADOR'S cybersecurity work for the City, which PARADIS provided to the government.

[37] These include documents mandated by the Federal Energy Regulatory Commission ("FERC") under a compliance regime known as "NERC-CIP" (North American Electric Reliability Corporation - Critical Infrastructure Protection).

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

54. DAVID ALEXANDER also informed PARADIS in a consensually recorded conversation that LADWP falsified paper records to avoid significant fines that might be imposed by NERC and FERC. For example, NERC-CIP Reliability Standard CIP-007-6 requires that bulk electric system facilities deploy a patch management process to monitor and address software vulnerabilities; this process includes adhering to a security patch evaluation timeline to ensure that all patches are up-to-date. In an April 2019 consensually recorded conversation with PARADIS, ALEXANDER said that a comparison of LADWP's paper records to its computers would show that LADWP claimed it applied patches in a timely fashion when, in fact, it did not. ALEXANDER's proposed solution to the problem, which he disclosed to PARADIS, was to simply dispose of all the old computers evidencing delayed patching, and replace them with new computers that had no evidence of any patching issues.

D. Alleged Circumvention of LADWP's Contracting Process

1. WRIGHT and LEVINE Discussed the Necessity of Cyber Services for LADWP

55. On January 8, 2019, WRIGHT sent a text message to LEVINE, "Cyber and IT will always need external staff (I think [redacted] - Business Manager, IBEW Local 18][38] already supports this), we are increasing staff everywhere in the department as fast as reasonable. Need to get more supportive on

[38] IBEW Local 18 is a labor union. According to IBEW Local 18's website, Local 18 is an "affiliate of the International Brotherhood of Electrical Workers (IBEW). Although our name says "electrical workers," our members come from hundreds of different job classifications."

outsourcing as we have hired a net increase of couple thousand staff in the last few years. We support greater workforce development but LADWP needs to have a greater role in screening them for base line qualifications."

56. On March 14, 2019, LEVINE sent a text message to WRIGHT, "Ok. I need to talk with Dakota [Smith - Los Angeles Times Reporter] again in the next few minutes. Pretty much told her what we are doing to keep the cyber employees. She questioned if that is consistent with board instruction to cancel AVENTADOR contract.[39] Joe [Brajevich - LADWP General Counsel] gave me a good response to that." Based on the context of the communication it appears as though Smith inquired into the retention of City cyber employees and the fate of the AVENTADOR employees post cancellation. The formation of ARDENT, a subsequent awarded contract discussed below, do not appear to me to be consistent with the LADWP Board's demand.

57. On March 26, 2019, WRIGHT sent a text message to LEVINE, "I have to share at some point that [we are] deliberately vague on our public descriptions as we were worried about publicly communicating our specific cyber vulnerabilities. And we discussed this in closed session and in our meetings with other city staff. Will try to mention it in general in the

[39] According to PARADIS, after his dual role in the civil litigation came under scrutiny as described herein, in order to keep AVENTADOR employees working on the City contract, PARADIS submitted to pressure to sell AVENTADOR and have no part in any subsequent companies that form. PARADIS sold AVENTADOR below market value and has in fact remained an integral part of ARDENT (the new company). Based on consensually recorded conversations, WRIGHT and LEVINE are aware of PARADIS' continued involvement.

meeting tomorrow morning if it fits into the discussion." LEVINE replied, "Good. Radio silence from CYNTHIA [MCCLAIN-HILL] after calling and emailing."

58. On March 27, 2019, WRIGHT sent a text message to LEVINE, "Check LADWP email. Excellent summary document regarding cyber we will discuss at tomorrow's meeting." LEVINE replied, "Can you send it to my other email?"[40] I believe LEVINE requested the information to be sent to his "other email" to possibly conceal information involved in the Target Offenses.

2. Manipulation of the SCCPA Bidding Process

59. According to PARADIS, LADWP management and members of the Board (including WRIGHT, LEVINE, and MCCLAIN-HILL) have successfully manipulated LADWP's contracting processes to ensure that AVENTADOR's successor company, ARDENT UTILITY SOLUTIONS, LLC ("ARDENT")[41], is awarded a lucrative contract to continue AVENTADOR's cybersecurity work without engaging in the required competitive bidding process (the "ARDENT contract"). According to information proffered by PARADIS, LADWP routinely uses the Southern California Public Power Authority ("SCPPA")[42] to

---

[40] Based on my interviews of PARADIS, LEVINE utilized his Gibson Dunn email to conduct City business, not his LADWP email.

[41] Despite a sham sale in March 2019, PARADIS appears to still effectively control this company.

[42] According to the SCPPA website, SCPPA is "a Joint Powers Authority, created in 1980, for the purpose of providing joint planning, financing, construction, and operation of transmission and generation projects."

circumvent LADWP's standard 12-18 month competitive bidding process, and did so for the ARDENT contract.[43]

60. The SCCPA website shows that in February 2019, SCCPA issued a Request for Proposals for Cybersecurity Services. On March 27, 2019, WRIGHT sent a text message to LEVINE, "During the discussion with Cynthia and [redacted] after the larger meeting today, it was determined that no report will go forward at the next board meeting. We will move the second meeting to April 16th and take the contact forward then. I can discuss more over the phone if you'd like." LEVINE replied, "Yes. Still in meetings. Will reach Out when able."

61. On March 29, 2019, WRIGHT sent a text message to LEVINE, "The mayors office directed me about 90 minutes ago to put an item on the agenda for 4/2 that covers critical incident cyber response. The thought is that we will cite our ability to utilize the city's ITA contract hours and their 24 hour response time with two vendors they have - Fireeye and Dell. And then to direct staff to negotiate a separate LADWP contract for more hours and a faster response time. I've got Donna [Stevener - LADWP Chief Administrative Officer] and Stephen [KWOK] figuring out the best language for an agenda item and then running it past Joe B[rajevich]. The written report can submitted Monday or Tuesday morning per Joe [Brajevich]." LEVINE replied, "Will call you in a few minutes to discuss."

---

[43] According to the SCPPA website, WRIGHT is the Secretary of SCPPA and a current member of the SCPPA Board of Directors.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

62. On April 5, 2019, in a consensually recorded conversation, LEVINE and MCCLAIN-HILL confirmed to PARADIS that ARDENT would be the primary vendor (out of 28 candidates), *despite the fact that SCPPA was not scheduled to vote on the contract until a meeting on April 18, 2019* — almost two weeks later. Based on my training, experience, and knowledge of the investigation, this behind-the-scenes manipulation of City contracting processes appears to be consistent with related unethical and/or illegal behavior by LADWP officials. On April 23, 2019, the LADWP Board approved a 60-day contract of $3,600,000 for ARDENT and two other companies.[44]

[44] The Board's action is confirmed in public materials on the LADWP website. According to PARADIS and confirmed in a consensually recorded conversation with WRIGHT on April 21, 2019, the original plan for a larger contract to ARDENT was tabled after the Mayor's office exerted pressure on LADWP to avoid such a large contract with ARDENT due to the potential for negative publicity related to ARDENT, a successive company to AVENTADOR, being awarded another large contract. PARADIS reported that LADWP planned that the majority of the $3.6M 60-day contract would go to ARDENT, and that the contract would thereafter be extended or expanded.

E. Alleged Conspiracy and Falsification of Records by Attorney Members of the LADWP Board, LADWP Attorneys, and Members of the City Attorney's Office[45]

1. The City's Debarment of PwC

63. In June 2016, while representing the City in its litigation against PwC, PARADIS proposed debarring[46] PwC in the wake of salacious public allegations that PwC employees had misspent City money on personal entertainment (including prostitutes and alcohol) in Las Vegas. According to PARADIS, in a closed session on June 21, 2016, the LADWP Board agreed with PARADIS and voted 4-0 in favor of debarring PwC, with Board President LEVINE recusing himself from the discussion and vote due to a conflict of interest.[47] Based on LADWP's minutes of the public board meeting on that same date, it appears that the four other board commissioners at the time were FUNDERBURK, Michael Fleming, Christina Noonan, and Jill Banks Barad.

[45] PARADIS proffered the information in this section and provided the government with his correspondence with LEVINE, WRIGHT, FUNDERBURK, Brajevich, and others. While the version seen by the prosecution team to date was heavily redacted by the government's filter attorneys, it generally corroborates PARADIS's account, as detailed below.

[46] Debarment is the state of being excluded from enjoying certain possessions, rights, privileges, or practices and the act of prevention by legal means. For example, companies can be debarred from contracts due to allegations of fraud, mismanagement, and similar improprieties.

This initiative to debar PwC came in the wake of public allegations that PwC managers overbilled the City and then spent the money on prostitutes, luxury bottle service liquor, and entertainment in Las Vegas. See https://www.latimes.com/local/lanow/la-me-ln-dwp-billing-20160630-snap-story.html.

[47] According to PARADIS, LEVINE is supposed to be recused from LADWP Board matters involving PwC because PwC is a prominent and lucrative Gibson Dunn client. (LEVINE is a partner at Gibson Dunn, and Clark retired from Gibson Dunn as a partner.)

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

64. PARADIS further reported that a press release touting the debarment was drafted and circulated among the staff of the City Attorney's Office. According to PARADIS, LEVINE, City Attorney Michael Feuer, former Chief of Civil Litigation PETERS, LADWP General Counsel Joseph Brajevich, and others thereafter embarked on a furtive and successful campaign to influence the other LADWP Board members to secretly change their votes, which ultimately resulted in the PwC debarment issue being dropped. The initial 4-0 vote in favor of debarment was not reflected in Board materials and PwC was not debarred.

65. According to PARADIS, he and his law partner, GINA TUFARO, were called to meet with Feuer and others (including PETERS, Brajevich, and Leela Kapur, Feuer's Chief of Staff) in Feuer's office on June 30, 2016. Feuer was angry about the debarment initiative and informed PARADIS that he (Feuer) was the "team captain" and as such was charged with making the decision as to whether to pursue debarment. PARADIS stated that the Board had already voted and debarment was therefore going to happen, and Feuer said words to the effect that, "We'll see about that."[48] At Feuer's direction, PARADIS made a presentation to LADWP management, including WRIGHT, in favor of debarment, and PETERS gave a contrary presentation against debarment. PARADIS then met with LADWP Board Vice President FUNDERBURK, who told PARADIS that both he and another Board member, Michael

[48] According to PARADIS, Feuer claimed that the debarment process was "in shambles," and thus that debarment was not a viable option. However, PARADIS noted that the Board also voted to debar another entity at the same June 21, 2016 meeting, and that the other debarment vote was never challenged.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Fleming, were committed to debarment and would stand by their votes in favor of debarring PwC. A few days later, FUNDERBURK contacted PARADIS to advise that debarment was probably not going to happen. PARADIS went to WRIGHT and threatened to "blow the whistle" - meaning he would disclose information related to certain criminal schemes to the public - if he didn't learn what was going on, and obtained WRIGHT's permission to review the emails from the LADWP server during the period of the debarment dispute.

66. PARADIS then printed a large number of emails reflecting communications about debarment and behind-the-scene efforts by LEVINE, Feuer, Brajevich, then-LADWP General Manager Marcie Edwards, and others to reverse the Board's 4-0 vote to debar PwC. The prosecution team has since reviewed redacted versions of some of those emails, as received from the government's filter team. While the text of almost all of the emails is heavily redacted (due in part to the apparent default practice of copying General Counsel Brajevich on nearly every piece of correspondence), the email traffic is generally consistent with PARADIS's account of the debarment episode.

67. Specifically, the emails indicate that:

- On June 30, 2016, City Attorney Michael Feuer held a scheduled meeting with Brajevich, PETERS, and Kapur, regarding PwC.
- Over the next few days, FUNDERBURK, PETERS, Kapur, Feuer, Brajevich, and others traded numerous emails on the subject of PwC and the debarment issue.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

- On July 1, 2016, at the end of an email exchange between FUNDERBURK, WRIGHT, Michael Fleming, Marcie Edwards, Joseph Brajevich, and later, LEVINE, regarding a special board meeting to discuss PwC, Marcie Edwards forwarded the email chain only to FUNDERBURK with the message, "Please. Trust me and stand down." (emphasis added).
- On July 1, 2016, LEVINE and Edwards discussed having Feuer speak with FUNDERBURK.
- On July 1, 2016, notwithstanding his recusal from PwC debarment matters, LEVINE sent an email to all Board commissioners, Edwards, and Brajevich, with the subject "PWC lawsuit."
- On July 1, 2016, after emails between FUNDERBURK and Edwards, WRIGHT advised Edwards that FUNDERBURK "wants to be removed from this specific item as it's heard."

68. As stated above, debarment of PwC did not ultimately happen, and the minutes from the June 21, 2016 LADWP Board meeting do not reflect the original 4-0 vote in favor of debarment. Rather, the Board meeting minutes from June 21, 2016, note: "Discussion held - action taken but not a final action that is reportable." Based on my knowledge of the investigation, I believe the minutes did not accurately reflect the events that actually transpired at the meeting. It is presently unclear to me the motivations of LEVINE, Feuer, and other members of the City Attorney's Office preventing the debarment and why LEVINE was included in the discussions despite being recused.

F. Obstruction of Justice by WRIGHT[49]

1. WRIGHT's Request That PARADIS Destroy Evidence in His Email Accounts and on His Laptop and Cell Phone

69. On March 28, 2019, PARADIS and WRIGHT exchanged text messages arranging a meeting in Rancho Mirage, California, approximately 120 miles from Los Angeles. PARADIS proffered that he and WRIGHT would previously meet in Rancho Mirage to conceal their meetings when discussing their criminal schemes, including the quid pro quo AVENTADOR arrangement and certain criminal schemes.

70. On March 29, 2019, in a consensually recorded conversation, PARADIS and WRIGHT arranged a meeting on March 30, 2019, at 6:00 AM at PARADIS' residence in Rancho Mirage. WRIGHT said he wanted an early hour meeting because he was worried that people would see PARADIS and WRIGHT together. Specifically, WRIGHT said he was concerned because the Daily Journal and LA Times were reporting on the suspected fraud(s) discussed above.

71. On March 30, 2019, in a consensually recorded meeting, PARADIS and WRIGHT discussed the quid pro quo arrangement and confirmed WRIGHT's financial interest in AVENTADOR. PARADIS informed WRIGHT that WRIGHT's future employment with AVENTADOR was still in the works. WRIGHT stated that he thought that prospect was dead because of the sale of AVENTADOR and scrutiny of PARADIS due to PARADIS' improper dual role in the collusive

[49] The recordings described in the section are some of the consensually recorded conversations with WRIGHT. I have not included every recording between PARADIS and WRIGHT. *See footnote 8.*

civil litigation; but after speaking to PARADIS, he now felt "resurrected." WRIGHT and PARADIS discussed the need to be "on the same page" and what to say if anyone, including specifically "the FBI", were to inquire into their conduct and the formation of AVENTADOR. WRIGHT was concerned about potential discovery of his text message and email communications between himself, PARADIS, and LEVINE over **WRIGHT's PHONE.**[50] WRIGHT was also concerned about the AVENTADOR laptop computer (WRIGHT's laptop) that PARADIS had previously given to him.[51] Following a discussion of their options concerning those communications, WRIGHT requested that PARADIS "get his people" to destroy all evidence of their communications on **WRIGHT'S PHONE** and all information on WRIGHT'S laptop.[52] Specifically, WRIGHT told PARADIS to destroy all his emails from his two AOL email accounts, as well as the corresponding iCloud accounts for them.

---

[50] PARADIS informed me that he received emails from WRIGHT from both of WRIGHT's AOL email accounts: [redacted] and [redacted]. PARADIS also informed me that on some of these emails, he was cc'd on communications between WRIGHT and the other subjects in this investigation, including, but not limited to, GINA TUFARO, MEL LEVINE, CYNTHIA MCCLAIN-HILL, STEPHEN KWOK, DAVID ALEXANDER, JACK LANDSKRONER, PAUL KIESEL, JAMES CLARK, THOMAS PETERS, WILLIAM FUNDERBURK, PAUL BENDER and others from the Los Angeles City Attorney's Office. While PARADIS has offered to show me some of these emails, I have not reviewed any of them, given that the possibility that some may implicate an attorney-client privilege.

[51] According to WRIGHT, in a consensually recorded conversation, WRIGHT maintained the laptop at **WRIGHT's RIVERSIDE RESIDENCE.**

[52] Based on the context of the conversation and my knowledge of this case, I understood this to be a reference to the team of hackers and intelligence agency veterans that PARADIS had recruited and hired to work for AVENTADOR on the above-referenced cybersecurity issues.

72. WRIGHT agreed to provide PARADIS **WRIGHT'S PHONE** and WRIGHT'S laptop so that WRIGHT could "wipe" the devices clean of incriminating evidence. In addition, WRIGHT told PARADIS that he already shredded all related documents within **WRIGHT's OFFICE** that involved PARADIS and/or LEVINE, and that he planned to do so again the following week.[53] PARADIS agreed to wipe **WRIGHT's PHONE** and laptop and delete all emails on the provider's servers. In addition, WRIGHT and PARADIS discussed utilizing the application Confide to communicate as a means to conceal their communications.[54]

73. On March 31, 2019, in a consensually recorded meeting, WRIGHT provided PARADIS **WRIGHT'S PHONE** and WRIGHT'S laptop so that, as he and PARADIS had agreed, PARADIS could wipe the devices to include deleting all text messages and emails. WRIGHT and PARADIS agreed to meet in Santa Monica, California, on April 1, 2019, to return **WRIGHT's PHONE** wiped. PARADIS subsequently provided **WRIGHT's PHONE** and WRIGHT's laptop to the FBI to preserve all evidence on the phone and laptop.

---

[53] Based on WRIGHT confirming that evidence related to the Target Offenses was contained in **WRIGHT's OFFICE**, and that WRIGHT planned to destroy additional evidence the next week, I believe there is probable cause and a search warrant for **WRIGHT's OFFICE** is necessary to identify (1) indicia that evidence was destroyed (shredded paper, labeled but empty labeled folders/cabinets, other evidence of missing items), (2) if WRIGHT failed to destroy everything and there still remains evidence of the Target Offenses and criminal schemes, or (3) if WRIGHT did not destroy the evidence as described and the evidence remains in **WRIGHT's OFFICE.**

[54] Confide is an encrypted messaging application that deletes each communication after it is viewed. PARADIS proffered that WRIGHT had previously asked him to use Confide in connection with the Target Offenses and criminal schemes.

74. On April 1, 2019, in a consensually recorded meeting, PARADIS and WRIGHT discussed further concealing their future communication via "burner"[55] phones. PARADIS and WRIGHT agreed to meet on April 3, 2019, at the Disney Concert Hall in Los Angeles, California, for WRIGHT to pick up a burner phone from PARADIS.

75. On April 3, 2019, I conducted surveillance of PARADIS and WRIGHT's meeting at the Disney Concert Hall. PARADIS was seated at a table in the back corner of the café with a brown paper bag that contained **WRIGHT's BURNER PHONE** (provided to him by the FBI) and **WRIGHT's PHONE**. WRIGHT approached PARADIS and provided a head nod which PARADIS understood to mean WRIGHT acknowledged PARADIS' presence. PARADIS subsequently left the bag with the two phones on the table and walked into the men's bathroom. WRIGHT then approached the table and removed the bag from the table and exited the concert hall before PARADIS returned back to the table. PARADIS and WRIGHT had no verbal interactions during this exchange. Based on my training and experience, PARADIS and WRIGHT's behavior was consistent with a surreptitious "drop" designed to mask the existence of any meeting or transaction between the two. PARADIS then sent a text message via his own FBI provided burner phone disclosing to **WRIGHT's BRUNER PHONE** the number for PARADIS' new burner phone.[56]

76. PARADIS then requested from WRIGHT the usernames and

---

[55] A "burner" phone is typically a difficult to trace phone that provides little to no paper trail back to its user.

[56] Subsequent to receiving the "burner" phone, WRIGHT communicated with PARADIS via **WRIGHT's BURNER PHONE.**

passwords for WRIGHT's email accounts and Apple iCloud accounts that WRIGHT requested be wiped. WRIGHT subsequently provided the information for his accounts [redacted], [redacted],[57] and iCloud accounts [redacted] and [redacted]. These accounts were the email accounts and Apple iCloud accounts associated with **WRIGHT's PHONE** and email accounts, that WRIGHT requested be wiped because they contained communications with PARADIS, LEVINE, and others related to certain Target Offenses. PARADIS subsequently provided this account information to the FBI.

77. WRIGHT provided PARADIS the devices and account information freely and with the request and expectation that PARADIS wipe and delete all information on the devices/accounts as a means to destroy evidence related to the Target Offenses. The government did not believe WRIGHT maintained an expectation of privacy in the referenced devices/accounts. Nevertheless, in the abundance of caution, the government sought and obtained the April 18 search warrants to search the extractions/downloads of the devices/accounts for evidence of the Target Offense and criminal schemes. The instant additional requested search warrants are to gather additional evidence.

78. On April 3, 2019, in a consensually recorded conversation, WRIGHT told PARADIS, "I have gone through

---

[57] On April 3, 2019, WRIGHT inadvertently provided an incorrect email address as [redacted] when it actually was [redacted]. On April 11, 2019, PARADIS confirmed the email address in a text message utilizing the burner phones. WRIGHT responded, "I don't think [redacted] is mine. Just [redacted]."

[**WRIGHT's OFFICE**] and checked everything. I literally just got rid of a whole bunch of shit… what I am concerned, is what if [the timeline] is found in your possession? . . . . I am anxious right now . . . **my risk is how you and I talked about eventually setting something up**. There is not much there [documentation wise], the timeline read and shred it. I know I am being overly extreme, but there are search warrants that are served and you know." Based information received from PARADIS, the timeline WRIGHT referred to was the events related to the AVENTADOR contract. I believe WRIGHT provided an omission to the quid pro quo with PARADIS and specifically acknowledged his criminal liability as his "risk." In addition, it appears as though WRIGHT is aware that the government can utilize search warrants and therefore destroying the evidence in **WRIGHT's OFFICE**, **WRIGHT's PHONE** and WRIGHT's email's was a priority and is evidence of WRIGHT's intent to obstruct justice.

2. **WRIGHT** Maintains Evidence of the Criminal Schemes in **WRIGHT's PALM SPRINGS RESIDENCE**

79. On April 19, 2019, in a consensually recorded conversation, PARADIS met WRIGHT at **WRIGHT's PALM SPRINGS RESIDENCE** to further discuss some of the Target Offenses and criminal schemes. Amongst the topics was WRIGHT's future partnership with PARADIS in the formation of a new company, NEWCO,[58] to replace ARDENT. In addition, WRIGHT told PARADIS

[58] According to my interviews with PARADIS, NEWCO was a temporary company name that WRIGHT and PARADIS used to discuss the future iteration of the company that was AVENTADOR and is now ARDENT. Their plan is for NEWCO to replace ARDENT for

that he had a stack of documents to "cover his ass" related to the AVENTADOR contract in the event that the City Attorney's Office attempted to throw WRIGHT under the bus for any wrong doing. WRIGHT stated he maintained the stack of documents at **WRIGHT's RIVERSIDE RESIDENCE.** Based on my training, experience, and knowledge of this investigation, I believe WRIGHT meant that these documents contained evidence that certain City officials directed and approved the no-bid AVENTADOR contract.

3. PARADIS Continues to Meet with WRIGHT to Discuss the Criminal Schemes and Target Offenses[59]

80. Since April 19, 2019, in consensually recorded conversations, PARADIS has communicated and/or met with WRIGHT on multiple occasions. During these meetings, PARADIS and WRIGHT continued to discuss aspects of the criminal schemes and Target Offenses.

81. On May 14, 2019, in a consensually recorded conversation, PARADIS met WRIGHT at WRIGHT's son's apartment in downtown Los Angeles. Prior to the meeting, in a consensually recorded conversation, WRIGHT requested PARADIS to review/edit a presentation regarding the history and oversight of the

future contracts and add lucrative partnerships around the United States and with Israeli companies, thereby further enriching PARADIS and WRIGHT.

[59] I have not yet listened to the recordings referenced in this section given the volume of recordings and my other work responsibilities. The information outlined in this section was provided by PARADIS in his debrief to me after PARADIS conducted the consensual recordings. The debriefs included PARADIS' account of the substance of the recording at that time. However, based on my review of other recordings conducted by PARADIS, the debriefs he provided at that time related to those recordings, and other evidence I have obtained in the investigation, PARADIS' debriefs appear to be consistent with the recordings conducted. *See* fn 9.

AVENTADOR contract to be presented to the Mayor's Office, City Attorney's Office, and LADWP. During the meeting, PARADIS disclosed to WRIGHT that he intentionally omitted: (1) information related to WRIGHT's financial interest in AVENTADOR being awarded the contract and (2) the false regulatory reporting LADWP was engaged in related concerning its long running CIP violations, which thereby made it appear that WRIGHT was acting properly and prudently on behalf of LADWP. WRIGHT verbally acknowledged both items and agreed those items should be concealed in the presentation. In subsequent consensually recorded meetings with WRIGHT, WRIGHT agreed to conceal this information from the Mayor's Office, City Attorney's Office, and LADWP Board.

82. On May 18, 2019, in a consensually recorded meeting, PARADIS met WRIGHT at PARADIS Rancho Mirage residence. During the meeting PARADIS and WRIGHT discussed the presentation further. WRIGHT stated that he wanted to show PARADIS edits he had made, but that he had forgotten the presentation at **WRIGHT's RIVERSIDE RESIDENCE.** WRIGHT therefore requested PARADIS to meet him at **WRIGHT's RIVERSIDE RESISENCE** the following day. WRIGHT discussed an initial presentation that he had with City officials including Deputy Mayor Barbara Romero, staff members of the Mayor's Office, [redacted] (LADWP Assistant General Manager), Joe Brajevich, and LEVINE. According to WRIGHT, the first version of this presentation detailed the events at LADWP that led to the award of the contracts to PARADIS LAW GROUP and AVENTADOR. WRIGHT described the presentation as a thirty-seven

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

page blend of what WRIGHT and PARADIS drafted. WRIGHT stated that the presentation laid out the CC&B billing system problems that led WRIGHT to offer PARADIS the "Project Management" contract to lead the CC&B system remediation effort. In addition, the presentation included PARADIS's role in implementing the requirements of the Jones class action settlement and in remediation of cyber security issues. WRIGHT stated that he pointed out how many times people in the Mayor's Office, the City Attorney's Office, and the LADWP Board were informed of the circumstances involving these three areas and how they had all approved of PARADIS leading these efforts on a number of occasions. WRIGHT told PARADIS that Romero and the others in the Mayor's Office were quick to change course during his presentation and soon said that they now recalled these events and that these could not be dredged back up again because doing so would potentially hurt the Mayor's public opinion. Romero then said that the presentation should be made to the City Council Energy and Environmental Committee in closed session only and that the presentation needed to be cut down drastically to omit the background facts that led to PARADIS's appointment in the first place.

83. During this same meeting, WRIGHT and PARADIS discussed a cyber contract that would be subject to a request for proposal ("RFP") process and be awarded at the conclusion of ARDENT's current contract. WRIGHT instructed PARADIS to work with KWOK

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000198
Page 198 of 1425

and ALEXANDER to draft the RFP.[60] WRIGHT however did not want KWOK or ALEXANDER to know that PARADIS was in communication with WRIGHT because WRIGHT did not feel KWOK would lie under oath[61] for WRIGHT, regarding his communications with PARADIS, and WRIGHT did not trust ALEXANDER.

84. Regarding the Jones case, WRIGHT recalled being a part of a 2015 meeting with the City Attorney's Office and PARADIS in which CLARK directed PARADIS to "flip" Jones to LANDSKRONER so that the City could control the settlement and that CLARK was the one who quarterbacked the strategy and the settlement of the Jones case. In addition, WRIGHT recalled a meeting with CLARK, PARADIS, TUFARO, PETERS, and WRIGHT prior to CLARK's deposition testimony in which this strategy, orchestrated by CLARK, was discussed. WRIGHT said that CLARK is now lying to the court by saying he did not have knowledge of the Jones arrangements.

85. On May 20, 2019, in a consensually recorded conversation, PARADIS met WRIGHT at WRIGHT's son's apartment in downtown Los Angeles. During the meeting, PARADIS and WRIGHT further discussed the presentation for the Energy and Environmental Committee. In PARADIS's presence, WRIGHT spoke to LEVINE utilizing the **TARGET PHONES**. PARADIS overheard WRIGHT and LEVINE discussing strategy regarding what should and should

---

[60] Based on subsequent recorded conversations between PARADIS and KWOK and/or ALEXANDER, the new contract would be directly awarded by LADWP. The contract was expected to be a three-year contract totaling $75 million to $87.5 million.

[61] PARADIS believed this to mean KWOK would not lie under oath in the event he was deposed in any civil litigation related to Aventador/Ardent, or questioned by law enforcement about the same.

not be included in the closed E & E Committee presentation. After the call with LEVINE, WRIGHT and PARADIS discussed the presentation further and WRIGHT stated that LEVINE was going to request the same presentation in closed session to the LADWP Board.

86. On May 21, 2019, in a consensually recorded conversation, PARADIS met with KWOK to discuss the RFP. Included in the discussion was the evaluation criterion for who would be selected. KWOK started that he spoke to ALEXANDER about how they could control the evaluation team to ensure that they determine the outcome to guarantee that those entities they wanted to hire were certain of being selected. In a May 29, 2019 text message from **WRIGHT's BURNER PHONE**, WRIGHT instructed PARADIS to instruct KWOK and ALEXANDER to include WRIGHT as an evaluator. I believe WRIGHT wanted to be an evaluator to help ensure ARDENT/NEWCO (in which WRIGHT had a significant financial interest) received this future lucrative contract.

87. On May 26, 2019, PARADIS met with WRIGHT at **WRIGHT's PALM SPRINGS RESIDENCE**. PARADIS and WRIGHT primarily discussed a LADWP Cyber RFP[62] for additional cyber services. WRIGHT requested that PARADIS send the draft to KWOK and ALEXANDER so that they could in turn "officially" send the REF to WRIGHT for his approval. Based on my review of emails between PARADIS, KWOK, and ALEXANDER regarding the RFP, KWOK and ALEXANDER were aware that PARADIS was drafting the RFP directly with WRIGHT,

[62] WRIGHT, KWOK, and ALEXANDER requested PARADIS's assistance in drafting the RFP.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

indicating that the process was fixed and not an arms-length City process, as it should have been. In addition, WRIGHT admitted that LEVINE knew that PARADIS could have, but did not, report LEVINE for having improperly intervened in the debarment process involved PwC despite being recused and was appreciative of PARADIS concealing that fact. WRIGHT suggested that PARADIS could use LEVINE as a "front" ownership regarding CYBERGYM.

88. Based on the context of the conversation and my review of pen register data, I believe that WRIGHT is in communication with LEVINE and that the **TARGET PHONES** are utilized in this communication. It is notable to me that LEVINE and WRIGHT communicated with each other around the time PARADIS discussed with WRIGHT aspects of their criminal schemes and also discussed concealing LEVINE's role in the failed PwC debarment. Soon thereafter, LEVINE uncharacteristically (in that, LEVINE rarely communicated directly with PARADIS during this time) reached out to PARADIS. Based on my knowledge of this investigation, I believe this communication[63] was suspicious in that it may have reflected LEVINE's attempt to "feel out" PARADIS and whether PARADIS was going to disclose potentially damaging information.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

89. As used herein, the term "digital device" includes the **TARGET PHONES.**

90. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I

[63] I have reviewed this communication and the substance on its face consists only of innocuous well wishes regarding PARADIS's health.

know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

91. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000203
Page 203 of 1425

average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

92. Other than what has been described herein, to my knowledge, the United States has not attempted to review this data by other means.

VII. CONCLUSION

93. Based on the foregoing, I request that the Court issue the requested search warrants.

ANDREW CIVETTI, Special Agent
Federal Bureau of
Investigation

Subscribed to and sworn before me on June 4th, 2019.

Patrick J. Walsh

HONORABLE
UNITED STATES MAGISTRATE JUDGE

AO 93 (Rev. 11/13) Search and Seizure Warrant (USAO CDCA Rev. 04/17)

UNITED STATES DISTRICT COURT

for the

Central District of California

ORIGINAL

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	Case No. 2:19-MJ-02347
111 N. Hope Street #1603, Los Angeles, California	

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 6/4/19 5:30 p.m.

Patrick J. Walsh

Judge's signature

City and state: Los Angeles, CA

PATRICK J. WALSH

Printed name and title

AUSA: Melissa Mills x0627

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:19-MJ-02347	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-4

PROPERTY TO BE SEARCHED

The premises to be searched is the 15th Floor of the John Ferraro Building located at 111 N. Hope Street, Los Angeles, California, which is DAVID WRIGHT's employment ("**WRIGHT's OFFICE**"). Specifically, **WRIGHT's OFFICE** includes the office suite and conference room known as Room 1550. **WRIGHT's OFFICE** building is pictured below:

ATTACHMENT B-4

I. ITEMS TO BE SEIZED

1. Evidence of the criminal schemes and evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 666 (Bribery and Kickbacks Concerning Federal Funds), 1341 (Mail Fraud), 1343 (Wire Fraud), and 1346 (Deprivation of Honest Services), 1505 (Obstruction of Federal Proceeding), 1510 (Obstruction of Justice), 1951 (Extortion), and 1956 (Money Laundering) (collectively, the "Target Offenses"), occurring after February 1, 2015, namely:

a. Communications or agreements referencing: the Subjects identified in Section 3 of the Affidavit (the "Subjects");

b. Records, documents, programs, applications, or materials referencing:

xxv. DAVID WRIGHT's bank accounts, credit card accounts, other financial accounts, and wire transfer records;

xxvi. DAVID WRIGHT's calendar or date book, including calendars or date books stored on digital devices;

xxvii. Los Angeles Department of Water and Power contracts, proposed contracts, and contracting processes, including but not limited to any manipulations of contracting processes, the use of other entities to circumvent the requirement for open-bid contracts, and procedures and actions regarding debarment of vendors;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

xxviii. Any private business ventures in which a City official had a financial interest, including but not limited to AVENTADOR UTILITY SOLUTIONS, LLC, CYBERGYM, and ARDENT UTILITY SOLUTIONS, LLC;

xxix. Any lawsuit where the City was a party to the lawsuit and appears to have had a legal, representational, and/or financial interest in both sides of the lawsuit.

xxx. Financial payments, gifts, services, or other benefits given or offered to officials at LADWP or the City Attorney's Office or their staff or family members, or solicited by officials at LADWP or the City Attorney's Office or their staff or family members;

xxxi. Records, data, or other information required by or submitted to the Federal Energy Regulatory Commission ("FERC") or the North American Electric Reliability Corporation, Critical Infrastructure Protection ("NERC-CIP"); and

c. Cybersecurity vulnerabilities within the LADWP, including the City's power grid, water supply, and other critical infrastructure.

2. Law enforcement personnel are authorized to seize the cellular telephones with telephone numbers [redacted] ("**WRIGHT's PHONE**") and [redacted] ("**WRIGHT's BURNER PHONE**"), and any cellular phone in the possession of DAVID WRIGHT ("**TAREGT PHONES**" or the "digital devices").

3. During the execution of this search warrant, law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of DAVID WRIGHT onto the Touch ID sensor of the **TARGET PHONES**, or hold the **TARGET PHONES** in front of WRIGHT's face to activate the Face ID sensor, in order to gain access to the contents of any such device as authorized by this warrant. The government may not use more force than is reasonable to obtain this access.

4. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the Electronically Stored Information ("ESI") and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review and seize the ESI contained on the **TARGET PHONES** for evidence of the criminal schemes and evidence, contraband, fruits, and instrumentalities of Target Offenses, occurring after February 1, 2015, namely:

a. Items (a) through (c) above.

b. Evidence of who accessed or used the digital device, including records about their identities and whereabouts.

xxxii.

g. Any **TARGET PHONES** which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Target Offenses, and forensic copies thereof.

c. With respect to any **TARGET PHONES** used to facilitate the Target Offenses or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations;

ii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

iii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications or other text or written communications sent to or received from any digital device;

iv. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

v. evidence of the presence or absence of software that would allow others to control the device, such as

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

vi. evidence of the attachment of other devices;

vii. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

viii. evidence of the times the device was used;

ix. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

x. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

xi. records of or information about Internet Protocol addresses used by the device;

xii. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

5. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

6. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications, work product, or other potentially privileged communications:

7. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will review only digital device data which has been released by the Privilege Review Team.

8. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

9. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing

potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

10. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

11. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

12. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

13. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

14. If the search determines that a digital device does not contain any data falling within the list of items to be

seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

15. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

16. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

17. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

18. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

19. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

20. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

III. SEARCH PROCEDURE FOR DIGITAL DEVICES

21. In searching the **TARGET PHONES** or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any **TARGET PHONES** capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each **TARGET PHONES** where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the **TARGET PHONES** as soon as is practicable but not to exceed 180 days from the date of issuance of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each **TARGET PHONES** capable of containing any of the items to be seized to the search protocols to determine whether the **TARGET PHONES** and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques [, including to search for known images of child pornography.]

e. If the search team, while searching a **TARGET PHONES**, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that **TARGET PHONES** pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

f. If the search determines that a **TARGET PHONES** does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

the **TARGET PHONES** and delete or destroy all forensic copies thereof.

g. If the search determines that a **TARGET PHONES** does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the **TARGET PHONES** is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a **TARGET PHONES** if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the **TARGET PHONES**(S), the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

k. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000220
Page 220 of 1425

do not apply to any search of digital devices pursuant to any other court order.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AO 93 (Rev. 11/13) Search and Seizure Warrant (USAO CDCA Rev. 04/17)

UNITED STATES DISTRICT COURT

ORIGINAL

for the

Central District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

[redacted] Palm Springs, California

Case No. 2:19-MJ-02348

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for____days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 6/9/19 5:30 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

PATRICK J. WALSH
Printed name and title

AUSA: Melissa Mills x0627

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:19-MJ-02348	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-1

PROPERTY TO BE SEARCHED

The premises to be searched is a single-family residence located at [redacted], Palm Springs, California which is a residence of DAVID WRIGHT ("**WRIGHT's PALM SPRINGS RESIDENCE**"). **WRIGHT's PALM SPRINGS RESIDENCE** is pictured below:

ATTACHMENT B-1

I. CELL PHONE ITEMS TO BE SEIZED

1. Law enforcement personnel are authorized to seize the cellular telephones with telephone numbers [redacted] ("**WRIGHT's PHONE**") and [redacted] ("**WRIGHT's BURNER PHONE**"), and any cellular phone in the possession of DAVID WRIGHT ("**TAREGT PHONES**" or the "digital devices").

2. During the execution of this search warrant, law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of DAVID WRIGHT onto the Touch ID sensor of the **TARGET PHONES**, or hold the **TARGET PHONES** in front of WRIGHT's face to activate the Face ID sensor, in order to gain access to the contents of any such device as authorized by this warrant. The government may not use more force than is reasonable to obtain this access.

3. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the Electronically Stored Information ("ESI") and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review and seize the ESI contained on the **TARGET PHONES** for evidence of the criminal schemes and evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 666 (Bribery and Kickbacks Concerning Federal

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Funds), 1341 (Mail Fraud), 1343 (Wire Fraud), and 1346 (Deprivation of Honest Services), 1505 (Obstruction of Federal Proceeding), 1510 (Obstruction of Justice), 1951 (Extortion), and 1956 (Money Laundering) (collectively, the "Target Offenses"), occurring after February 1, 2015, namely:

a. Evidence of who accessed or used the digital device, including records about their identities and whereabouts.

b. Communications or agreements on or after February 1, 2015, referencing: the Subjects identified in Section 3 of the Affidavit (the "Subjects").

c. Records, documents, programs, applications, or materials from on or after February 1, 2015, referencing:

i. DAVID WRIGHT's bank accounts, credit card accounts, other financial accounts, and wire transfer records;

ii. DAVID WRIGHT's calendar or date book, including calendars or date books stored on digital devices;

iii. Los Angeles Department of Water and Power contracts, proposed contracts, and contracting processes, including but not limited to any manipulations of contracting processes, the use of other entities to circumvent the requirement for open-bid contracts, and procedures and actions regarding debarment of vendors;

iv. Any private business ventures in which a City official had a financial interest, including but not limited to AVENTADOR UTILITY SOLUTIONS, LLC, CYBERGYM, and ARDENT UTILITY SOLUTIONS, LLC;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000226
Page 226 of 1425

v. Any lawsuit where the City was a party to the lawsuit and appears to have had a legal, representational, and/or financial interest in both sides of the lawsuit.

vi. Financial payments, gifts, services, or other benefits given or offered to officials at LADWP or the City Attorney's Office or their staff or family members, or solicited by officials at LADWP or the City Attorney's Office or their staff or family members;

vii. Records, data, or other information required by or submitted to the Federal Energy Regulatory Commission ("FERC") or the North American Electric Reliability Corporation, Critical Infrastructure Protection ("NERC-CIP"); and

viii. Cybersecurity vulnerabilities within the LADWP, including the City's power grid, water supply, and other critical infrastructure.

d. Any **TARGET PHONES** which is itself or which contains evidence, contraband, fruits, or instrumentalities of the criminal schemes and evidence of the Target Offenses, and forensic copies thereof.

e. With respect to any **TARGET PHONES** used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations;

ii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

iii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications or other text or written communications sent to or received from any digital device;

iv. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

v. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

vi. evidence of the attachment of other devices;

vii. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000228
Page 228 of 1425

viii. evidence of the times the device was used;

ix. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

x. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

xi. records of or information about Internet Protocol addresses used by the device;

xii. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

5. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications, work product, or other potentially privileged communications:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

6. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will review only digital device data which has been released by the Privilege Review Team.

7. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

8. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

9. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000230
Page 230 of 1425

Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

10. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

11. In performing the reviews, both the Privilege Review Team and the Search Team may:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

12. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

13. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

14. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

15. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000232
Page 232 of 1425

within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

16. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

17. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

18. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000233
Page 233 of 1425

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

19. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

III. SEARCH PROCEDURE FOR DIGITAL DEVICES

20. In searching the **TARGET PHONES** or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any **TARGET PHONES** capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each **TARGET PHONES** where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the **TARGET PHONES** as soon as is practicable but not to exceed 180 days from the date of issuance of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each **TARGET PHONES** capable of containing any of the items to be seized to the search protocols to determine whether the **TARGET PHONES** and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques [, including to search for known images of child pornography.]

e. If the search team, while searching a **TARGET PHONES**, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that **TARGET PHONES** pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

f. If the search determines that a **TARGET PHONES** does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the **TARGET PHONES** and delete or destroy all forensic copies thereof.

g. If the search determines that a **TARGET PHONES** does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the **TARGET PHONES** is (1) itself an item to be seized and/or (2) contains data

falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a **TARGET PHONES** if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the **TARGET PHONES**(S), the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

k. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AO 93 (Rev. 11/13) Search and Seizure Warrant (USAO CDCA Rev. 04/17)

UNITED STATES DISTRICT COURT

for the

Central District of California

ORIGINAL

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

[redacted], Riverside, California

Case No. 2:19-MJ-02349

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 6/4/19 5:30 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

PATRICK J. WALSH
Printed name and title

AUSA: Melissa Mills x0627

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:19-MJ-02349	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-3

PROPERTY TO BE SEARCHED

The premises to be searched is a single-family residence located at [redacted], Riverside, California, which is a residence of DAVID WRIGHT ("**WRIGHT's RIVERSIDE RESIDENCE**"). **WRIGHT's RIVERSIDE RESIDENCE** is pictured below:

ATTACHMENT B-3

I. ITEMS TO BE SEIZED

1. Evidence of the criminal schemes and evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 666 (Bribery and Kickbacks Concerning Federal Funds), 1341 (Mail Fraud), 1343 (Wire Fraud), and 1346 (Deprivation of Honest Services), 1505 (Obstruction of Federal Proceeding), 1510 (Obstruction of Justice), 1951 (Extortion), and 1956 (Money Laundering) (collectively, the "Target Offenses"), occurring after February 1, 2015, namely:

a. Communications or agreements referencing: the Subjects identified in Section 3 of the Affidavit (the "Subjects");

b. Records, documents, programs, applications, or materials referencing:

xvii. DAVID WRIGHT's bank accounts, credit card accounts, other financial accounts, and wire transfer records;

xviii. DAVID WRIGHT's calendar or date book, including calendars or date books stored on digital devices;

xix. Los Angeles Department of Water and Power contracts, proposed contracts, and contracting processes, including but not limited to any manipulations of contracting processes, the use of other entities to circumvent the requirement for open-bid contracts, and procedures and actions regarding debarment of vendors;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

xx. Any private business ventures in which a City official had a financial interest, including but not limited to AVENTADOR UTILITY SOLUTIONS, LLC, CYBERGYM, and ARDENT UTILITY SOLUTIONS, LLC;

xxi. Any lawsuit where the City was a party to the lawsuit and appears to have had a legal, representational, and/or financial interest in both sides of the lawsuit.

xxii. Financial payments, gifts, services, or other benefits given or offered to officials at LADWP or the City Attorney's Office or their staff or family members, or solicited by officials at LADWP or the City Attorney's Office or their staff or family members;

xxiii. Records, data, or other information required by or submitted to the Federal Energy Regulatory Commission ("FERC") or the North American Electric Reliability Corporation, Critical Infrastructure Protection ("NERC-CIP"); and

c. Cybersecurity vulnerabilities within the LADWP, including the City's power grid, water supply, and other critical infrastructure.

2. Law enforcement personnel are authorized to seize the cellular telephones with telephone numbers [redacted] ("**WRIGHT's PHONE**") and [redacted] ("**WRIGHT's BURNER PHONE**"), and any cellular phone in the possession of DAVID WRIGHT ("**TAREGT PHONES**" or the "digital devices").

3. During the execution of this search warrant, law enforcement personnel are authorized to depress the fingerprints

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

and/or thumbprints of DAVID WRIGHT onto the Touch ID sensor of the **TARGET PHONES**, or hold the **TARGET PHONES** in front of WRIGHT's face to activate the Face ID sensor, in order to gain access to the contents of any such device as authorized by this warrant. The government may not use more force than is reasonable to obtain this access.

4. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the Electronically Stored Information ("ESI") and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review and seize the ESI contained on the **TARGET PHONES** for evidence of the criminal schemes and evidence, contraband, fruits, and instrumentalities of Target Offenses, occurring after February 1, 2015, namely:

a. Items (a) through (c) above.

b. Evidence of who accessed or used the digital device, including records about their identities and whereabouts.

xxiv.

f. Any **TARGET PHONES** which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Target Offenses, and forensic copies thereof.

c. With respect to any **TARGET PHONES** used to facilitate the Target Offenses or containing evidence falling

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

within the scope of the foregoing categories of items to be seized:

i. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations;

ii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

iii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications or other text or written communications sent to or received from any digital device;

iv. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

v. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

as well as evidence of the presence or absence of security software designed to detect malicious software;

vi. evidence of the attachment of other devices;

vii. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

viii. evidence of the times the device was used;

ix. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

x. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

xi. records of or information about Internet Protocol addresses used by the device;

xii. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

5. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

6. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications, work product, or other potentially privileged communications:

7. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will review only digital device data which has been released by the Privilege Review Team.

8. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

9. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

10. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

11. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_000247
Page 247 of 1425

concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

12. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

13. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

14. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

15. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

16. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

17. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

18. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

19. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_000249
Page 249 of 1425

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

20. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

apply to any search of digital devices pursuant to any other court order.

III. SEARCH PROCEDURE FOR DIGITAL DEVICES

21. In searching the **TARGET PHONES** or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any **TARGET PHONES** capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each **TARGET PHONES** where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the **TARGET PHONES** as soon as is practicable but not to exceed 180 days from the date of issuance of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each **TARGET PHONES** capable of containing any of the items to be seized to the search protocols to determine whether

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_000251
Page 251 of 1425

the **TARGET PHONES** and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques [, including to search for known images of child pornography.]

e. If the search team, while searching a **TARGET PHONES**, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that **TARGET PHONES** pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

f. If the search determines that a **TARGET PHONES** does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the **TARGET PHONES** and delete or destroy all forensic copies thereof.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_000252
Page 252 of 1425

g. If the search determines that a **TARGET PHONES** does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the **TARGET PHONES** is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a **TARGET PHONES** if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the **TARGET PHONES**(S), the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

k. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_000253
Page 253 of 1425

AO 93 (Rev. 11/13) Search and Seizure Warrant (USAO CDCA Rev. 04/17)

UNITED STATES DISTRICT COURT

for the

Central District of California

ORIGINAL

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

[redacted] Riverside, California

Case No. 2:19-MJ-02349

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 6/18/19 3:45 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

PATRICK J. WALSH, U.S. MAGISTRATE JUDGE
Printed name and title

AUSA: Melissa Mills x0627

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:19-MJ-02349	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

PROPERTY TO BE SEARCHED

The premises to be searched is a single-family residence located at [redacted], Riverside, California, which is a residence of DAVID WRIGHT ("**WRIGHT's RIVERSIDE RESIDENCE**"). **WRIGHT's RIVERSIDE RESIDENCE** is pictured below:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. Evidence of the criminal schemes and evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 666 (Bribery and Kickbacks Concerning Federal Funds), 1341 (Mail Fraud), 1343 (Wire Fraud), and 1346 (Deprivation of Honest Services), 1505 (Obstruction of Federal Proceeding), 1510 (Obstruction of Justice), 1951 (Extortion), and 1956 (Money Laundering) (collectively, the "Target Offenses"), occurring after February 1, 2015, namely:

a. Communications or agreements referencing: the Subjects identified in Section 3 of the Affidavit (the "Subjects");

b. Records, documents, programs, applications, or materials referencing:

i. DAVID WRIGHT's bank accounts, credit card accounts, other financial accounts, and wire transfer records;

ii. DAVID WRIGHT's calendar or date book, including calendars or date books stored on digital devices;

iii. Los Angeles Department of Water and Power contracts, proposed contracts, and contracting processes, including but not limited to any manipulations of contracting processes, the use of other entities to circumvent the requirement for open-bid contracts, and procedures and actions regarding debarment of vendors;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

iv. Any private business ventures in which a City official had a financial interest, including but not limited to AVENTADOR UTILITY SOLUTIONS, LLC, CYBERGYM, and ARDENT UTILITY SOLUTIONS, LLC;

v. Any lawsuit where the City was a party to the lawsuit and appears to have had a legal, representational, and/or financial interest in both sides of the lawsuit.

vi. Financial payments, gifts, services, or other benefits given or offered to officials at LADWP or the City Attorney's Office or their staff or family members, or solicited by officials at LADWP or the City Attorney's Office or their staff or family members;

vii. Records, data, or other information required by or submitted to the Federal Energy Regulatory Commission ("FERC") or the North American Electric Reliability Corporation, Critical Infrastructure Protection ("NERC-CIP"); and

c. Cybersecurity vulnerabilities within the LADWP, including the City's power grid, water supply, and other critical infrastructure.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

2. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications, work product, or other potentially privileged communications:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

3. The Privilege Review Team will review the identified materials as set forth herein. The Search Team will review only materials which have been released by the Privilege Review Team.

4. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the materials beyond this 180-day period without obtaining an extension of time order from the Court.

5. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_000259
Page 259 of 1425

6. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AO 93 (Rev. 11/13) Search and Seizure Warrant (USAO CDCA Rev. 04/17)

UNITED STATES DISTRICT COURT

ORIGINAL

for the

Central District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

DAVID WRIGHT, date of birth [redacted]1960, [redacted], Riverside, California

Case No. 2:19-MJ-02350

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for____days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 6/4/19 5:30 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

PATRICK J. WALSH
Printed name and title

AUSA: Melissa Mills x0627

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:19-MJ-02350	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

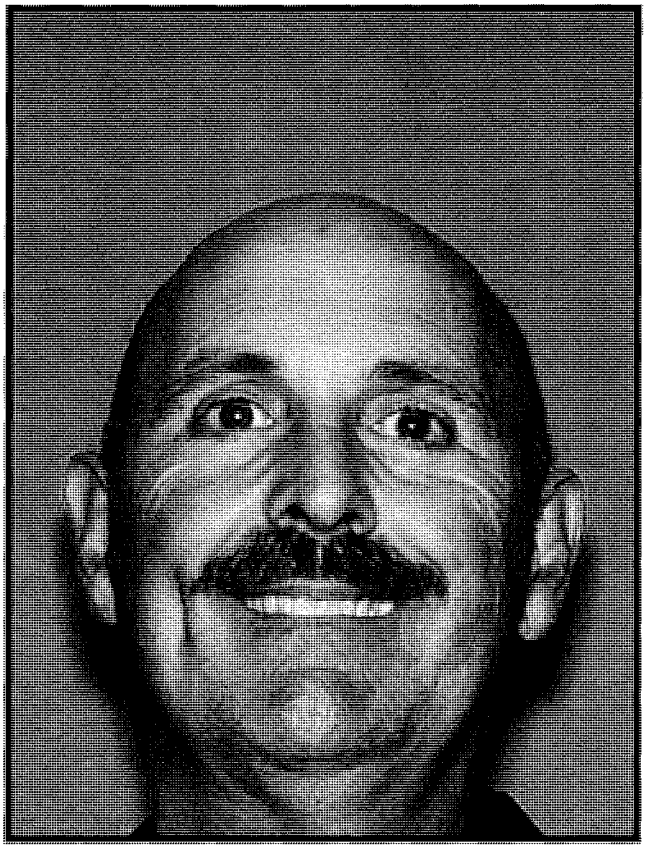
_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-2

PERSON TO BE SEARCHED

The person to be searched is **DAVID WRIGHT**, date of birth [redacted]/1960, as pictured below:



ATTACHMENT B-2

I. CELL PHONE ITEMS TO BE SEIZED

1. Law enforcement personnel are authorized to seize the cellular telephones with telephone numbers [redacted] ("**WRIGHT's PHONE**") and [redacted] ("**WRIGHT's BURNER PHONE**"), and any cellular phone in the possession of DAVID WRIGHT ("**TAREGT PHONES**" or the "digital devices").

2. During the execution of this search warrant, law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of DAVID WRIGHT onto the Touch ID sensor of the **TARGET PHONES**, or hold the **TARGET PHONES** in front of WRIGHT's face to activate the Face ID sensor, in order to gain access to the contents of any such device as authorized by this warrant. The government may not use more force than is reasonable to obtain this access.

3. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the Electronically Stored Information ("ESI") and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review and seize the ESI contained on the **TARGET PHONES** for evidence of the criminal schemes and evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 666 (Bribery and Kickbacks Concerning Federal

Funds), 1341 (Mail Fraud), 1343 (Wire Fraud), and 1346 (Deprivation of Honest Services), 1505 (Obstruction of Federal Proceeding), 1510 (Obstruction of Justice), 1951 (Extortion), and 1956 (Money Laundering) (collectively, the "Target Offenses"), occurring after February 1, 2015, namely:

a. Evidence of who accessed or used the digital device, including records about their identities and whereabouts.

b. Communications or agreements on or after February 1, 2015, referencing: the Subjects identified in Section 3 of the Affidavit (the "Subjects").

c. Records, documents, programs, applications, or materials from on or after February 1, 2015, referencing:

ix. DAVID WRIGHT's bank accounts, credit card accounts, other financial accounts, and wire transfer records;

x. DAVID WRIGHT's calendar or date book, including calendars or date books stored on digital devices;

xi. Los Angeles Department of Water and Power contracts, proposed contracts, and contracting processes, including but not limited to any manipulations of contracting processes, the use of other entities to circumvent the requirement for open-bid contracts, and procedures and actions regarding debarment of vendors;

xii. Any private business ventures in which a City official had a financial interest, including but not limited to AVENTADOR UTILITY SOLUTIONS, LLC, CYBERGYM, and ARDENT UTILITY SOLUTIONS, LLC;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000265
Page 265 of 1425

xiii. Any lawsuit where the City was a party to the lawsuit and appears to have had a legal, representational, and/or financial interest in both sides of the lawsuit.

xiv. Financial payments, gifts, services, or other benefits given or offered to officials at LADWP or the City Attorney's Office or their staff or family members, or solicited by officials at LADWP or the City Attorney's Office or their staff or family members;

xv. Records, data, or other information required by or submitted to the Federal Energy Regulatory Commission ("FERC") or the North American Electric Reliability Corporation, Critical Infrastructure Protection ("NERC-CIP"); and

xvi. Cybersecurity vulnerabilities within the LADWP, including the City's power grid, water supply, and other critical infrastructure.

e. Any **TARGET PHONES** which is itself or which contains evidence, contraband, fruits, or instrumentalities of the criminal schemes and evidence of the Target Offenses, and forensic copies thereof.

f. With respect to any **TARGET PHONES** used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000266
Page 266 of 1425

ii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

iii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications or other text or written communications sent to or received from any digital device;

iv. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

v. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

vi. evidence of the attachment of other devices;

vii. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000267
Page 267 of 1425

viii. evidence of the times the device was used;

ix. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

x. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

xi. records of or information about Internet Protocol addresses used by the device;

xii. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

21. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications, work product, or other potentially privileged communications:

22. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will review only digital device data which has been released by the Privilege Review Team.

23. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

24. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

25. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000269
Page 269 of 1425

Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

26. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

27. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

28. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

29. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

30. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

31. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000271
Page 271 of 1425

within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

32. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

33. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

34. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000272
Page 272 of 1425

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

35. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

III. SEARCH PROCEDURE FOR DIGITAL DEVICES

36. In searching the **TARGET PHONES** or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any **TARGET PHONES** capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each **TARGET PHONES** where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the **TARGET PHONES** as soon as is practicable but not to exceed 180 days from the date of issuance of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each **TARGET PHONES** capable of containing any of the items to be seized to the search protocols to determine whether the **TARGET PHONES** and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000274
Page 274 of 1425

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques [, including to search for known images of child pornography.]

e. If the search team, while searching a **TARGET PHONES**, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that **TARGET PHONES** pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

f. If the search determines that a **TARGET PHONES** does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the **TARGET PHONES** and delete or destroy all forensic copies thereof.

g. If the search determines that a **TARGET PHONES** does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the **TARGET PHONES** is (1) itself an item to be seized and/or (2) contains data

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000275
Page 275 of 1425

falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a **TARGET PHONES** if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the **TARGET PHONES**(S), the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

k. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

UNITED STATES DISTRICT COURT

for the

Central District of California

ORIGINAL

In the Matter of the Search of:
Information associated with account identified as [redacted] that is within the possession, custody, or control of Gibson, Dunn & Crutcher LLP

Case No. 2:19-MJ-02351

WARRANT PURSUANT TO 18 U.S.C. § 2703

To: Any Authorized Law Enforcement Officer

An application by a federal law enforcement officer requests the production and search of the following data:

See Attachment A

The data to be produced and searched, described above, are believed to contain the following:

See Attachment B

I find that the affidavit, or any recorded testimony, establishes probable cause to produce and search the data described in Attachment A, and to seize the data described in Attachment B. Such affidavit is incorporated herein by reference.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE HEREBY COMMANDED to serve this warrant on Gibson, Dunn & Crutcher LLP in the daytime, between the hours of 6:00 a.m. and 10:00 p.m., within 14 days from the date of its issuance.

GIBSON DUNN & CRUTCHER LLP IS HEREBY COMMANDED to produce the information described in Attachment A within 10 calendar days of the date of service of this order. **GIBSON DUNN & CRUTCHER LLP IS FURTHER COMMANDED** to comply with the further orders set forth in Attachment B, and, pursuant to 18 U.S.C. § 2705(b), shall not notify any person, including the subscriber(s) of the account/s identified in Attachment A, of the existence of this warrant.

The officer executing this warrant, or an officer present during the execution, shall prepare an inventory as required by law, and shall promptly return this warrant and the inventory to the United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE FURTHER COMMANDED to perform the search of the data provided by Gibson, Dunn & Crutcher LLP pursuant to the procedures set forth in Attachment B.

Date and time issued: 6/4/19 5:30 p.m. Patrick J. Walsh

Judge's signature

City and State: L.A., CA

Patrick J. Walsh, U.S. Magistrate Judge

Printed name and title

AUSA: Melissa Mills x0627

Return	
Case No: 2:19-MJ-02351	*Date and time warrant served on provider:*
Inventory made in the presence of:	
Inventory of data seized: [Please provide a description of the information produced.]	

Certification

I declare under penalty of perjury that I am an officer involved in the execution of this warrant, and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the **SUBJECT ACCOUNT** identified as [redacted] that is within the possession, custody, or control of Gibson, Dunn & Crutcher LLP, a company that accepts service of legal process at 333 South Grand Avenue, Los Angeles, California, regardless of where such information is stored, held, or maintained.

ATTACHMENT B

ITEMS TO BE SEIZED

I. SEARCH PROCEDURE INCLUDING PRIVILEGE REVIEW PROCEDURE

1. The search warrant will be presented to personnel of Gibson Dunn & Crutcher LLP (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide the Section II information in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below in Section IV.

4. The government has designated multiple attorneys and multiple agents not participating in the investigation of the case to review potentially privileged materials (collectively, the "Privilege Review Team"), filter out privileged materials, and provide only unprivileged materials to law enforcement personnel conducting the investigation (collectively, the "Investigative Team").

5. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.13.a. below), members of the Privilege Review Team will review the content records using search protocols described herein. With respect to the non-content information produced by the PROVIDER (see Section II.14.b. below), no privilege review need be performed and the Investigative Team may review immediately.

6. The Privilege Review Team will conduct an initial review of all of the content records using search protocols specifically chosen to identify content records containing potentially privileged information. Content records that are identified by this initial review as not potentially privileged may be given to the Investigation Team.

7. Content records determined by this review to be potentially privileged will be reviewed by a Privilege Review Team attorney. Content records identified by the Privilege Review Team attorney after review as not potentially privileged may be given to the Investigative Team. If, after review, the Privilege Review Team attorney determines it to be appropriate, the Privilege Review Team attorney may apply to the court for a finding with respect to particular content records that no privilege, or an exception to the privilege, applies. Content records that are the subject of such a finding may be given to

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

the Investigative Team. Content records identified as privileged by the reviewing Privilege Review Team attorney review will be maintained under seal by the Privilege Review Team without further review, absent subsequent authorization.

8. The Investigative Team will search only the content records that the Privilege Review Team provides to the Investigative Team at any step listed above in order to locate, extract and seize content records that are within the scope of the search warrant (see Section III below). The Investigative Team does not have to wait until the entire privilege review is concluded to begin its review for content records within the scope of the search warrant. The Privilege Review Team may also conduct the search for content records within the scope of the search warrant if that is more efficient. The search may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

9. If, while reviewing content records or non-content information, either the Privilege Review Team or the Investigative Team encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime

was encountered, including how it was immediately apparent contraband or evidence of a crime.

10. The Privilege Review Team and the Investigative Team will complete the search of non-content information and both stages of the search of the content records discussed herein as soon as is practicable but not to exceed 180 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the records beyond this 180-day period without first obtaining an extension of time order from the Court.

11. Once the Privilege Review Team and the Investigative Team have completed their review of the non-content information and the content records and the Investigative Team has created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the Investigative Team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, neither the Privilege Review Team nor the Investigative Team will access the data from the sealed original production which fell outside the scope of the items to be seized or was determined to be privileged absent further order of the Court.

12. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant

to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

13. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDER

14. To the extent that the information described in Attachment A is within the possession, custody, or control of the PROVIDER, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each **SUBJECT ACCOUNT** listed in Attachment A:

a. All contents of all wire and electronic communications associated with the **SUBJECT ACCOUNT**, limited to that which occurred on or after January 1, 2013, including:

i. All e-mails, communications, or messages of any kind associated with the **SUBJECT ACCOUNT**, including stored or preserved copies of messages sent to and from the account, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information associated with each e-mail or message, and any related documents or attachments.

ii. All records pertaining to communications between the PROVIDER and any person regarding the **SUBJECT**

ACCOUNT, including contacts with support services and records of actions taken.

b. All other records and information, including:

i. All user connection logs and transactional information of all activity relating to the **SUBJECT ACCOUNT** described above in Section II.13.a., including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations.

ii. All subscriber information pertaining to the **SUBJECT ACCOUNT**, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), other account names or e-mail addresses associated with the account, telephone numbers, physical addresses, and other identifying information regarding the subscriber, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

15. For each **SUBJECT ACCOUNT** listed in Attachment A, the Search Team may seize:

c. All information described above in Section II.13.a. that constitutes evidence, contraband, fruits, or

instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 666 (Bribery and Kickbacks Concerning Federal Funds), 1341 (Mail Fraud), 1343 (Wire Fraud), and 1346 (Deprivation of Honest Services), those violations involving JAMES CLARK and other subjects and occurring after January 1, 2013, namely:

i. Information relating to who created, accessed, or used the **SUBJECT ACCOUNT**, including records about their identities and whereabouts.

ii. Collusive litigation strategies in any case involving the City of Los Angeles, including but not limited to actual or contemplated lawsuits arising from LADWP billing problems beginning in 2013;

iii. Knowledge or approval of representation by City officials, including but not limited to Special Counsel on behalf of the City, of litigants adverse to the City in any actual, contemplated, or threatened litigation;

iv. Knowledge, approval, or receipt of, or other involvement in, any bribes, kickbacks, benefits, or unauthorized payments to City officials, including but not limited to Special Counsel on behalf of the City;

v. Meeting agendas, meeting minutes, calendar invites, voice-mail messages, document links, draft documents, related to the above.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

d. All records and information described above in Sections II.13.b.

IV. PROVIDER PROCEDURES

16. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. The PROVIDER shall send such information to:

[redacted]

17. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

18. IT IS FURTHER ORDERED that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A, of the existence of the warrant.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

COPY [redacted]

FILED
CLERK, U.S. DISTRICT COURT
JUN - 4 2019
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

TRACY L. WILKISON
Attorney for the United States,
Acting Under Authority Conferred By 28 U.S.C. § 515
SCOTT GARRINGER
Assistant United States Attorney
Deputy Chief, Criminal Division
MACK E. JENKINS (Cal. Bar No. 242101)
Assistant United States Attorney
Chief, Public Corruption & Civil Rights Section
MELISSA MILLS (Cal. Bar No. 248529)
Assistant United States Attorney
Public Corruption and Civil Rights Section
DIANA KWOK (Cal. Bar No. 246366)
Assistant United States Attorney
Environmental and Community Safety Crimes Section
1500 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-0627
Facsimile: (213) 894-2927
E-mail: Melissa.Mills@usdoj.gov

Attorneys for Applicant
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

IN RE CELLULAR TELEPHONE	No. 2:19-mj-02372 GOVERNMENT'S *EX PARTE* APPLICATION FOR A WARRANT AUTHORIZING (1) THE DISCLOSURE OF GPS AND CELL-SITE INFORMATION AND (2) USE OF CELL-SITE SIMULATOR; REQUEST TO SEAL; AFFIDAVIT OF ANDREW CIVETTI **(UNDER SEAL)**

I. INTRODUCTION

The United States of America, by and through its counsel of record, the United States Attorney for the Central District of California, hereby applies for a warrant requiring cellular telephone service provider(s) to furnish the Federal Bureau of Investigation (the "Investigating Agency") with information relating to the following cellular telephone: [redacted], a cellular telephone

issued by provider Verizon, subscribed to by an as-yet unidentified person, and believed to be used by Melton Edises Levine (the "**Subject Telephone**").

Authorization is sought to obtain prospective cell-site information, as well as the physical location of the **Subject Telephone**, to include E-911 Phase II data and latitude and longitude data gathered for the **Subject Telephone**, including Global Positioning Satellite and/or network timing information, including Sprint's Per Call Measurement Data, Verizon's Real Time Tool, AT&T's Network Event Location System and T-Mobile's True Call data, and including information from such programs as Nextel Mobile Locator, Boost Mobile Loopt, Sprint/Nextel Findum Wireless, which will establish the approximate location of the **Subject Telephone**, and which information is acquired in the first instance by the Carrier ("GPS information"), at such intervals and times as the government may request, and the furnishing of all information, facilities, and technical assistance necessary to accomplish said disclosure unobtrusively, for a period of 45 days.

Additionally, this application seeks authorization for the Investigating Agency to use a cell-site simulator, commonly referred to as a "Stingray," in order to obtain dialing, routing, addressing, or signaling information (but not content) from the **Subject Telephone**, whether in use or not.

The application is made in connection with an investigation of offenses committed by PAUL PARADIS, DAVID WRIGHT, JAMES P. CLARK, THOMAS PETERS, WILLIAM FUNDERBURK, and others known and unknown (the "Target Subjects"), specifically, violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds);

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

1341 (Mail Fraud); 1343 (Wire Fraud); and 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); 16 U.S.C. §§ 824o, 825o (Electric Reliability Standards) (collectively, the "Target Offenses"), and is based upon the attached agent affidavit. There is probable cause to believe that federal crimes are being committed and that the information likely to be received concerning the approximate location of the **Subject Telephone**, currently within, or being monitored or investigated within, the Central District of California, will constitute or yield evidence of those crimes.

II. CELL SITE AND GPS INFORMATION FROM THE CARRIER(S)

The information sought by this application includes information about the location (physical address) of the "cell-sites" linked to the **Subject Telephone** at call origination (for outbound calling), call termination (for incoming calls), and, if reasonably available, during the progress of a call. This information, which is acquired in the first instance by the Carrier, includes any information, apart from the content of any communication, that is reasonably available to the Carrier and that is requested by the Investigating Agency, concerning the cell-sites/sectors receiving and transmitting signals to and from the **Subject Telephone** whether or not a call is in progress. This prospective information is sought based on 18 U.S.C. § 2701 et seq. (the "Stored Communications Act"). The Stored Communications Act provides:

> A governmental entity may require a provider of electronic communication service...to disclose a record or other information pertaining to a subscriber to or customer of

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

such service (not including the contents of communications) only[1] when the governmental entity --

> (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure...by a court of competent jurisdiction[.]

18 U.S.C. § 2703(c)(1); see also Carpenter v. United States, 138 S. Ct. 2206, (2018) (holding that a warrant is required to obtain seven or more days' worth of historical cell-site information).[2]

Prospective cell-site information is also sought based on the authority of 18 U.S.C. § 3121 et seq. (the "Pen Register Statute").[3]

---

[1] This section also provides other methods to compel disclosure, including via subpoena or court order. However, the government in this case is proceeding under the highest threshold, that is, obtaining a warrant as described in § 2703(c)(1)(A).

[2] The definition of terms in the Stored Communications Act makes clear that the "record or other information" that a court may order a provider to disclose to the government under Section 2703(c)(1)(A) includes both cell site and other location information. First, the Stored Communications Act expressly adopts the definition of statutory terms set forth in 18 U.S.C. § 2510. See 18 U.S.C. § 2711 ("As used in this chapter. . . (1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section"). Thus, the term "provider of electronic communication service" used in Section 2703(c) covers cellular telephone service providers, because 18 U.S.C. § 2510(15) defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Further, cell site and other location information is "a record or other information pertaining to a subscriber to or customer of" an electronic communications service – another term used in Section 2703(c) – because cellular telephone service providers receive and store the information, if sometimes only momentarily, before forwarding it to law enforcement officials. See In Re: Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F. Supp. 2d 448, 457-60 (S.D.N.Y. 2006). Finally, this Court is a "court of competent jurisdiction" because it is a "district court of the United States (including a magistrate judge of such a court)... that...has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

[3] 18 U.S.C. § 3127(3) defines "pen register" as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

The government therefore also complies with the provisions of that statute, including by providing the required certification by the attorney for the government at the end of this application. Pursuant to the Pen Register Statute, upon an application made under 18 U.S.C. § 3122(a)(1) a court "shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." 18 U.S.C. § 3123(a)(1).[4]

Cellular telephone companies routinely create and maintain, in the regular course of their business, records of information concerning their customers' usage. These records typically include for each communication a customer makes or receives (1) the date and time of the communication; (2) the telephone numbers involved; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer was connected at the end of the communication; and (5) the duration of the communication. The records may also, but do not always, specify a particular sector of a cell tower used to transmit a communication. Cell-site information is useful to law enforcement because of the

---

however, that such information shall not include the contents of any communication." A "trap and trace" device is similarly defined for any device or process which captures incoming data. See 18 U.S.C. § 3127(4).

[4] While 47 U.S.C. § 1002, which is part of the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"), would preclude seeking physical location information based on the Pen Register Statute alone, the Stored Communications Act provides the requisite additional authority for this Court to authorize the production by the Carrier of cell-site information to the government.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

limited information it provides about the general location of a cell phone when a communication is made.

This application also seeks GPS information for the **Subject Telephone**, which is sought based on 18 U.S.C. § 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41. As discussed above, data that provides information about the location of a customer's phone falls within 18 U.S.C. § 2703(c)'s definition of "a record or other information pertaining to a subscriber to or customer of [an electronic communication service]." Thus, the United States may obtain a warrant requiring a cell phone company to disclose GPS information "using the procedures described in the Federal Rules of Criminal Procedure," that is, Federal Rule of Criminal Procedure 41, as is contemplated by this application and order.

Some, but not all, cellular telephone service providers have the technical means to obtain GPS information. GPS information is not generated specifically for law enforcement, but is the product of United States Federal Communications Commission requirements that cellular telephone service providers maintain and access location information for emergency responders. To obtain GPS information, a "ping" (electronic signal) is sent to the cellular telephone, which unobtrusively activates the GPS chip in the telephone. This information is not provided in a streaming fashion regardless of the cellular telephone activity, but instead is sent only in response to specific law-enforcement agency requests. Location data through GPS information can be delivered as accurately as within three meters; however, if the cellular telephone is in motion, such as while in a moving vehicle, the error range in meters may be greater, or the cellular telephone service provider may simply provide cell-site

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

information. In addition, the cellular telephone must be powered on and, usually, not in the middle of a telephone call, for GPS information to be obtained. Moreover, if the cellular telephone is inside a building, or is in some other way blocked from the satellite, GPS information may not be obtainable. In such cases, the service provider will often provide law enforcement with cell-site information instead.

III. CELL-SITE SIMULATOR

This application also seeks a warrant authorizing the Investigating Agency to use a cell-site simulator, commonly referred to as a "Stingray," to obtain dialing, routing, addressing, or signaling information from the **Subject Telephone**, whether in use or not. This device simulates a cell site, and by combination of surveillance and action as a mobile cell site, allows the Investigating Agency to locate the **Subject Telephone** more conclusively. This Court has authority to issue the requested warrant under Fed. R. Crim. P. 41(b)(1) and (b)(2) because, as explained in the agent affidavit, the **Subject Telephone** is currently believed to be located within this District.[5] Because collecting the information authorized by this warrant may fall within the statutory definitions of a "pen register" or a "trap and trace device," see 18 U.S.C. § 3127(3) & (4), the application and proposed warrant are designed to comply with the requirements of the Pen Register Statute as well as Rule 41. See 18 U.S.C. §§ 3121-3127. The warrant

[5] Pursuant to Rule 41(b)(2), law enforcement may use the cell-site simulator outside this District provided the **Subject Telephone** is within the District when the warrant is issued.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

therefore includes all the information required to be included in a pen register order. See 18 U.S.C. § 3123(b)(1).

IV. OTHER REQUESTED ORDERS

Additionally, this application also seeks authorization under 18 U.S.C. § 3103a(b), for reasonable cause shown, to delay any notification the government is required to give regarding the requested warrant to the subscriber(s) and user(s) of the **Subject Telephone** for a period of 180 days from the date that the disclosure ends. This period of delay is warranted because much of the evidence that has been and will continue to be obtained in this case is subject to an extensive and time-consuming filter-review process. 18 U.S.C. § 3103a(b) states that any notice required following the issuance of a warrant may be delayed if, inter alia, the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result. An adverse result is defined in 18 U.S.C. § 2705(a)(2) to include endangering the life or physical safety of a person, flight from prosecution, destruction of or tampering with evidence, intimidation of potential witnesses, or otherwise seriously jeopardizing an investigation or unduly delaying a trial. Moreover, the Advisory Committee Notes for Fed. R. Crim. P. 41(f)(3) (2006 Amendments) state that delay of notice may be appropriate where "the officer establishes that the investigation is ongoing and that disclosure of the warrant will compromise that investigation." The attached agent affidavit provides reasonable cause to believe that immediate notification of the execution of the warrant may have an adverse result. The proposed warrant both provides for the giving of such notice within 180 days after the date that the disclosure ends and prohibits, as

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

part of the receipt of the requested information, the seizure of any tangible property or any other prohibited wire or electronic information as stated in 18 U.S.C. § 3103a(b)(2). As discussed in the attached agent affidavit, immediate notification of this warrant to the user(s) of the **Subject Telephone** may have an adverse result.

Similarly, pursuant to 18 U.S.C. § 2705(b) and 18 U.S.C. § 3123(d)(2), this application requests that the Court enter an order commanding the Carrier not to notify any person, including the subscriber(s) of the **Subject Telephone**, of the existence of the warrant until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date the Carrier complies with the warrant or such later date as may be set by the Court upon application for an extension by the United States, for the reasons outlined in the attached agent affidavit.

This application also seeks an order that: (1) authorizes the disclosure of the requested information whether the **Subject Telephone** is located within this District, outside of the District, or both, pursuant to 18 U.S.C. § 2703(c)(1)(A) and Rule 41(b), and, for good cause shown, at any time of the day or night pursuant to Rule of Criminal Procedure 41; (2) authorizes the disclosure of not only information with respect to the **Subject Telephone**, but also with respect to any changed telephone number(s) assigned to an instrument bearing the same ESN, IMSI, or IMEI (hereinafter "unique identifying number") as the **Subject Telephone**, or any changed unique identifying number subsequently assigned to the same telephone number as the **Subject Telephone**, or any additional changed telephone number(s) and/or unique identifying number, whether the changes occur

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

consecutively or simultaneously, listed to the same wireless telephone account number as the **Subject Telephone** within the period of disclosure authorized by the warrant; and (3) orders the Investigating Agency to reimburse the applicable cellular telephone service provider for its reasonable expenses directly incurred in providing the requested information and any related technical assistance.

Finally, this application requests that it, the proposed warrant that has been concurrently lodged, and the return to the warrant be sealed by the Court until such time as the Court directs otherwise. Allowing disclosure to the public at large would likely jeopardize the ongoing investigation for the reasons outlined in the attached agent affidavit.

Dated: June 4, 2019

Respectfully submitted,

NICOLA T. HANNA
United States Attorney

SCOTT GARRINGER
Assistant United States Attorney
Deputy Chief, Criminal Division

MELISSA MILLS
Assistant United States Attorney

Attorneys for Applicant
UNITED STATES OF AMERICA

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

CERTIFICATION

In support of this application, and pursuant to 18 U.S.C. § 3122, I state that I, Melissa Mills, am an "attorney for the Government" as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure. I certify that the information likely to be obtained from the requested warrant is relevant to an ongoing criminal investigation being conducted by the Investigating Agency of the Target Subjects for violations of the Target Offenses.

I declare under penalty of perjury under the laws of the United States of America that the foregoing paragraph is true and correct.

June 4, 2019

DATE

MELISSA MILLS
Assistant United States Attorney
Public Corruption & Civil Rights Section

AFFIDAVIT OF ANDREW CIVETTI

I, Andrew Civetti, being duly sworn, declare as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since September 2015. I am currently assigned to a Public Corruption Squad, where I specialize in the investigation of corrupt public officials, including bribery, fraud against the government, extortion, and money laundering. In addition, I have received training in the investigation of public corruption and other white collar crimes.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of an application for a warrant authorizing the disclosure of cell-site and GPS information, as well as the use of a cell-site simulator, also known as a "Stingray," as defined or discussed within the application, at such intervals and times as the government may request, and the furnishing of all information, facilities, and technical assistance necessary to accomplish said disclosure unobtrusively, which disclosure will establish the approximate location of the following cellular telephone(s) for a period of 45 days: [redacted], a cellular telephone issued by provider Verizon, subscribed to by an as-yet unidentified person, and believed to be used by Melton Edises Levine (the "**Subject Telephone**").

3. I also seek authorization under 18 U.S.C. § 3103a(b), for reasonable cause shown below, to delay notification of the proposed warrant for a period of 180 days from the date that the disclosure ends. This period of delay is warranted because much of the evidence

that has been and will continue to be obtained in this case is subject to an extensive and time-consuming filter-review process.

4. As described more fully below, I respectfully submit there is probable cause to believe that cell-site information, GPS information, and information from a cell-site simulator likely to be received concerning the approximate location of the **Subject Telephone**, will constitute or yield evidence of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1341 (Mail Fraud); 1343 (Wire Fraud); and 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); 16 U.S.C. §§ 824o, 825o (Electric Reliability Standards) (collectively, the "Target Offenses"), being committed by PAUL PARADIS, DAVID WRIGHT, JAMES P. CLARK, THOMAS PETERS, WILLIAM FUNDERBURK, and others known and unknown (the "Target Subjects").

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of, or investigation into, this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. STATEMENT OF PROBABLE CAUSE

A. The Bribery-Fueled No-Bid LADWP Contract to AVENTADOR

6. On March 29, 2017, PAUL PARADIS registered a company called AVENTADOR UTILITY SOLUTIONS, LLC ("AVENTADOR") for the purpose of

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

pursuing a separate $30 million no-bid contract from the Los Angeles Department of Water and Power ("LADWP"), which ostensibly covered further work to remediate the CC&B system.[1] To obtain support for AVENTADOR's single-source bid for this $30 million contract, PARADIS secretly offered the LADWP General Manager, DAVID WRIGHT, a future post-retirement position as CEO of AVENTADOR, with an annual salary of $1 million and various associated benefits and perks.[2] WRIGHT secretly accepted this offer.[3] Based on my training, experience, and knowledge of this investigation, I believe this secret arrangement to

---

[1] PARADIS proffered some of the information herein, as detailed herein. PARADIS has no criminal record and has agreed to assist the government in exchange for favorable consideration in a potential future prosecution of him related to his conduct in this matter.

The facts of AVENTADOR's incorporation were provided by PARADIS in a proffer and are reflected in records maintained by the California Secretary of State.

As noted below, the facts indicate that the primary purpose of this contract was different than that reflected in the contract itself and the LADWP Board's public materials about the contract.

[2] In a consensually recorded conversation, WRIGHT previously stated that he intended to retire from LADWP in 2020. In subsequent consensually recorded conversations, WRIGHT advised that he had prepared a resignation letter and informed the Mayor's Office that he would retire in October 2019. WRIGHT is seeking an arrangement with the City that would permit him, upon retirement, to be hired as a contractor to report to an offsite location (not requiring him to actually produce work) and provide transitional services to the yet to be determined LADPW General Manager.

In a consensually recorded conversation, WRIGHT referred to PARADIS as his "ATM" and requested that PARADIS begin paying WRIGHT in August 2019, despite WRIGHT's intention not to retire from the City until October 2019.

[3] In a proffer session, PARADIS described his agreement with WRIGHT as to WRIGHT's future employment with and financial interest in AVENTADOR. WRIGHT confirmed their agreement in multiple consensually recorded conversations with PARADIS.

In addition to WRIGHT's financial interest in AVENTADOR, PARADIS and WRIGHT are planning to engage in another business venture that would solicit lucrative contracts from LADWP. PARADIS's affiliation with this company is overt, but WRIGHT, as current LADWP General Manager, has endeavored to hide his role.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

constitute bribery of a public official because it established a quid pro quo, namely, PARADIS's receipt of a lucrative City contract in exchange for WRIGHT's lucrative future salary.

7. According to PARADIS, during the months preceding the LADWP Board's vote on the $30 million no-bid contract, PARADIS also courted support from LADWP Board Vice President, attorney WILLIAM FUNDERBURK, who, in turn, solicited financial benefits from PARADIS before the vote.[4] I believe this arrangement to similarly constitute a quid pro quo relationship between PARADIS and FUNDERBURK.

8. Specifically, on May 31, 2017, FUNDERBURK asked PARADIS to provide legal services on behalf of a class-action defendant that FUNDERBURK was representing. PARADIS agreed to assist because he knew that FUNDERBURK was set to vote on the $30 million no-bid contract the following week, and he wanted FUNDERBURK to vote in his favor. FUNDERBURK e-mailed PARADIS the necessary documents, and PARADIS wrote a brief and sent it back to FUNDERBURK. PARADIS never billed FUNDERBURK or FUNDERBURK's client, nor did FUNDERBURK ever reimburse PARADIS for his legal services. Between May 31, 2017, and August 6, 2017, PARADIS performed "free" legal work for FUNDERBURK and FUNDERBURK's client because of FUNDERBURK's influence over the $30 million no-bid contract and potential future contracts.

9. Additionally, in October 2016, during PARADIS's initial preparations to seek the contract the following year, FUNDERBURK invited PARADIS to an award ceremony at which FUNDERBURK was being honored, telling PARADIS that FUNDERBURK expected PARADIS's full

---

[4] PARADIS proffered the information herein regarding benefits that he provided to FUNDERBURK in exchange for FUNDERBURK's support of his contract.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

support. On the guidance of WRIGHT, who advised PARADIS that he needed to donate because FUNDERBURK would soon be voting on PARADIS's contract, PARADIS donated $5,000 to the organization hosting FUNDERBURK's award function.

10. On June 4, 2017, two days before the LADWP Board approved the AVENTADOR contract, WRIGHT sent a text message to LADWP Board President MELTON EDISES LEVINE with FUNDERBURK's contact information. LEVINE responded, "Left a detailed vm [voicemail]. Will call again." That same day, LEVINE left a voicemail for WRIGHT that said, "I just reached BILL [FUNDERBURK], **I do not believe BILL [FUNDERBURK] will end up being a problem**; however, the issue is diligence. He said why don't we have like a committee, an oversight committee to monitor the progress. I think that is probably a good idea, but I told him I want to run that idea by you and not sign off on anything. I was going to go with you, period. But, that sounded like a reasonable suggestion, so I wanted to hear your thoughts about it."[5] Based on my training, experience, and knowledge of the investigation, I believe that LEVINE referencing that "BILL will not end up being a problem" to mean that LEVINE and WRIGHT, utilizing the **TARGET PHONES**, were coordinating efforts to ensure the $30 million AVENTADOR contract was approved. FUNDERBURK, being the Vice-President, needed to "not be a problem" leading into the LADWP Board meeting.

11. At the LADWP Board meeting on June 6, 2017,[6] both WRIGHT and LADWP Board President (and Gibson Dunn attorney) LEVINE strongly argued in favor of awarding the $30 million no-bid contract to

---

[5] This voice-mail was seized pursuant to the April 18, 2019 authorized by the Honorable Magistrate Judge Jacqueline Choolijan.

[6] This meeting was audio/video recorded by the City and I have reviewed this recording.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AVENTADOR, underscoring that the need for AVENTADOR's billing-system remediation services was so imminent that there was not sufficient time to engage in the standard competitive bidding process usually required for LADWP contracts of that size.[7] In addition, LADWP Ratepayer Advocate, Frederick Pickel, was asked if he had any questions or input, to which Pickel replied with an inquiry about how oversight would be provided. WRIGHT suggested that a subcommittee be formed to evaluate the work being completed, and LEVINE and FUNDERBURK were selected to perform that role. According to the above-described June 4, 2017 voicemail message from LEVINE to WRIGHT, which I have reviewed, these comments appeared to be staged. Following the enthusiastic recommendations of WRIGHT and LEVINE, all the Board members (including FUNDERBURK) voted in favor of awarding the $30 million contract to AVENTADOR.[8] Based on the context of the communications, the recording of the meeting, the interviews I conducted, and my knowledge of the investigation, I believe WRIGHT and LEVINE utilized methods of communication including the **Subject Telephone** to coordinate together and/or with FUNDERBURK for the AVENTADOR contract approval. This is relevant evidence because of

---

[7] In this Board meeting, video footage of which is publicly available on LADWP's website, WRIGHT described the urgent need to award this no-bid contract to AVENTADOR based on the negotiated terms of the pending settlement agreement, which required the City to remediate the CC&B system. LEVINE enthusiastically concurred, noting that LADWP had no choice but to award the no-bid contract to AVENTADOR. As discussed further below, the representations made by WRIGHT and LEVINE do not appear to be a fair or accurate description of the choice the LADWP Board had to make when awarding this $30 million dollar contract and instead appear to be pre-textual reasons to get the contract approved expeditiously and with little scrutiny.

[8] The Los Angeles City Council has the prerogative to review a contract of this size. According to PARADIS, WRIGHT asked certain members of City Council not to review the AVENTADOR contract.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

WRIGHT's quid pro quo relationship with PARADIS, and I am seeking to determine who else (a) was aware of their illicit relationship and (b) was set to financially benefit from the AVENTADOR contract approval.

12. On May 12, 2018, in a text message, WRIGHT told LEVINE, "MEL[TON LEVINE], here's a short message I sent [redacted]LADWP Chief Operating Officer] that's entirely plausible from meetings that we attended over the entire trip.[9] Just wanted you to know… We provide rebates for facility energy management systems. Some of the light bulbs that could work with them have light sensors or motion sensors in them. Hackers could go through the light bulbs to hack their facility's entire IT systems. Now think if that energy management system services a hospital. It could actually kill patients! And on top of how horrible that is, we would likely be pulled into the lawsuit." LEVINE replied, "Yikes!!!!!" Based on my training, experience, and knowledge of the investigation, I believe WRIGHT informed LEVINE about his message to [redacted] in an effort to plant seeds related to the need for cyber security. I believe that although the cyber vulnerabilities and necessity for cyber security measures may indeed exist, WRIGHT was such an advocate for cyber awareness and security services at least in part because of his illicit quid pro quo relationship with PARADIS, namely, WRIGHT's self-interest in his future lucrative employment with AVENTADOR.

13. On August 17, 2018, WRIGHT sent a text message to LEVINE and LADWP Board Commissioner Christina Noonan, "we have experienced a

---

[9] Based on the timing of the text message and my knowledge of the investigation, I believe that this was a reference to the May 2018 Israel trip attended by PARADIS, WRIGHT, and LEVINE, along with other LADWP officials.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

phishing attack that has resulted in hackers obtaining staff credentials and gaining access into our systems. We don't know yet to what extent. AVENTADOR staff have been working 24/7 to contain the situation. Nothing on our systems has been compromised or information released that we are aware of. But his [PARADIS's] dozen staff are mostly from the NSA or DOE and are **the best in the nation.** I will fill you in as we know more." Noonan replied, "Just checking in on this situation. Is AVENTADOR pre-approved under our cyber insurance policy? Any of this 24/7 cost will need to go against our deductible. Also, **I suggest communication relating to this matter, particularly with AVENTADOR, go through our legal counsel so that the Department secures attorney/client privilege which will be beneficial.** All of this presumes we have noticed our insurance carriers." Based on my knowledge of the investigation, I believe that WRIGHT glorified the team as being "the best in the nation" to further praise ADVENTADOR, a company in which WRIGHT secretly had a strong financial interest. In addition, I believe Noonan's comments that communication regarding AVENTADOR should be cloaked in attorney/client privilege to be consistent with LADWP's pattern of behavior to conceal aspects of the AVENTADOR contract.

14. Later that day, WRIGHT provided an update regarding the situation and stated, "We have 10 former staff from the NSA and DOE working 24/7 throughout the weekend and next week on the most highly exposed areas of our SCADA operating systems. (Our contractor, AVENTADOR owned by PAUL PARDIS, hired almost all of the DOE's cyber team over the last six months to work for him, so we have the some of the best experts related to these hacking efforts in the world working on this.). Biggest worry is that several months of planned

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

system fixes now have to be expedited into just a few weeks. We can tell the hackers keep trying to attack us but we are on it. (As perspective, **if we called the Federal government for help, they would contact the DOE who would have assigned the staff AVENTADOR already hired to come out to help us.**)." LEVINE replied, "Wow. Thanks Dave. Hang in there. If you want to talk over the weekend or Monday let us know." Based on my knowledge of the investigation, I believe WRIGHT was again advocating for LADWP's continued reliance on AVENTADOR and excusing the need to contact the Federal government regarding the issues. WRIGHT's effusive adulation portrays AVENTADOR and PARADIS as saviors to the City, a depiction that appears unwarranted by the facts and in any event omits WRIGHT's covert financial entanglement with AVENTADOR.[10] In addition, I have reviewed text messages between PARADIS, WRIGHT, and LEVINE in which PARADIS echoes WRIGHT's sentiments about AVENTADOR's expertise and necessity, yet omits reference to WRIGHT's financial interest in AVENTADOR's hiring.

15. On August 23, 2018, WRIGHT sent a text message to LEVINE, "no need to call back unless you want more info. Cyber attack has been contained. Mayor briefed by PAUL [PARADIS] and I. It was sophisticated. But PAUL's [PARADIS] **elite team of experts** handled it

---

[10] In October 2016, AVENTADOR performed penetration testing at the Los Angeles International Airport ("LAX") to test cyber vulnerabilities. The FBI received notice from LAX regarding the intrusion. Cyber agents with the FBI subsequently conducted an investigation that lead to the execution of a search warrant for [redacted], an AVENTADOR employee. [redacted] stated that he was authorized to conduct the penetration test and that AVENTADOR had a contact with the City. Representatives from AVENTADOR (now ARDENT) have yet to produce said contract. Based on my interviews with PARADIS, no such contract existed regarding penetration testing at LAX; however, PARADIS maintains that the testing was verbally authorized by City officials. Based on my discussions with FBI cyber agents, AVENTADOR's work was in fact "amateur."

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

and prioritized fixes. **Staff is now becoming very accepting of AVENTADOR staff** and excited about getting some training from the experts. PAUL [PARADIS] is charging us for this time, but not overcharging. We are so messed up here that **I will likely suggest a two year extension and an increase to his contract.** But that's six months away. I want to brief the board again at the next meeting." LEVINE replied, "Thanks DAVE [WRIGHT]. Just received. Great news. Please get back to me today if possible with the names of the Israeli companies we are considering using so I can promptly get back to the guy st [at] DHS Rep. Schiff put us together with. Thanks." WRIGHT then responded, "PAUL [PARADIS] is sending via text. **We don't want to do via LADWP email.**" PARADIS then sent a text message to WRIGHT and LEVINE with the Israeli companies' information and stated, "I sent this as a text rather than email for security and public record disclosure reasons." LEVINE then responded, "Great. Thanks. This is what I need and a good way to send. Will get back to you after I hear back." Based on the context of the communication, it appears as though WRIGHT was once again praising AVENTADOR heavily and laying the groundwork to advocate for an extension for AVENTADOR while utilizing personal email, which would not be subject to City monitoring. To my knowledge, WRIGHT does not have any formal cyber training or knowledge to be able to distinguish the experts in the field nor be able to provide the LADWP Board a true and accurate assessment of AVENTADOR's work, qualifications, or necessity. I believe that WRIGHT praised and advocated for AVENTADOR so heavily based on his quid pro quo relationship with PARADIS, namely, his financial stake in AVENTADOR contracts.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

B. Alleged Falsification of Regulatory Paperwork by LADWP Employees

16. The above-described LADWP contract awarded to AVENTADOR purported — according to its own terms and to the related LADWP Board materials and proceedings — to cover services related to remediation of the CC&B system, as required by the terms of a court-ordered settlement agreement. However, evidence suggests that this $30 million single-source contract, which General Manager WRIGHT and Board President LEVINE advertised to the LADWP Board as urgent because it was mandated by the court-ordered settlement agreement, was in truth to address an entirely unrelated matter, that is, it was primarily intended to cover services related to assessing and improving cybersecurity for the City's power grid and other critical infrastructure.[11]

17. PARADIS alleges that in order to conceal and avoid responsibility for certain cybersecurity vulnerabilities related to critical infrastructure, LADWP employees falsified mandatory federal regulatory documents[12], including by regularly self-reporting minor violations in order to avoid the discovery of much more significant violations, which would carry substantial fines (in some cases, millions of dollars). Based on my interviews with PARADIS and my knowledge of the investigation, including review of recordings on

---

[11] The information in this section was proffered by PARADIS and has been corroborated in part by: 1) the aforementioned consensually recorded conversations with WRIGHT; 2) separate consensually recorded conversations with an AVENTADOR employee; and 3) an AVENTADOR work plan and other documents reflecting AVENTADOR'S cybersecurity work for the City, which PARADIS provided to the government.

[12] These include documents mandated by the Federal Energy Regulatory Commission ("FERC") under a compliance regime known as "NERC-CIP" (North American Electric Reliability Corporation - Critical Infrastructure Protection).

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

this topic, City officials stated that they were under the impression that if they self-reported certain violations, federal regulatory agencies would be less likely to inquire into or investigate other possible violations.

18. In separate consensually recorded conversations with both the current and former Chief Information Security Officers for LADWP (STEPHEN KWOK and DAVID ALEXANDER, respectively), PARADIS confirmed both LADWP's pattern of self-reporting of minor violations to conceal far more significant problems and the fact that members of LADWP management (including WRIGHT) and the LADWP Board (including LEVINE and CYNTHIA MCCLAIN-HILL) were aware of that unethical and potentially illegal practice.

19. DAVID ALEXANDER also informed PARADIS in a consensually recorded conversation that LADWP falsified paper records to avoid significant fines that might be imposed by NERC and FERC. For example, NERC-CIP Reliability Standard CIP-007-6 requires that bulk electric system facilities deploy a patch management process to monitor and address software vulnerabilities; this process includes adhering to a security patch evaluation timeline to ensure that all patches are up-to-date. In an April 2019 consensually recorded conversation with PARADIS, ALEXANDER said that a comparison of LADWP's paper records to its computers would show that LADWP claimed it applied patches in a timely fashion when, in fact, it did not. ALEXANDER's proposed solution to the problem, which he disclosed to PARADIS, was to simply dispose of all the old computers evidencing delayed patching, and replace them with new computers that had no evidence of any patching issues.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

C. Alleged Circumvention of LADWP's Contracting Process

1. Discussions Regarding Cyber Services for LADWP

20. On January 8, 2019, WRIGHT sent a text message to LEVINE at the **Subject Telephone** stating that, "Cyber and IT will always need external staff (I think [redacted] - Business Manager, IBEW Local 18][13] already supports this), we are increasing staff everywhere in the department as fast as reasonable. Need to get more supportive on outsourcing as we have hired a net increase of couple thousand staff in the last few years. We support greater workforce development but LADWP needs to have a greater role in screening them for base line qualifications."

21. On March 14, 2019, LEVINE sent a text message from the **Subject Telephone** to WRIGHT, "Ok. I need to talk with Dakota [Smith - Los Angeles Times Reporter] again in the next few minutes. Pretty much told her what we are doing to keep the cyber employees. She questioned if that is consistent with board instruction to cancel AVENTADOR contract.[14] Joe [Brajevich - LADWP General Counsel] gave me a good response to that." Based on the context of the communication it appears as though Smith inquired into the retention of City cyber employees and the fate of the AVENTADOR employees post cancellation.

---

[13] IBEW Local 18 is a labor union. According to IBEW Local 18's website, Local 18 is an "affiliate of the International Brotherhood of Electrical Workers (IBEW). Although our name says "electrical workers," our members come from hundreds of different job classifications."

[14] According to PARADIS, after his dual role in the civil litigation came under scrutiny as described herein, in order to keep AVENTADOR employees working on the City contract, PARADIS submitted to pressure to sell AVENTADOR and have no part in any subsequent companies that form. PARADIS sold AVENTADOR below market value and has in fact remained an integral part of ARDENT (the new company). Based on consensually recorded conversations, WRIGHT and LEVINE are aware of PARADIS' continued involvement.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

The formation of ARDENT, a subsequent awarded contract discussed below, do not appear to me to be consistent with the LADWP Board's demand.

22. On March 26, 2019, WRIGHT sent a text message to LEVINE, "I have to share at some point that [we are] deliberately vague on our public descriptions as we were worried about publicly communicating our specific cyber vulnerabilities. And we discussed this in closed session and in our meetings with other city staff. Will try to mention it in general in the meeting tomorrow morning if it fits into the discussion." LEVINE replied, "Good. Radio silence from CYNTHIA [MCCLAIN-HILL] after calling and emailing."

23. On March 27, 2019, WRIGHT sent a text message to LEVINE, "Check LADWP email. Excellent summary document regarding cyber we will discuss at tomorrow's meeting." LEVINE replied, "Can you send it to my other email?"[15]

2. Manipulation of the SCCPA Bidding Process

24. According to PARADIS, LADWP management and members of the Board (including WRIGHT, LEVINE, and MCCLAIN-HILL) have successfully manipulated LADWP's contracting processes to ensure that AVENTADOR's successor company, ARDENT UTILITY SOLUTIONS, LLC ("ARDENT")[16], is awarded a lucrative contract to continue AVENTADOR's cybersecurity work without engaging in the required competitive bidding process (the "ARDENT contract"). According to information proffered by PARADIS, LADWP routinely uses the Southern California Public Power

---

[15] Based on my interviews of PARADIS, LEVINE utilized his Gibson Dunn email to conduct City business, not his LADWP email.

[16] Despite a sham sale in March 2019, PARADIS appears to still effectively control this company.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Authority ("SCPPA")[17] to circumvent LADWP's standard 12-18 month competitive bidding process, and did so for the ARDENT contract.[18]

25. The SCCPA website shows that in February 2019, SCCPA issued a Request for Proposals for Cybersecurity Services. On March 27, 2019, WRIGHT sent a text message to LEVINE, "During the discussion with Cynthia and [redacted] after the larger meeting today, it was determined that no report will go forward at the next board meeting. We will move the second meeting to April 16th and take the contact forward then. I can discuss more over the phone if you'd like." LEVINE replied, "Yes. Still in meetings. Will reach Out when able."

26. On March 29, 2019, WRIGHT sent a text message to LEVINE, "The mayors office directed me about 90 minutes ago to put an item on the agenda for 4/2 that covers critical incident cyber response. The thought is that we will cite our ability to utilize the city's ITA contract hours and their 24 hour response time with two vendors they have - Fireeye and Dell. And then to direct staff to negotiate a separate LADWP contract for more hours and a faster response time. I've got Donna [Stevener - LADWP Chief Administrative Officer] and Stephen [KWOK] figuring out the best language for an agenda item and then running it past Joe B[rajevich]. The written report can submitted Monday or Tuesday morning per Joe [Brajevich]." LEVINE replied, "Will call you in a few minutes to discuss."

27. On April 5, 2019, in a consensually recorded conversation, LEVINE and MCCLAIN-HILL confirmed to PARADIS that ARDENT would be the

---

[17] According to the SCPPA website, SCPPA is "a Joint Powers Authority, created in 1980, for the purpose of providing joint planning, financing, construction, and operation of transmission and generation projects."

[18] According to the SCPPA website, WRIGHT is the Secretary of SCPPA and a current member of the SCPPA Board of Directors.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_000313
Page 313 of 1425

primary vendor (out of 28 candidates), *despite the fact that SCPPA was not scheduled to vote on the contract until a meeting on April 18, 2019* — almost two weeks later. Based on my training, experience, and knowledge of the investigation, this behind-the-scenes manipulation of City contracting processes appears to be consistent with related unethical and/or illegal behavior by LADWP officials. On April 23, 2019, the LADWP Board approved a 60-day contract of $3,600,000 for ARDENT and two other companies.[19]

D. Alleged Conspiracy and Falsification of Records by Attorney Members of the LADWP Board, LADWP Attorneys, and Members of the City Attorney's Office[20]

1. The City's Debarment of PwC

28. In June 2016, while representing the City in litigation against PwC related to implementation of a billing system that allegedly caused massive LADWP billing problems, PARADIS proposed debarring[21] PwC in the wake of salacious public allegations that PwC

---

[19] The Board's action is confirmed in public materials on the LADWP website. According to PARADIS and confirmed in a consensually recorded conversation with WRIGHT on April 21, 2019, the original plan for a larger contract to ARDENT was tabled after the Mayor's office exerted pressure on LADWP to avoid such a large contract with ARDENT due to the potential for negative publicity related to ARDENT, a successive company to AVENTADOR, being awarded another large contract. PARADIS reported that LADWP planned that the majority of the $3.6M 60-day contract would go to ARDENT, and that the contract would thereafter be extended or expanded.

[20] PARADIS proffered the information in this section and provided the government with his correspondence with LEVINE, WRIGHT, FUNDERBURK, Brajevich, and others. While the version seen by the prosecution team to date was heavily redacted by the government's filter attorneys, it generally corroborates PARADIS's account, as detailed below.

[21] Debarment is the state of being excluded from enjoying certain possessions, rights, privileges, or practices and the act of prevention by legal means. For example, companies can be debarred from contracts due to allegations of fraud, mismanagement, and similar improprieties.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

employees had misspent City money on personal entertainment (including prostitutes and alcohol) in Las Vegas. According to PARADIS, in a closed session on June 21, 2016, the LADWP Board agreed with PARADIS and voted 4-0 in favor of debarring PwC, with Board President LEVINE recusing himself from the discussion and vote due to a conflict of interest.[22] Based on LADWP's minutes of the public board meeting on that same date, it appears that the four other board commissioners at the time were FUNDERBURK, Michael Fleming, Christina Noonan, and Jill Banks Barad.

29. PARADIS further reported that a press release touting the debarment was drafted and circulated among the staff of the City Attorney's Office. According to PARADIS, LEVINE, City Attorney Michael Feuer, former Chief of Civil Litigation PETERS, LADWP General Counsel Joseph Brajevich, and others thereafter embarked on a furtive and successful campaign to influence the other LADWP Board members to secretly change their votes, which ultimately resulted in the PwC debarment issue being dropped. The initial 4-0 vote in favor of debarment was not reflected in Board materials and PwC was not debarred.

30. According to PARADIS, he and his law partner, GINA TUFARO, were called to meet with Feuer and others (including PETERS, Brajevich, and Leela Kapur, Feuer's Chief of Staff) in Feuer's office

---

This initiative to debar PwC came in the wake of public allegations that PwC managers overbilled the City and then spent the money on prostitutes, luxury bottle service liquor, and entertainment in Las Vegas. See https://www.latimes.com/local/lanow/la-me-ln-dwp-billing-20160630-snap-story.html.

[22] According to PARADIS, LEVINE is supposed to be recused from LADWP Board matters involving PwC because PwC is a prominent and lucrative Gibson Dunn client. (LEVINE is a partner at Gibson Dunn, and Clark retired from Gibson Dunn as a partner.)

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

on June 30, 2016. Feuer was angry about the debarment initiative and informed PARADIS that he (Feuer) was the "team captain" and as such was charged with making the decision as to whether to pursue debarment. PARADIS stated that the Board had already voted and debarment was therefore going to happen, and Feuer said words to the effect that, "We'll see about that."[23] At Feuer's direction, PARADIS made a presentation to LADWP management, including WRIGHT, in favor of debarment, and PETERS gave a contrary presentation against debarment. PARADIS then met with LADWP Board Vice President FUNDERBURK, who told PARADIS that both he and another Board member, Michael Fleming, were committed to debarment and would stand by their votes in favor of debarring PwC. A few days later, FUNDERBURK contacted PARADIS to advise that debarment was probably not going to happen. PARADIS went to WRIGHT and threatened to "blow the whistle" - meaning he would disclose information related to certain criminal schemes to the public - if he didn't learn what was going on, and obtained WRIGHT's permission to review the emails from the LADWP server during the period of the debarment dispute.

31. PARADIS then printed a large number of emails reflecting communications about debarment and behind-the-scene efforts by LEVINE, Feuer, Brajevich, then-LADWP General Manager Marcie Edwards, and others to reverse the Board's 4-0 vote to debar PwC. The prosecution team has since reviewed redacted versions of some of those emails, as received from the government's filter team. While

---

[23] According to PARADIS, Feuer claimed that the debarment process was "in shambles," and thus that debarment was not a viable option. However, PARADIS stated that the Board also voted to debar another entity at the same June 21, 2016 meeting, and that the other debarment vote was never challenged.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

the text of almost all of the emails is heavily redacted (due in part to the apparent default practice of copying General Counsel Brajevich on nearly every piece of correspondence), the email traffic is generally consistent with PARADIS's account of the debarment episode.

32. Specifically, the emails indicate that:

- On June 30, 2016, City Attorney Michael Feuer held a scheduled meeting with Brajevich, PETERS, and Kapur, regarding PwC.
- Over the next few days, FUNDERBURK, PETERS, Kapur, Feuer, Brajevich, and others traded numerous emails on the subject of PwC and the debarment issue.
- On July 1, 2016, at the end of an email exchange between FUNDERBURK, WRIGHT, Michael Fleming, Marcie Edwards, Joseph Brajevich, and later, LEVINE, regarding a special board meeting to discuss PwC, Marcie Edwards forwarded the email chain only to FUNDERBURK with the message, "Please. Trust me and stand down." (emphasis added).
- On July 1, 2016, LEVINE and Edwards discussed having Feuer speak with FUNDERBURK.
- On July 1, 2016, notwithstanding his recusal from PwC debarment matters, LEVINE sent an email to all Board commissioners, Edwards, and Brajevich, with the subject "PWC lawsuit."
- On July 1, 2016, after emails between FUNDERBURK and Edwards, WRIGHT advised Edwards that FUNDERBURK "wants to be removed from this specific item as it's heard."

33. As stated above, debarment of PwC did not ultimately happen, and the minutes from the June 21, 2016 LADWP Board meeting do

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

not reflect the original 4-0 vote in favor of debarment. Rather, the Board meeting minutes from June 21, 2016, note: "Discussion held - action taken but not a final action that is reportable." Based on my knowledge of the investigation, I believe the minutes did not accurately reflect the events that actually transpired at the meeting. It is presently unclear to me the motivations of LEVINE, Feuer, and other members of the City Attorney's Office preventing the debarment and why LEVINE was included in the discussions despite being recused.

6. PARADIS has informed me that LEVINE uses the **Subject Telephone**, a fact that is corroborated by text messages to LEVINE at the **Subject Telephone** number obtained from PARADIS's and WRIGHT's telephones. LEVINE is known to spend most of his time in the Central District of California.

7. I seek GPS/cell-site information via this application because this information will assist me in gathering evidence in the ongoing investigation I have described above in the following ways: (1) I am investigating a conspiracy, and determining concert of action and contact between the conspirators is of value to my investigation; (2) the information will allow me to identify members of the conspiracy that I have not previously identified; (3) the information will provide insight into the roles and actions of the members of the conspiracy, and the criminal conduct committed by the people being investigated; (4) it will provide information regarding whether the individuals being investigated meet or have contact prior to, or after, committing any criminal conduct; and (5) the information will often identify locations where evidence is stored and where search warrants may be appropriate. Moreover, it will

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

assist in targeting surveillance conducted in this case, and reduce the risk of being detected and revealing the nature or fact of the investigation. People who are involved in criminal activity are often conscious of being followed and keep a close eye out for surveillance units. The chance of being discovered increases with the more surveillance that is done and the closer the surveillance units must get to the target subjects. Use of the prospective cell-site/GPS information enables the investigative team to be more focused and judicious in its use of surveillance to those times when it appears that events of significance are going to occur. It also allows the investigative team the ability to conduct surveillance at a greater distance, because the fear of losing the target is reduced when surveillance is maintained via GPS/cell-site information.

IV. TECHNICAL BACKGROUND REGARDING CELL-SITE SIMULATORS

8. Based on my training an experience and my conversations with other agents and investigators, I understand the following regarding cell-site simulators:

a. Cell-site simulators function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the device identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would with a networked tower.

b. A cell-site simulator receives and uses an industry standard unique identifying number (e.g., Electronic Serial Number (ESN), Mobile Equipment Identifier (MEID), International Mobile Subscriber Identity (IMSI), International Mobile Equipment Identity (IMEI), Mobile Station Identity (MSID), Mobile Directory Number (MDN)

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

or the Universal Fleet Member Identity (UFMI)) that is assigned by a device manufacturer or cellular network provider. When used to locate a known cellular device, a cell-site simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator. Once the cell-site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone.

c. By transmitting as a cell tower, cell-site simulators acquire the unique identifying information from cellular devices. This identifying information is limited, however. Cell-site simulators provide only the relative signal strength and general direction of a subject cellular telephone; they do not function as a GPS locator, as they do not obtain or download any location information from the device or its applications. Moreover, cell-site simulators do not collect the contents of any communication. This includes any data contained on the phone itself: the simulator does not remotely capture emails, texts, contact lists, images, or any other data from the phone. In addition, cell-site simulators do not provide subscriber account information (for example, an account holder's name, address, or telephone number).

V. INTENDED USE OF THE CELL-SITE SIMULATOR AND DELETION OF NON-TARGET DATA

9. Investigators intend to use the cell-site simulator to send signals to the **Subject Telephone** that will cause the **Subject Telephone**, and non-target cellular phones on the same provider network in close physical proximity, to emit unique identifying information, which the cell-site simulator will collect. Investigators will then use the information collected by the cell-

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

site simulator to determine the physical location of the **Subject Telephone**.

10. Although the cell-site simulator will collect the unique identifiers not only of the **Subject Telephone**, but also identifiers belonging to nearby non-target cellular telephones, these latter identifiers will not be used by law enforcement for investigative purposes, just as the extraneous incoming and outgoing telephone numbers necessarily recorded by conventional pen registers and trap-and-trace devices are not used for affirmative investigative purposes. Absent further order of the court, law enforcement will make no investigative use of information concerning non-targeted cellular devices other than distinguishing the **Subject Telephone** from all other devices. Once law enforcement has located the **Subject Telephone**, it will delete all information not associated with the **Subject Telephone**.

11. The cell-site simulator may interrupt cellular service of cellular devices within its immediate vicinity. Any service disruption will be brief and temporary, and all operations will attempt to limit the interference with cellular devices.

VI. GROUNDS FOR SEALING AND DELAYING NOTICE

12. Based on my training and experience and my investigation of this matter, I believe that reasonable cause exists to seal this application and warrant, as well as the return to the warrant. I also believe that reasonable cause exists to delay the service of the warrant by the Investigating Agency as normally required for a period of 180 days beyond the end of the disclosure period pursuant to 18 U.S.C. § 3103a(b) and, pursuant to 18 U.S.C. § 2705(b), to enter an order commanding the Carrier not to notify any person, including the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

subscriber(s) of the **Subject Telephone**, of the existence of the warrant until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date the Carrier complies with the warrant or such later date as may be set by the Court upon application for an extension by the United States. There is reason to believe that such notification will result in (1) flight from prosecution; (2) destruction of or tampering with evidence; (3) intimidation of potential witnesses; or (4) otherwise seriously jeopardizing the investigation.

13. Furthermore, there is good cause for the warrant to be issued such that the information may be provided to law enforcement at any time of the day or night because in my training and experience, and knowledge of this investigation, the subjects of the investigation do not confine their activities to daylight hours, and it is often even more difficult to conduct surveillance at night.

///

///

///

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

VII. CONCLUSION

14. For all of the above reasons, there is probable cause to believe that prospective cell-site information, GPS information, as well as information from a cell-site simulator, likely to be received concerning the approximate location of the **Subject Telephone**, currently within, or being monitored or investigated within, the Central District of California, will constitute or yield evidence of violations of the Target Offenses being committed by the Target Subjects.

/s/
Andrew Civetti, Special Agent
Federal Bureau of
Investigation

Subscribed to and sworn before me
this 4th day of June, 2019.

Patrick J. Walsh
UNITED STATES MAGISTRATE JUDGE

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

ORIGINAL

TRACY L. WILKISON
Attorney for the United States,
Acting Under Authority Conferred By 28 U.S.C. § 515
SCOTT GARRINGER
Assistant United States Attorney
Deputy Chief, Criminal Division
MACK E. JENKINS (Cal. Bar No. 242101)
Assistant United States Attorney
Chief, Public Corruption & Civil Rights Section
MELISSA MILLS (Cal. Bar No. 248529)
Assistant United States Attorney
Public Corruption and Civil Rights Section
DIANA KWOK (Cal. Bar No. 246366)
Assistant United States Attorney
Environmental and Community Safety Crimes Section
1500 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-0627
Facsimile: (213) 894-2927
E-mail: Melissa.Mills@usdoj.gov

Attorneys for Applicant
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

IN RE CELLULAR TELEPHONE	No. 2:19-mj-02372
	~~[PROPOSED]~~ WARRANT
	(UNDER SEAL)

Upon application by the United States of America, supported by the law enforcement agent's affidavit, for a warrant relating to the following cellular telephone: [redacted] a cellular telephone issued by provider Verizon, subscribed to by an as-yet unidentified person, and believed to be used by Melton Edises Levine (the "**Subject Telephone**").

THIS COURT FINDS THAT there is probable cause to believe that prospective cell-site information, GPS information, and information obtained from a cell-site simulator likely to be received concerning

the approximate location of the **Subject Telephone**, currently within, or being monitored or investigated within, the Central District of California, will constitute or yield evidence of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1341 (Mail Fraud); 1343 (Wire Fraud); and 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); 16 U.S.C. §§ 824o, 825o (Electric Reliability Standards) (collectively, the "Target Offenses"), being committed by PAUL PARADIS, DAVID WRIGHT, JAMES P. CLARK, THOMAS PETERS, WILLIAM FUNDERBURK, and others known and unknown (the "Target Subjects").

THIS COURT FURTHER FINDS THAT, pursuant to 18 U.S.C. § 3123, the attorney for the government has certified that the information likely to be obtained is relevant to an ongoing criminal investigation of the Target Subjects being conducted by the Federal Bureau of Investigation (the "Investigating Agency") for violations of the Target Offenses.

THIS COURT FURTHER FINDS reasonable cause exists to believe that providing immediate notification of this warrant to the user of the **Subject Telephone** may have an adverse result.

GOOD CAUSE HAVING BEEN SHOWN, THIS COURT HEREBY ISSUES THIS WARRANT AND ORDERS THAT:

1. The Carrier shall disclose, at such intervals and times as directed by the Investigating Agency, information concerning the location (physical address) of the cell-site at call origination (for outbound calling), call termination (for incoming calls), and, if reasonably available, during the progress of a call, for the **Subject Telephone**, as well as such other information, apart from the content

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

of any communication, that is reasonably available to the Carrier and that is requested by the Investigating Agency or any law enforcement agency working with the Investigating Agency, concerning the cell-sites/sectors receiving and transmitting signals to and from the **Subject Telephone** whether or not a call is in progress.

2. The Carrier shall disclose at such intervals and times as directed by the Investigating Agency the approximate physical location of the **Subject Telephone**, to include E-911 Phase II data and latitude and longitude data gathered for the **Subject Telephone**, including Global Positioning Satellite ("GPS") and/or network timing information, including Sprint's Per Call Measurement Data, Verizon's Real Time Tool, AT&T's Network Event Location System and T-Mobile's True Call data, and including information from such programs as Nextel Mobile Locator, Boost Mobile Loopt, Sprint/Nextel Findum Wireless, or a similar program, which will establish the approximate location of the **Subject Telephone**, and which information is acquired in the first instance by the Carrier, which will establish the approximate location of the **Subject Telephone** (referred to herein as "GPS information"), and shall furnish all information, facilities, and technical assistance necessary to accomplish said disclosure unobtrusively.

3. The Investigating Agency may also use a mobile electronic device or cell site simulator to obtain dialing, routing, addressing, or signaling information (but not content) from the **Subject Telephone** in order to help identify the location of the **Subject Telephone.** The individuals operating the cell-site simulator shall use technology reasonably available to restrict the recording or decoding of electronic or other impulses to the dialing, routing, addressing and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000326
Page 326 of 1425

signaling information used in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communication, and so as to ensure that the device is used with minimum interference with the services accorded to customers of such service. Information collected by the cell-site simulator pursuant to this warrant that is not associated with the **Subject Telephone** shall not be used by the Investigative Agency, or individuals operating the cell-site simulator, for any investigative purpose.

4. As part of the receipt of the requested GPS information, the Investigating Agency is prohibited from seizing any tangible property pursuant to this warrant, or any other prohibited wire or electronic information as stated in 18 U.S.C. § 3103a(b)(2). This warrant does not address whether the Investigating Agency may seize such property or information in relation to any other investigation authorized by law.

5. The Investigating Agency is permitted to delay service of this warrant to the subscriber(s) of the **Subject Telephone** for a period of 180 days from the date that the disclosure ends. The extensive and time-consuming filter-review process necessarily involved in the review of evidence in this case constitutes good cause for this period of delay. Any requests for a continuance of this delay should be filed with this Court, unless directed to the duty United States Magistrate Judge by this Court.

6. The Investigating Agency shall make a return of this warrant to the United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office within ten calendar days after the disclosure of information ceases. The return

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000327
Page 327 of 1425

shall state the date and time the telephone company began providing information pursuant to this warrant, and the period during which information was provided, including pursuant to any orders permitting continued disclosure.

7. The disclosure of the requested information by the Carrier shall begin during the daytime on the earlier of the day on which law enforcement officers first begin to receive information pursuant to this warrant or ten days after the date of this warrant, and continue for up to 45 days from the date of this warrant unless additional orders are made continuing the period of the disclosure. The Investigating Agency's use of the cell-site simulator shall begin no later than 10 days after the date of this warrant, and may continue for up to 45 days from the date of this warrant unless additional orders are made permitting continued usage.

8. The disclosure of the requested information and the Investigating Agency's use of the cell-site simulator shall occur whether the **Subject Telephone** is located within this District, outside of the District, or both, and, for good cause shown, shall extend to any time of the day or night as required.

9. The disclosure of the requested information shall not only be with respect to the **Subject Telephone**, but also with respect to any changed telephone number(s) assigned to an instrument bearing the same ESN, IMSI, or IMEI (hereinafter "unique identifying number") as the **Subject Telephone**, or any changed unique identifying number subsequently assigned to the same telephone number as the **Subject Telephone**, or any additional changed telephone number(s) and/or unique identifying number, whether the changes occur consecutively or simultaneously, listed to the same wireless telephone account number

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

USAO_000328
Page 328 of 1425

as the **Subject Telephone** within the period of disclosure authorized by the warrant.

10. The Carrier shall execute the Court's warrant as soon as practicable after it is signed. If a copy of the warrant is given to the Carrier, the copy may be redacted by law enforcement to exclude the Target Subjects and any description of the offenses under investigation.

11. The Investigating Agency shall reimburse the Carrier for their reasonable expenses directly incurred by the Carrier in providing the requested information and any related technical assistance.

12. To avoid prejudice to this criminal investigation, the Carrier and its agents and employees shall not disclose to or cause a disclosure of this Court's warrant and orders, or the request for information by the Investigating Agency or other law enforcement agencies involved in the investigation, or the existence of this investigation, except as necessary to accomplish the assistance hereby ordered, until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date the Carrier complies with this warrant or such later date as may be set by the Court upon application for an extension by the United States. In particular, the Carrier and its agents and employees are ordered not to make any disclosure to the lessees of the telephone or telephone subscribers. Upon expiration of this order, at least ten business days prior to disclosing the existence of the warrant, the Carrier shall notify the agent identified below of its intent to so notify:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

[redacted]

13. The application, this warrant, and the return to the warrant shall remain under seal until otherwise ordered by the Court. Law enforcement is permitted to provide a copy of the warrant to the Carrier.

DATE/TIME OF ISSUE:
6/4/19 5:30 p.m.

Patricia J. Walsh
UNITED STATES MAGISTRATE JUDGE

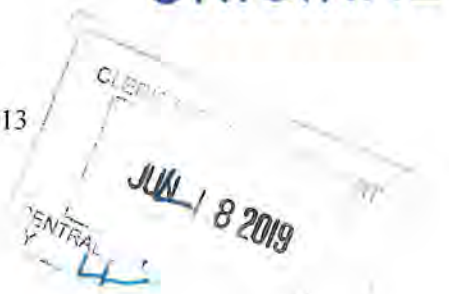
Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

UNITED STATES DISTRICT COURT

for the

Central District of California

ORIGINAL



In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	Case No. 2:19-MJ-02913
Information associated with items identified in Attachment A-7 that is within the possession, custody, or control of Aventador/Ardent Offices, 221 N. Figueroa Street, Los Angeles, CA	

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-7

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B-7

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 666	Bribery and Kickbacks Concerning Federal Funds
18 U.S.C. § 1341	Mail Fraud
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1346	Deprivation of Honest Services
18 U.S.C. § 1505	Obstructing Federal Proceeding
18 U.S.C. § 1510	Obstruction of Justice
18 U.S.C. § 1951	Extortion
18 U.S.C. § 1956	Money Laundering
16 U.S.C. §§ 824o & 825o	Knowing and Willful Violation of Electric Reliability Standards

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of_____days (*give exact ending date if more than 30 days:*_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Andrew Civetti, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 7/18/19

Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh, U.S. Magistrate Judge

Printed name and title

AUSA: Melissa Mills (213) 894-0627

ATTACHMENT A-7 [Aventador/Ardent Offices]

PROPERTY TO BE SEARCHED

The premises to be searched are located at **221 N. Figueroa Street, 15th Floor, Los Angeles, California ("City Property 15th Floor")** and pictured below. Specifically, the following locations within the City Property are to be searched.

1. **Aventador/Ardent Office's** (15th Floor – North side of building)

ATTACHMENT B-7 (Ardent Offices)

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 16 U.S.C. §§ 824o, 825o (Knowing and Willful Violation of Electric Reliability Standards) (the "Target Offenses"), namely:

a. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Formation, incorporation, purchase, or transfer of the company;

ii. Contracts, bids, proposals, or requests for proposal;

iii. Invoices, bills, timesheets, expense reimbursements, daily cash reports, expense reports;

iv. Business development, marketing, or advertising;

v. Board, agency, City Council, or other customer presentations;

vi. Communications with or concerning officials or employees with the City of Los Angeles;

vii. Communications with or concerning PAUL PARADIS, GINA TUFARO, PARADIS LAW GROUP, [redacted], or any other employee or officer of PARADIS LAW GROUP;

viii. AVENTADOR UTILITY SOLUTIONS LLC ("AVENTADOR");

ix. Any future enterprise to be developed from ARDENT UTILITY SOLUTIONS LLC ("ARDENT") or AVENTADOR;

x. Business-related foreign travel by employees or officers of AVENTADOR or ARDENT, or by employees or officials of the City of Los Angeles, between January 1, 2018, through the present; coordination by AVENTADOR, ARDENT, or the City of Los Angeles with foreign governments or entities; memoranda of understanding or other information-sharing agreements with foreign governments or entities; witting or unwitting transfer of proprietary or sensitive information belonging or relating to the City of Los Angeles;

xi. Penetration testing or other intrusions into networks or systems of any entity, whether authorized or unauthorized;

xii. Any physical security or cybersecurity issues, risks, or threats identified at LADWP, including any communications or presentations to LADWP employees, LADWP Board members, or Los Angeles City Council members;

xiii. Any physical security or cybersecurity assessments or surveys performed for or at LADWP, from June 1, 2008, to the present, whether by ARDENT, AVENTADOR, Element

Digital, Oracle, SDI Presence, LLC, Robert Bigman, West Monroe, or any other cybersecurity vendor;

xiv. Any cybersecurity or physical security risk management, mitigation or remediation relating to cybersecurity or physical security issues identified at LADWP after June 1, 2008;

xv. Any certifications, reports, statements, or other communications to the Western Electricity Coordinating Council ("WECC"), the North American Electric Reliability Corporation ("NERC"), or the Federal Energy Regulatory Commission ("FERC") regarding compliance or failure to comply with NERC Critical Infrastructure Protection ("NERC-CIP") standards;

xvi. Falsification, manipulation, or destruction of records, data, or other information relating to compliance with NERC-CIP standards;

xvii. Destruction or concealment of evidence.

b. Bank records, tax records, and other financial records;

c. Employment and personnel records for all current and former AVENTADOR and ARDENT employees or officers, including work history, performance reviews, evaluations, ethical screens, lodged complaints, disciplinary actions, administrative leave, suspension, and dismissal;

d. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

e. Any digital device and data servers, to include the Los Angeles City server, capable of being used to commit or further the Target Offenses, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such Target Offenses, and forensic copies thereof.

f. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

1. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

2. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

3. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

4. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

Table of Contents

I. INTRODUCTION.....1

II. PURPOSE OF AFFIDAVIT.....3

III. BACKGROUND ON SUBJECTS.....11

IV. OTHER RELEVANT PERSONS AND ENTITIES.....18

V. STATEMENT OF PROBABLE CAUSE.....21

A. The Underlying Civil Litigation.....21

1. Collusive Litigation Practices between the Los Angeles City Attorney's Office, PARADIS, PAUL KIESEL, and JACK LANDSKRONER.....21

2. The City's Filing of Selected Documents....43

3. Hush Money to Conceal Collusive Litigation Practices.....45

B. The Manipulation of the Court-Appointed "Independent Monitor".....47

C. No-Bid LADWP Contracts Awarded to Attorney PARADIS and Quid Pro Quo Established with City Officials.....49

1. 2015 and 2016 No-Bid Contract for $6,000,000.....49

2. 2017 No-Bid Contract for $30,000,000.....49

3. WRIGHT Advocated For and Praised AVENTADOR in an Effort to Gain Support for Future Contracts.....55

4. Clear Warnings to LADWP and LEVINE About the AVENTADOR Contract and PARADIS.....59

D. Alleged Falsification of Regulatory Paperwork by LADWP Employees.....63

1. Underreporting and Failure to Report Cybersecurity Issues.....63

E. Alleged Circumvention of LADWP's Contracting Process.....67

1. Manipulation of the SCPPA Bidding Process..67

2. Continuing Manipulation of the LADWP Bidding Process.....72

F. Alleged Conspiracy and Falsification of Records by Attorney Members of the LADWP Board, LADWP Attorneys, and Members of the City Attorney's Office.....74

1. The City's Contemplated Actions to Debar PwC.....74

G. LADWP's Use of a Foreign Broker Known to Receive Kickbacks From Successful Contract Vendors.....79

H. Obstruction of Justice by WRIGHT.....84

1. WRIGHT's Request That PARADIS Destroy Evidence in His Email Accounts and on His Laptop and Cell Phone.....84

2. PARADIS Met with WRIGHT to Discuss the Criminal Schemes and Target Offenses Through Early June 2019.....90

VI. CONCERNS ABOUT SPOLIATION OF EVIDENCE.....94

A. Destruction or Concealment of Evidence and False Testimony.....95

B. The City's April 26, 2019 Filing of Selected Documents.....96

C. Attempts to Shield Certain Deposition Testimony.....98

D. The Overall Conduct of the Collusive Litigation.....99

VII. PREMISES INFORMATION.....100

VIII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES.....101

IX. BACKGROUND ON E-MAIL AND THE PROVIDER.....104

X. REQUEST FOR NON-DISCLOSURE.....110

XI. AFFIDAVIT NOT ATTACHED TO SEARCH WARRANT.....110

XII. CONCLUSION.....111

XIII. Search Warrants Reference Chart.....112

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AFFIDAVIT

I, Andrew Civetti, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since September 2015. I am currently assigned to a Public Corruption Squad, where I specialize in the investigation of corrupt public officials, including bribery, fraud against the government, extortion, and money laundering. In addition, I have received training in the investigation of public corruption and other white collar crimes.

2. I am currently one of the agents assigned to an investigation of alleged corrupt activities at the Los Angeles Department of Water and Power ("LADWP") and the Los Angeles City Attorney's Office ("City Attorney's Office") by PAUL PARADIS, JACK LANDSKRONER, PAUL KIESEL, DAVID WRIGHT, MELTON EDISES LEVINE, WILLIAM FUNDERBURK, JAMES CLARK, THOMAS PETERS, RICHARD BROWN, RICHARD TOM, ESKEL SOLOMON, DEBORA DORNY, DONNA STEVENER, DAVID ALEXANDER, STEPHEN KWOK, and PAUL BENDER. As discussed in more detail below, these activities include the following criminal schemes:

a. Collusive litigation practices related to lawsuits involving the City Attorney's Office and LADWP, which were fueled in at least one instance by a $2.175 million kickback from plaintiff's attorney JACK LANDSKRONER to attorney

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

PAUL PARADIS, a Special Counsel retained by the City Attorney's Office.

b. An $800,000 hush-money payment to a prospective whistleblower by Special Counsels PARADIS and PAUL KIESEL in exchange for silence as to collusive and potentially fraudulent litigation practices involving PARADIS, KIESEL, and THOMAS PETERS, then the Chief of Civil Litigation at the City Attorney's Office.

c. Offering of bribes by PARADIS, and acceptance of those bribes by LADWP General Manager DAVID WRIGHT and then-LADWP Board Vice President WILLIAM FUNDERBURK, in exchange for supporting at least one $30 million no-bid[1] LADWP contract to PARADIS's company.

d. LADWP's pattern and practice of falsifying records required by the Federal Energy Regulatory Commission ("FERC"), with the knowledge and approval of WRIGHT, LADWP Board President MELTON EDISES LEVINE, and other LADWP managers and Board members, in order to conceal and avoid responsibility for cybersecurity vulnerabilities related to the City's power grid, water supply, and other critical infrastructure.

e. Manipulation of LADWP contract processes by WRIGHT, LEVINE, other members of LADWP management and the LADWP Board, and members of the City Attorney's Office.

[1] A "no-bid" contract or "sole source contract" is a contract awarded without competitive bidding. Based on my training and experience, a government entity's award of large and lucrative "no bid" contracts can be (but is not always) an indication that improper and possibly illegal deals were made to secure that contract, or that the vendor was selected for reasons beyond its suitability for the job.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

f. Conspiracy and falsification of records by the President of the LADWP Board, other members of the LADWP Board, LADWP managers, and members of the City Attorney's Office, in order to obscure Board business from public scrutiny.

g. Payments to an Israeli broker to facilitate connections with foreign vendors vying for potential LADWP contracts, with the knowledge that the broker would receive kickbacks from foreign vendors who successfully obtained contracts with LADWP.

3. I am aware that the City receives in excess of $10,000 annually in federal funds through various programs.

4. While some of the evidence sought by the requested warrants could, under other circumstances, be obtained by other means, specific concerns about spoliation of evidence have compelled the government to seek the instant warrants. These concerns are detailed below in Section IV.

II. PURPOSE OF AFFIDAVIT

5. I make this affidavit in support of applications for eight search warrants,[2] described in more detail below, for:

a. Two search warrants for the initial seizure of information associated with nineteen e-mail accounts from two Providers;

b. Six search warrants for the premises of sixteen locations.

[2] A chart detailing each of the proposed search warrants is attached to my affidavit.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

A. Email Search Warrants

6. I make this affidavit in support of applications for two search warrants for the seizure of information associated with the following nineteen email accounts (collectively, the **TARGET ACCOUNTS**):

a. kiesel@kiesellaw.com, an e-mail account stored at premises controlled by Microsoft Corporation, and being used by PAUL KIESEL ("**KIESEL's ACCOUNT**");

b. david.wright@ladwp.com, an e-mail account stored at premises controlled by Microsoft Corporation, and being used by DAVID WRIGHT ("**WRIGHT's ACCOUNT**");

c. mel.levine@ladwp.com, an e-mail account stored at premises controlled by Microsoft Corporation, and being used by MELVIN EDISES LEVINE ("**LEVINE's CITY ACCOUNT**")[3];

d. william.funderburk@ladwp.com, an e-mail account stored at premises controlled by Microsoft Corporation, and being used by WILLIAM FUNDERBURK ("**FUNDERBURK's CITY ACCOUNT**");

e. [redacted], an e-mail account stored at premises controlled by Microsoft Corporation, and being used by WILLIAM FUNDERBURK ("**FUNDERBURK's PERSONAL ACCOUNT**");

[3] Many of LEVINE's e-mails involving LADWP business, as referenced herein, were sent to or from LEVINE's Gibson Dunn e-mail account. PARADIS proffered that on one or two occasions, he advised LEVINE to use **LEVINE'S CITY ACCOUNT** for LADWP Board business involving AVENTADOR, and that LEVINE would do so for a few weeks, but would then revert to using his Gibson Dunn account. I believe there is probable cause to believe that **LEVINE'S CITY ACCOUNT**, which PARADIS reported that LEVINE used on some occasions to discuss matters pertaining to AVENTADOR's work, will contain evidence of the criminal schemes and Target Offenses related to AVENTADOR as described herein.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

f. james.p.clark@lacity.org, an e-mail account stored at premises controlled by Microsoft Corporation, and being used by JAMES CLARK ("**CLARK's ACCOUNT**");

g. thom.peters@lacity.org, an e-mail account stored at premises controlled by Microsoft Corporation, and being used by THOMAS PETERS ("**PETER's ACCOUNT**");

h. richard.brown@ladwp.com, an e-mail account stored at premises controlled by Microsoft Corporation, and being used by BROWN ("**BROWN's ACCOUNT**");

i. richard.tom@ladwp.com, an e-mail account stored at premises controlled by Microsoft Corporation, and being used by RICHARD TOM ("**TOM's ACCOUNT**");

j. eskel.solomon@ladwp.com, an e-mail account stored at premises controlled by Microsoft Corporation, and being used by ESKEL SOLOMON ("**SOLOMON's ACCOUNT**");

k. deborah.dorny@ladwp.com, an e-mail account stored at premises controlled by Microsoft Corporation, and being used by DEBORAH DORNY ("**DORNY's ACCOUNT**");

l. donna.stevener@ladwp.com, an e-mail account stored at premises controlled by Microsoft Corporation, and being used by DONNA STEVENER ("**STEVENER's ACCOUNT**");

m. stephen.kwok@ladwp.com, an e-mail account stored at premises controlled by Microsoft Corporation, and being used by STEPHEN KWOK ("**KWOK's CITY ACCOUNT**");

n. [redacted], an e-mail account stored at premises controlled by Microsoft Corporation, and being used by STEPHEN KWOK ("**KWOK's PERSONAL ACCOUNT**");

o. david.alexander@ladwp.com, an e-mail account stored at premises controlled by Microsoft Corporation, and being used by DAVID ALEXANDER ("**ALEXANDER's ACCOUNT**");

p. [redacted], an e-mail account stored at premises controlled by Microsoft Corporation, and being used by DAVID ALEXANDER ("**ALEXANDER's PERSONAL ACCOUNT**");

q. marcie.Edwards@ladwp.com, an e-mail account stored at premises controlled by Microsoft Corporation, and being used by Marcie Edwards ("**Edwards' ACCOUNT**");

r. [redacted], an e-mail account stored at premises controlled by Microsoft Corporation, and being used by PAUL BENDER ("**BENDER's ACCOUNT**");

s. [redacted], an e-mail account stored at premises controlled by Google, Inc., and being used by PAUL BENDER ("**BENDER's PERSONAL ACCOUNT**").

7. Microsoft Corporation ("PROVIDER #1") is a provider of electronic communication and remote computing services, headquartered at Redmond, Washington. Google, Inc. ("PROVIDER #2") is a provider of electronic communication and remote computing services, headquartered at Mountain View, California (collectively the "PROVIDERS").[4]

[4] Because this Court has jurisdiction over the offenses being investigated, it may issue the warrant to compel the PROVIDER pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). See 18 U.S.C. §§ 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction") and 2711 ("the term 'court of competent jurisdiction' includes -- (A) any district court of the United States (including a magistrate

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

8. The information to be searched is described in Attachments A-1 and A-2. This affidavit is made in support of applications for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A) and 2703(d)[5] to require the PROVIDERS to disclose to the government copies of the information (including the content of communications) described in Section II of Attachment B-1 and B-2. Upon receipt of the information described in Section II of Attachment B-1 and B-2, law enforcement agents and/or individuals assisting law enforcement and acting at their direction will review that information to locate the items described in Section III of Attachment B-1 and B-2 subject to the search protocol and potential privilege review procedures outlined in Attachment B-1

judge of such a court) or any United States court of appeals that -- (i) has jurisdiction over the offense being investigated; (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title").

[5] The government is seeking non-content records pursuant to 18 U.S.C. § 2703(d). To obtain the basic subscriber information, which do not contain content, the government needs only a subpoena. See 18 U.S.C. § 2703(c)(1), (c)(2). To obtain additional records and other information--but not content--pertaining to subscribers of an electronic communications service or remote computing service, the government must comply with the dictates of section 2703(c)(1)(B), which requires the government to supply specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation in order to obtain an order pursuant to 18 U.S.C. § 2703(d). The requested warrant calls for both records containing content as well as subscriber records and other records and information that do not contain content (see Attachment B).

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

and B-2. Attachments A-1 and A-2 and B-1 through B-2 are incorporated herein by reference.

9. As described more fully below, I respectfully submit there is probable cause to believe that the information associated with the **TARGET ACCOUNTS** constitutes evidence, contraband, fruits, or instrumentalities of criminal violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 16 U.S.C. §§ 824o, 825o (Knowing and Willful Violation of Electric Reliability Standards)[6] (collectively, the Target Offenses).

B. Premises Search Warrants

10. This affidavit is made in support of applications for six warrants to search the following six premises that cumulatively include sixteen locations for evidence related to the criminal schemes and Target Offenses:

a. (Attachment A-3) 200 N. Main Street, Los Angles, California (“**City Hall East**”):

i. JAMES CLARK’s Office(“**CLARK’s OFFICE**”);

ii. File Storage Locations [specifically containing records of former employees, and files and records from litigation and other processes related to the Los Angeles

[6] The elements of this offense are as follows: Defendant (1) willfully and knowingly violated (2) any rule, regulation, restriction, condition, or order made or imposed by the Federal Power Commission under authority of the Federal Power Act (16 U.S.C. ss 791a, et seq.).

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Department of Water and Power billing system](“**City Attorney Storage Location**”).

b. (Attachment A-4) 111 N. Hope Street, Los Angeles, California (“**LADWP**”);

i. The Office of the General Manager(“**WRIGHT’s OFFICE**”);

ii. LADWP Commissioner’s Offices (Room #1555);

iii. LADWP Board Office, including work space used by LADWP Board Secretary and LADWP Board Assistants (Room #1555);

iv. LADWP Board Room (Room #1555-H);

v. LADWP Board file storage space outside LADWP Board Room (15th floor);

vi. STEPHEN KWOK’s Office (Room #1544)(“**KWOK’s OFFICE**”);

vii. [redacted] Office (Room #1221)(“[redacted]**s Office**”);

viii. DAVID ALEXANDER’s Office (Room #251) (“**ALEXANDER’s OFFICE**”).

c. (Attachment A-5) 221 N. Figueroa Street, 10th Floor, Los Angeles, California (“**City Property 10th Floor**”):

i. RICHARD TOM’s Office (10th floor, in or near Suite 1000)(“**TOM’s OFFICE**”);

ii. DEBROAH DORNEY’s Office (10th floor, in or near Suite 1000);

iii. ESKEL SOLOMON’s Office (10th floor, in or near Suite 1000).

d. (Attachment A-6) 5848 Miramonte Boulevard, Los Angeles, California ("**LADWP Records Retention**");

e. (Attachment A-7) 221 N. Figueroa Street, 15th Floor, Los Angeles, California ("**City Property 15th Floor**"):

i. AVENTADOR/ARDENT Office's (15th Floor – North side of building) ("**AVENTADOR/ARDENT OFFICE**").

f. (Attachment A-8) 8648 Wilshire Boulevard, Beverly Hills, California which is known as Kiesel Law, LLP ("**KIESEL's OFFICE**").

11. In connection with the investigation into this matter, the requested search warrants seek authorization to search the above-referenced premises for the items to be seized described in Attachments B-3 through B-8, respectively, that constitute evidence of the criminal schemes and evidence or fruits of violations of the Target Offenses. Attachments A-3 through A-8 and B-3 through B-8 are incorporated herein by reference.

12. The facts set forth in this affidavit are based upon my personal observations, my training and experience, information obtained from other agents and witnesses, consensually recorded conversations, and information obtained from the prior related search warrants, as detailed further below. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

III. BACKGROUND ON SUBJECTS[7]

15. Based on my knowledge of the investigation, below is general background on certain subjects. Although this investigation currently has other subjects, this affidavit focuses on the subjects most relevant to the requested search warrants.

16. PAUL PARADIS is an attorney and partner at Paradis Law Group, PLLC, operating in New York and Los Angeles. In 2015, PARADIS was appointed as Special Counsel for the City in a civil litigation against PricewaterhouseCoopers ("PwC") regarding an alleged faulty billing system, (Superior Court of California, captioned *City of Los Angeles v. PricewaterhouseCoopers*, Case No. BC574690 ("PwC Case")).

17. On March 15, 2019, I initially interviewed PARADIS, in the presence of his attorney, regarding his involvement in the criminal schemes and Target Offenses detailed herein pursuant to a proffer agreement. [8] I have subsequently interviewed PARADIS on numerous occasions.[9] PARADIS has no criminal record and has

[7] Unless otherwise noted, the e-mail communications described throughout this affidavit involved the **TARGET ACCOUNTS** identified in this section per individual.

[8] Under the terms of the proffer sessions discussed herein, the government is allowed to make derivative use of the information provided to it. The government agrees only not to use the information against the provider of the information in the government's case-in-chief against that person, provided the person is entirely truthful in proffer sessions.

[9] Where possible at this early stage of the investigation, I have attempted to corroborate PARADIS's proffer statements with independent evidence. However, these efforts are presently complicated by the fact that many of the relevant communications may implicate attorney-client privilege or attorney work

agreed to assist the government in exchange for favorable consideration in a potential future prosecution of him related to his conduct in this matter. At my direction, PARADIS has conducted multiple consensual recordings with certain subjects, including WRIGHT and LEVINE, in the investigation, some of which are detailed herein.[10]

15. JACK LANDSKRONER is a Cleveland-based attorney and partner at Landskroner, Grieco, Merriman, LLC. LANDSKRONER was a counsel for Antwon Jones in a civil litigation against the City (Superior Court of California, captioned *Jones v. City of Los Angeles*, Case No. BC577267 ("*Jones v. City*")).

a. On March 14, 2019, I interviewed LANDSKRONER, in the presence of his attorney and pursuant to a proffer agreement, regarding his involvement in the Target Offenses pursuant to a proffer agreement. LANDSKRONER has no criminal record and has agreed to assist the government in exchange for favorable consideration in a future prosecution of him related to his conduct in this matter.

---

product. The FBI and the U.S. Attorney's Office are working to resolve these issues through a combination of filter reviews, requests for waivers, and on June 26, 2019, a request for a judicial determination on the crime/fraud exception was filed with the Court and remains pending before the Court.

[10] As of July 18, 2019, PARADIS has conducted at least fifty hours' worth of recordings with numerous relevant persons in the investigation. I received debriefings from PARADIS regarding each of these recordings; however, due to the high volume, I have not yet listened to each part of every recording. Except where explicitly noted, any citation to a recording in this affidavit means I have reviewed that recording and/or reviewed a detailed summary thereof prepared by other FBI personnel who have reviewed that recording.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

16. PAUL KIESEL is a Beverly Hills-based attorney and partner at Kiesel Law LLP. Along with PARADIS, KIESEL was retained as local Special Counsel for the City in the PwC litigation.

a. Based on review of Kiesel Law LLP's website, the firm is located at 8648 Wilshire Blvd, Beverly Hills, California ("**KIESEL's OFFICE**").

b. Based on review of email communications, I know that KIESEL used kiesel@kiesel.law ("**KIESEL's ACCOUNT**") for the communications detailed below.

17. DAVID WRIGHT is the General Manager of the Los Angeles Department of Water and Power ("LADWP"). WRIGHT originally joined LADWP in February 2015 as the Senior Assistant General Manager and then became Chief Operating Officer before being appointed as General Manager in September 2016. According to LADWP's website, WRIGHT spearheaded major LADWP initiatives to restore customer trust in the utility, and to create a clean energy future and a sustainable water supply for Los Angeles. On or around June 14, 2019, the Mayor's office announced that WRIGHT would retire on October 1, 2019. On July 16, WRIGHT provided an email chain indicating that the Mayor's office intended to transition the LADWP General Manager role to WRIGHT's replacement commencing on July 23, 2019, with WRIGHT continuing to serve as an advisor to the General Manager.

a. On April 18, 2019, the Honorable Jacqueline Chooljian, United States Magistrate Judge, authorized search warrants for WRIGHT's phone, WRIGHT's laptop, two of WRIGHT's

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

email addresses, and two of WRIGHT's Apple iCloud accounts (collectively, the "April 2019 search warrants"). On June 4, 2019, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized search warrants for two of WRIGHT's residences, **WRIGHT's OFFICE**,[11] WRIGHT's cellular phone, and a burner cellular phone that the FBI had surreptitiously provided to WRIGHT; on June 18, 2019, Judge Walsh authorized a subsequent search warrant for WRIGHT's Riverside residence (collectively, the "June 2019 search warrants"). The April 2019 and June 2019 search warrants and their supporting affidavits are incorporated herein by reference, and copies can be made available for the Court.

b. On June 6, 2019, I interviewed WRIGHT after he waived his Miranda rights. I have since interviewed WRIGHT on several occasions, in the presence of his attorney and pursuant to a proffer agreement, regarding his involvement in the criminal schemes and the Target Offenses described herein.

c. WRIGHT has no criminal record and has agreed to assist the government in exchange for favorable consideration in a potential future prosecution of him related to his conduct in this matter. At my direction, WRIGHT has conducted multiple consensual recordings with certain subjects, including LEVINE, in the investigation, some of which are detailed herein.

d. Based on my review of LADWP's website and information I received in interviews, I know WRIGHT to utilize the Office of the General Manager of the John Ferraro Building

[11] For operational reasons, this warrant was not executed.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

located at 111 N. Hope Street, Los Angeles, California for his LADWP work ("**WRIGHT's OFFICE**").

e. Based on review of email communications, I know that WRIGHT used david.wright@ladwp.com ("**WRIGHT'S ACCOUNT**") communications detailed below.

18. MELTON EDISES LEVINE is a Los Angeles-based attorney and counsel at Gibson, Dunn, & Crutcher, LLP. LEVINE is also the President of the LADWP Board of Commissioners ("LADWP Board"). LEVINE is a former United States Congressman from California, having served in the United States House of Representatives from 1983 to 1993.

a. Based on review of email communications, I know that LEVINE used mel.levine@ladwp.com ("**LEVINE'S ACCOUNT**") communications detailed below.

19. WILLIAM FUNDERBURK is a Los Angeles-based attorney and former Vice-President of the LADWP Board.

a. Based on my review of email communications related to the Target Offenses, I know that FUNDERBURK used [redacted] ("**FUNDERBURK's ACCOUNT**") for the communications detailed below.

b. Based information I received in interviews, FUNDERBURK also used william.funderburk@ladwp.com ("**FUNDERBURK's CITY ACCOUNT**").

20. JAMES CLARK is the Deputy Chief for the Los Angeles City Attorney and a retired partner with Gibson, Dunn & Crutcher, LLP ("Gibson Dunn").

a. On June 4, 2019, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized a search warrant for CLARK's email account on the Gibson Dunn server (the "CLARK GDC email warrant"), which CLARK used for his City Attorney's Office business and in furtherance of the criminal schemes and Target Offenses described herein. That warrant and its supporting affidavit are incorporated herein and can be made available to the Court.[12]

b. Based on review of email communications, I know that CLARK used james.p.clark@lacity.org ("**CLARK's ACCOUNT**") for relevant communications detailed below. As further described in the affidavit in support of the CLARK GDC email warrant, CLARK auto-forwarded his City Attorney's Office emails to his Gibson Dunn account. Unless otherwise noted, CLARK's communications referenced herein were sent to or from **CLARK's ACCOUNT**.

21. THOMAS PETERS was the former Chief of the Civil Litigation Branch of the LA City Attorney's Office. PETERS abruptly resigned from his position on or about March 22, 2019, in the wake of allegations that he received money from plaintiffs' firms who had lawsuits against the City. PETERS oversaw the City's civil litigation in the PwC Case.

[12] The search warrant for CLARK's GDC email account was not executed after Gibson Dunn 1) agreed to produce the requested material [redacted] and 2) reversed its earlier position regarding intended disclosure by agreeing to [redacted] subject to the terms of the nondisclosure order that was issued with the search warrant.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. Based on review of email communications, I know that PETERS used thom.peters@lacity.org ("**PETER's ACCOUNT**") for the communications detailed below.

22. RICHARD BROWN is a former Assistant City Attorney and the former General Counsel for LADWP.

a. Based on review of email communications, I know that BROWN used Richard.brown@ladwp.com ("**BROWN's ACCOUNT**") for the communications detailed below.

23. RICHARD TOM is an Assistant City Attorney and the Assistant General Counsel for LADWP.

a. Based on review of email communications, I know that TOM used Richard.tom@ladwp.com ("**TOM's ACCOUNT**") for the communications detailed below.

24. ESKEL SOLOMON is an Assistant City Attorney assigned to LADWP.

a. Based on review of email communications, I know that SOLOMON used eskel.solomon@ladwp.com ("**SOLOMON's ACCOUNT**") for the communications detailed below.

25. DEBORAH DORNY is an Assistant City Attorney assigned to LADWP.

a. Based on review of email communications, I know that DORNY used Deborah.dorny@ladwp.com ("**DORNEY's ACCOUNT**") for the communications detailed below.

26. DONNA STEVENER is the Chief Administrative Officer for LADWP.

a. Based on review of email communications, I know that STEVENER used donna.stevener@ladwp.com (“**STEVENER’s ACCOUNT**”) for the communications detailed below.

27. DAVID ALEXANDER was previously the Chief Information Security Officer (“CISO”) at LADWP. In approximately March 2019, he was promoted from that position to the Chief Cyber Risk Officer.

a. Based on review of email communications, I know that ALEXANDER used David.Alexander@ladwp.com (“**ALEXANDER’s CITY ACCOUNT**”) and [redacted] (“**ALEXANDER’s PERSONAL ACCOUNT**”) for relevant communications detailed below.

28. STEPHEN KWOK is the CISO of LADWP.

a. Based on review of email communications, I know that KWOK used Stephen.kwok@ladwp.com (“**KWOK’s CITY ACCOUNT**”) and [redacted] (“**KWOK’s PERSONAL ACCOUNT**”) for relevant communications detailed below.

29. PAUL BENDER was appointed by the presiding Los Angeles Superior Court judge as the “independent monitor” for the City related to the settlement of the Jones Case.

a. Based on review of email communications, I know that BENDER used [redacted] (“**BENDER’s ACCOUNT**”) and [redacted] (“**BENDER’s PERSONAL ACCOUNT**”) for relevant communications detailed below.

IV. OTHER RELEVANT PERSONS AND ENTITIES

30. MARCIE EDWARDS is the former General Manager for LADWP. She retired in or around August 2016.

a. Based on review of email communications, I know that Edwards used Marcie.Edwards@ladwp.com ("**EDWARDS' ACCOUNT**") for the communications detailed below.

31. GINA TUFARO is a New York-based attorney and the law partner of PARADIS.

a. On June 19, 2019, I interviewed TUFARO in the presence of her attorney [redacted].[13]

32. MICHAEL LIBMAN is a Los Angeles-based attorney. Along with LANDSKRONER, LIBMAN represented plaintiff Antwon Jones as local counsel in the *Jones v. PwC* case.

33. CYNTHIA MCCLAIN-HILL is a Los Angeles-based attorney and the current Vice President of the LADWP Board.

34. BARUCH ("BOOKY") OREN is an Israel-based broker with a utilities-based consulting firm, Booky Oren Global Water Technologies LTD.

35. LOS ANGELES DEPARTMENT OF WATER AND POWER ("LADWP") is, according to its website, the nation's largest municipal utility, with a $7.5 billion annual budget for water, power and combined services. LADWP is responsible for a Power System that provides over 26 million megawatt-hours of electricity per year to over 1.5 million electric services, and a Water System that delivers 160 billion gallons of water per year to 681,000 services in the City. LADWP has a workforce of approximately 10,000 employees. As the user, owner, or operator of a bulk-

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

power system, the LADWP is required to follow the reliability standards approved by the Federal Power Commission.

36. THE LOS ANGELES CITY ATTORNEY'S OFFICE, according to its website, "writes every municipal law, advises the Mayor, City Council and all city departments and commissions, defends the city in litigation, brings forth lawsuits on behalf of the people and prosecutes misdemeanor crimes[.]"

37. AVENTADOR UTILITY SOLUTIONS, LLC ("AVENTADOR") is a cybersecurity company incorporated by PARADIS on or about March 29, 2017. Around March 2019, AVENTADOR was sold at below-market value to another owner and changed its name to ARDENT CYBER SOLUTIONS, LLC ("ARDENT").

38. CYBERGYM, according to its website, "is a joint venture of the Israel Electric Corporation, a 7.7 billion USD company that faces countless cyberattacks on a daily basis, and Cyber Control, Israel's leading cybersecurity consultancy established by ex-NISA operatives and security experts. CYBERGYM conducts cyber-warfare readiness training for governmental and private enterprises. It focuses on the weakest link in any emergency response system – the people who run it."

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

V. STATEMENT OF PROBABLE CAUSE

A. The Underlying Civil Litigation[14]

1. Collusive Litigation Practices between the Los Angeles City Attorney's Office, PARADIS, PAUL KIESEL, and JACK LANDSKRONER

a. Initial Stages of the City's Contemplated Litigation Against PwC

39. In 2013, LADWP implemented a new billing system pursuant to a contract with PwC. Upon implementation of the system, widespread billing errors ensued. On December 8, 2014, an overbilled LADWP ratepayer named Antwon Jones retained New York-based attorney PAUL PARADIS to represent him in a lawsuit for damages related to a $1300 overcharge by LADWP.[15]

40. On or about December 16, 2014, PARADIS and Beverly Hills-based attorney PAUL KIESEL, serving as local counsel, met

---

[14] The facts surrounding the collusive litigation scheme are complex and we continue to investigate its various parts and culpable parties. The investigation has been further complicated by invocations of privilege as to many of the underlying communications. The information herein represents my best understanding of this evolving landscape, based on court filings in the underlying litigation, deposition transcripts, deposition exhibits, witness interviews, proffers with co-conspirators, and communications and other documents received or seized from various parties, among other sources. Where a relevant fact is known to me to be materially in dispute, I have so stated to the best of my ability and knowledge.

[15] PARADIS maintains that Jones retained him to sue PwC, and CLARK, PETERS, and KIESEL have also testified to that understanding. However, Jones has testified that his intent at all times was to sue the City (not PwC), which he eventually did.

I am aware of no wrongdoing by Jones. In early 2015, four other class action lawsuits were filed against LADWP and the City of Los Angeles alleging damages related to overbilling. These lawsuits were filed by other attorneys not referenced herein; I am aware of no wrongdoing by those attorneys or plaintiffs.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

at the City Attorney's Office with then-Chief of Civil Litigation THOMAS PETERS to discuss the possibility of obtaining LADWP information in support of a prospective ratepayer action involving the overbilling. PETERS was KIESEL's former law partner.[16]

41. At or shortly after the December 16, 2014 meeting, personnel from the City Attorney's Office retained PARADIS and KIESEL to represent the City as Special Counsel in a contemplated affirmative lawsuit related to the overbilling (*City v. PwC*).[17] According to deposition testimony by CLARK and information proffered by PARADIS, CLARK knew in December 2014 that PARADIS represented Antwon Jones.[18]

---

[16] PETERS resigned from the City Attorney's Office on or about March 22, 2019, in the wake of allegations that he received referral income from plaintiffs' attorneys who had filed lawsuits against the City.

[17] The contract formalizing PARADIS's and KIESEL's retention as Special Counsel for the overbilling matter was issued on or about April 21, 2015, and approved by the City Council on or about April 23, 2015. However, the agreement was backdated to January 1, 2015, and CLARK testified that PARADIS's and KIESEL's effectively commenced in December 2014.

[18] From court filings and deposition transcripts, I have learned that in conducting pretrial discovery to prepare for trial in the lawsuit brought by the City, PwC noticed a "Person Most Qualified" or "PMQ" deposition, which required the City to provide a witness who had conducted any necessary investigation to allow the witness to testify knowledgeably about the deposition topics. PETERS was offered as the initial PMQ deponent and was represented by PARADIS. PETERS appeared at the deposition on September 13, 2018, but he brought no documents responsive to the subpoena, testified that he had conducted no investigation, refused to answer most questions on grounds of privilege that were later overruled, and offered little or no relevant information in response to the questions. In the middle of the deposition, PETERS abruptly walked out. The court denied the City's subsequent motion for a protective order and granted PwC's motion to compel the City's PMQ deposition.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

42. The day after the December 16, 2014 meeting, PARADIS sent PETERS an email, which I have reviewed, stating that his team was "already hard at work on the draft complaint you requested" and asking for specific internal LADWP documents to aid in that effort. Subsequent emails reflect that PARADIS received those internal documents from LADWP to use in drafting the *City v. PwC* complaint, and that on January 5, 2015, PARADIS sent a draft *City v. PwC* complaint to PETERS for review and consideration by the City Attorney's Office.

43. Around the time that the City Attorney's Office retained PARADIS and KIESEL and directed them to begin pursuing the *City v. PwC* action, the City Attorney's Office also began exploring the possibility of arranging for a class of ratepayers to sue PwC for damages. Members of the City Attorney's Office believed that a ratepayer suit against PwC would benefit it politically and financially because it would inoculate the City against lawsuits by ratepayers. They also saw a strategic

---

On February 26, 2019, CLARK appeared for the second attempt at the City's required PMQ deposition. At this deposition, CLARK was represented by PETERS. During the deposition, CLARK disclosed that he had taken four or five pages of handwritten notes during the course of his investigation to prepare for the PMQ deposition, but that he had discarded those notes. Having destroyed his investigative notes that he described as "a method to remember things," CLARK testified repeatedly during the deposition that he did not recall relevant facts. For example, while describing his investigation, CLARK was asked what facts he had learned from Assistant City Attorney DEBORAH DORNY. CLARK replied, "I'm not going to be able to do this, Counsel. I —— I don't remember which facts which person told me about."

Following the first day of his PMQ deposition, CLARK submitted a lengthy "errata" list of answers that he wished to withdraw, reverse, or otherwise substantively change, as further described herein.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

advantage in taking the negative media attention then centered on LADWP and refocus it against PwC, which members of the City Attorney's Office described as the "real culprit" and the "villain." For that reason, CLARK and PETERS directed PARADIS, as Special Counsel for the City, to draft a complaint in a contemplated lawsuit by Jones (PARADIS's client) against PwC ("*Jones v. PwC*").[19] PARADIS did so, and in January 2015, he sent copies of the draft complaint both to his client Jones, and to personnel at the City Attorney's Office.[20]

44. At his deposition, PETERS described the draft Jones v. PwC complaint as a "thought experiment" and stated that it was never intended to be filed. I believe[21] that the communications described herein, many of which came to light only after PETERS so testified, demonstrate that this sworn statement by PETERS was untrue.

---

[19] CLARK testified that in December 2014, he directed PETERS to have the *Jones v. PwC* complaint prepared.

Throughout their depositions, CLARK and other lawyer-witnesses regularly couched their affirmative responses in terms such as "I think" and "I believe." Other than where answers are quoted verbatim, I have omitted these boilerplate qualifiers for the sake of readability. Where a response appears to reflect actual or significant uncertainty, I have so noted.

[20] In his deposition, Chief Deputy City Attorney CLARK testified that he likely advised City Attorney Michael Feuer of the existence of the draft *Jones v. PwC* complaint. CLARK further testified that the draft complaint was also forwarded to the LADWP Board, and that LADWP Board President LEVINE was also involved in decisions relating to the draft complaint.

[21] Unless otherwise stated, my "belief statements" are based on my training, experience, and knowledge of this investigation.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. The City's Pursuit of a Toll-and-Dismiss Strategy and Tandem Litigation Against PwC

45. By mid-January 2015, the City Attorney's Office decided to try to obtain voluntary dismissals of the existing class action lawsuits against LADWP, and to invite counsel for those classes to join a future ratepayer complaint against PwC. Accordingly, the City Attorney's Office directed PARADIS and KIESEL to contact the class counsel and provide draft agreements by which the statute of limitations would be tolled while this alternative course was pursued. PARADIS and KIESEL sent the draft tolling agreements to the existing class counsel, obtained signatures, and forwarded the signed agreements to PETERS.

46. On or about January 23, 2015, Assistant City Attorney ESKEL SOLOMON distributed via e-mail to other Assistant City Attorneys and LADWP personnel the draft *City v. PwC* and *Jones v. PwC* complaints and called for a meeting to discuss the City's intended strategy to orchestrate both cases. In this email, SOLOMON referenced "a significant positive development in the class action billing case(s)." SOLOMON warned the recipients that "you are not to discuss [the attached draft *Jones v. PwC* complaint] with anyone."

47. Based on the context of this and other contemporaneous documents and my knowledge of the investigation, I understand SOLOMON's discussion of "a significant positive development in the class action billing case(s)" to refer to the toll-and-dismiss strategy and tandem litigation against PwC that the City then wanted to pursue.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

48. Three days later, on January 26, 2015, SOLOMON's assistant forwarded the above-referenced email chain to CLARK and PETERS and advised that any questions should be directed to Assistant City Attorney DEBORAH DORNY. Later on January 26, 2015, CLARK replied to all to ask what the meeting was about, and advised that he would not be available at the appointed time. Assistant City Attorney (and Assistant General Counsel to LADWP) RICHARD TOM replied to all advising CLARK that this meeting was intended to make LADWP internal staff available to PARADIS and KIESEL "for purposes of vetting the draft complaints." TOM further opined that CLARK and PETERS did not need to attend this meeting, but suggested scheduling a follow-up meeting with CLARK and PETERS for two days later to determine whether CLARK and City Attorney Michael Feuer had any questions or a decision on how to proceed.

49. In a January 26, 2015 email to KIESEL, CLARK reported that City Attorney Feuer was "completely on board" with the strategy of first tolling and dismissing the existing lawsuits, and then joining forces with the existing class counsel in a new ratepayer suit against PwC to be litigated by PARADIS and KIESEL.[22] CLARK further stated in the email that he was "100% sure" that LADWP Board President LEVINE would also be fine with

[22] City Attorney Feuer's involvement in the strategy is further suggested in a February 2, 2015 email from KIESEL to PETERS setting out a timeline for working toward simultaneous filing of the two complaints —— with the *LADWP v. PwC* complaint to be filed first and the ratepayer case against PwC second —— on February 11, 2015, to be followed by a "a 'joint' press conference" at City Hall. The timeline indicates the need for a meeting on February 6, 2015, with Feuer, CLARK, PETERS, PARADIS, and KIESEL.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

it, and that he was working to get LEVINE's "sign off" before formally approving the strategy. In the next several days, the City Attorney's Office obtained signatures from both existing class counsel on tolling agreements. Nonetheless, by early February 2015, the City Attorney's Office's "toll-and-dismiss" strategy had fallen apart due to the class counsel's ultimate reluctance to dismiss the existing lawsuits against the City of Los Angeles.

50. I believe that the above-referenced January 26, 2015 emails indicate that the City Attorney's Office was at least in part involved in formulating the strategy to direct and control a ratepayer lawsuit against PwC, which would be filed by Special Counsels PARADIS and KIESEL, in coordination with a tandem City lawsuit against PwC (which would also be filed by Special Counsels PARADIS and KIESEL), and that this strategy was ultimately approved by City Attorney Feuer and Board President LEVINE.

c. Development of the "White Knight" Strategy

51. On February 17, 2015, a law firm defending the City against the existing class action overbilling cases sent a memo to SOLOMON and DORNY outlining certain concerns with the City's plan to have PARADIS and KIESEL represent both a ratepayer and LADWP in parallel suits against PwC. In addition to strategic and practical issues, the memo noted the potential for an ethical conflict in the likely event that PwC joined[23] LADWP as a

[23] In a civil lawsuit, a defendant claiming that a third party may bear all or part of the liability claimed by the plaintiff can "join" or bring that third party into the suit.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

defendant in the ratepayer case, which would leave PARADIS and KIESEL representing two adverse parties in the resulting three-party suit. That is, PARADIS and KIESEL would be representing (a) the City as plaintiffs against PWC and (b) ratepayer plaintiffs against the City, all related to the same overbilling conduct. This memo and a follow-up email from the law firm were subsequently forwarded to other officials at the City Attorney's Office including CLARK, PETERS, BROWN, and TOM.

52. After these concerns were circulated, and in the wake of the failed attempt to gather support for the toll-and-dismiss strategy, the City Attorney's Office abandoned its strategy of parallel lawsuits by a ratepayer and LADWP against PwC.[24] KIESEL has testified that after this strategy fell apart, he attended a meeting in late February 2015 with CLARK, PETERS, and PARADIS, at which CLARK and PETERS agreed to use Jones, whom they knew to be represented by PARADIS, as the vehicle to achieve the City Attorney's Office's goals in settling the overbilling litigation on the favorable terms and obtaining a release sufficiently broad to resolve all existing claims against the City.[25]

---

[24] At his deposition, KIESEL testified that the law firm memo which raised ethical concerns with the City Attorney's Office's strategy resulted in "the end of the discussion with regard to [PARADIS and KIESEL] being involved with a ratepayer action against PricewaterhouseCoopers." Moreover, CLARK testified that the other class counsel's unreasonableness in refusing to toll their claims against the City operated in favor of LANDSKRONER as the "more reasonable" choice of opposing counsel. Immediately after so testifying, CLARK denied using those words (which were recorded by the court reporter and heard by the deposing attorney).

[25] KIESEL's testimony about this February 2015 meeting is consistent with information proffered by both PARADIS and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

According to KIESEL, PARADIS, and TUFARO, the City Attorney's Office came to refer to this plan as the "White Knight Complaint" strategy.

53. In his deposition, CLARK identified the following three goals that the City Attorney's Office hoped to achieve in resolving the ratepayer claims: 1) to refund 100% of the money that had been wrongfully overpaid due to billing errors; 2) to remediate PwC's CC&B billing system, which the City Attorney's Office blamed for the errors; and 3) to obtain a release sufficiently broad to cover all of the diverse claims made against the City by all of the class-action plaintiffs. CLARK acknowledged that the City did not need litigation to accomplish the first two of these three goals. CLARK further stated his view that the City had an obligation to return the money it had wrongfully taken from ratepayers.

TUFARO. Both CLARK and PETERS have filed sworn declarations in the state court litigation attesting that they did not attend such a meeting. CLARK's declaration unequivocally stated that he had never taken any action to facilitate a lawsuit being filed against a client that he represented and never participated in any decision about such an action. These statements appear to be irreconcilable with CLARK's repeated statements during the first day of his PMQ deposition (further discussed herein) that he was aware that a suit would be filed against the City (his client) before it happened, that he was involved in discussions involving the selection of plaintiff's counsel for that lawsuit against his client, and that he knew that the City was providing other complaints to aid plaintiff's counsel in drafting a complaint that would cover all the existing causes of action against his client. (For example, "As I said, a few days before [April 1, 2015], I'm sure, in discussion who's going to represent Mr. Jones against the City, I'm sure I heard [LANDSKRONER'S] name.")

The date of this alleged meeting is unknown, but KIESEL testified that it was between February 17, 2015 (the date of the law firm memo) and March 3, 2015, when emails reflect that the draft *Jones v. City* complaint was being prepared.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

54. In a proffer, WRIGHT informed me that he recalled being a part of a 2015 meeting with the City Attorney's Office and PARADIS in which CLARK directed PARADIS to "flip" Jones to LANDSKRONER so that the City Attorney's Office could control the settlement and that CLARK was the one who quarterbacked the strategy and the settlement of the Jones case. In addition, WRIGHT recalled a meeting with CLARK, PARADIS, TUFARO, PETERS, and WRIGHT prior to CLARK's deposition testimony in which this strategy, orchestrated by CLARK, was discussed. According to WRIGHT, CLARK's deposition testimony that he did not have knowledge of the Jones arrangements was false.

d. The City's Hand-Selection of Plaintiff's Counsel

55. KIESEL testified that at the February 2015 meeting where the White Knight Complaint strategy was conceived, PARADIS suggested to CLARK and PETER that LANDSKRONER be selected as the white knight counsel for Jones, and KIESEL identified MICHAEL LIBMAN to serve as local counsel.

56. In his deposition, **CLARK was asked whether the City Attorney's Office knew or expected the *Jones v. City* complaint before it was filed on April 1, 2015. CLARK replied, "I'm sure we knew before April 1, yes."**

57. **CLARK was also asked, "How much earlier than April 1 did you know that the settlement demand would be forthcoming at some point and that you would be settling with Mr. Jones?" CLARK replied, "Sometime during the latter half of —— the end of March."** After his deposition, CLARK submitted, through the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

City's new representative counsel, a signed and sworn document containing an "errata" list of several dozen transcribed answers that he wished to substantively change.[26] In his errata, CLARK retracted this answer and changed it to, "I didn't."

58. In his deposition, CLARK testified that he first learned that Jones would be suing LADWP in March 2015, after it became clear that the *Jones v. PwC* lawsuit was not going to go forward. CLARK further testified that after PARADIS concluded that he had a conflict in representing Jones against the City, which was PARADIS's client, CLARK was aware that PARADIS recommended that LANDSKRONER be brought in as Jones's new

---

[26] I understand that an "errata" is typically a vehicle after the deposition to correct minor form changes and transcription errors. Based on opinions offered by attorneys involved in the civil cases, including in-court representations by PwC's counsel on this topic, I believe it is unusual for an errata to be used as a mechanism for later substantively changing numerous answers to those that the deponent wished he had given during his testimony. CLARK was subsequently deposed again on two occasions and gave answers that were in relevant part inconsistent with his original testimony on the issues described herein and in line with the changed answers given in his post-deposition errata.

At the start of his second day of testimony, after the errata, CLARK began by reading from a prepared statement, in what counsel for the City and counsel for PwC agreed was an "unusual" procedure. In CLARK's statement, he blamed poor preparation and advice from his attorneys, as well as inaccurate information from the witnesses from whom he had gathered facts in conducting his pre-deposition investigation, for what he described as inaccurate testimony during his first day.

Because, for the reasons noted herein, I believe that CLARK's first day of testimony was largely truthful and the information provided in his errata and his later testimony was largely untruthful, the CLARK deposition testimony recounted herein is from the first day. Where CLARK signaled an intent to change that testimony in his errata, I have so indicated.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

counsel, and that CLARK assumed that someone at the City authorized that action. In his errata, CLARK disavowed his sworn testimony that "I assume somebody authorized it. That wasn't —— that wasn't me."

59. In a reply to a question as to why one of the existing class counsel was not recommended to Jones, CLARK testified as follows: "My understanding, and this is mostly from outside counsel, the Liner people, who have been trying to deal with Mr. Blood, [redacted], and I think there was another plaintiff's lawyer involved, too, that **they were just intransigent, couldn't —— they wouldn't —— didn't want to negotiate or propose things that were not —— were not acceptable.**[27] **And I don't know if they were willing to do what DWP wanted**, which was basically —— there would have been overcharge repaid and have the —— and have oversight of the system to correct it." In his post-deposition errata, CLARK retracted his lengthy substantive answer and changed it to, "I don't know what Mr. Paradis recommended to Mr. Jones."

60. At his deposition, CLARK was asked the following question: **"No one brought Mr. Landskroner into the case because he was viewed as someone who would be the most zealous advocate available for Mr. Jones to pursue claims; correct?" CLARK replied, "That's —— that's right."** In his errata, CLARK sought

[27] Court documents indicate that Mr. Blood and [redacted] represented class representatives in two of the other LADWP overbilling class actions that were filed before *Jones v. City*. Based on interviews and court documents, I understand "the Liner people" as a reference to the City's outside counsel at a law firm then known as Liner LLP.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to change his reply to, "I don't know why Mr. Paradis recommended him to Mr. Jones."

61. I believe that CLARK's initial deposition testimony —— that he and others at the City Attorney's Office knew about and approved 1) the *Jones v. City* litigation plan; 2) the selection of LANDSKRONER to represent the plaintiff because he was the most compliant counsel and would do what the City Attorney's Office wanted, as opposed to zealously advocate for his actual client (Jones); 3) the plan to rapidly settle the case on terms that the City Attorney's Office desired, including obtaining a broad release of all other causes of action —— was consistent with other evidence, including that the City Attorney's Office wanted a "white knight" plaintiff's counsel over whom they would have influence. CLARK's initial testimony is materially consistent with KIESEL's deposition testimony, information proffered by PARADIS and TUFARO, and documents made available through the deposition process. I further believe that when CLARK sought to change key parts of his initial deposition testimony through the use of an errata, it appeared designed to ameliorate damage to the City Attorney's Office that was done by the admissions he made in his initial deposition.

e. Filing of City v. PwC and Continued Preparations for Jones v. City

62. KIESEL testified that the White Knight Complaint strategy was appealing to the City Attorney's Office because it was facing three to four lawsuits, and it wanted to refund overbilled money in one lawsuit and did not want to be involved

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

in protracted litigation with multiple firms. The White Knight Complaint was thus intended to be sufficiently broad to encompass and subsume all existing claims. To accomplish this goal, an official from the City Attorney's Office provided copies of the existing complaints to PARADIS.[28]

63. On March 3, 2015, SOLOMON sent an email, marked with high importance,[29] to BROWN, DORNY, and TOM, to relay the following information arising from his call with KIESEL:

a. A Los Angeles Neighborhood Council Coalition ("LANCC") meeting was scheduled for Saturday March 7, 2015, and a presentation discussing LADWP billing matters was planned.

b. PARADIS and KIESEL were concerned about the meeting and presentation undermining LADWP.

c. In light of those concerns, **PARADIS and KIESEL were "arranging for the PwC lawsuit (and although [KIESEL] did not directly mention it, I assume also the consumer law suit)** to be filed" by Friday, March 6, 2015.

d. KIESEL and SOLOMON would attend the Saturday LANCC meeting, provide the website for accessing the complaint, indicate that LADWP was being proactive and pursuing PwC, and

---

[28] KIESEL testified that these complaints were provided to PARADIS by either SOLOMON or DORNY. This is consistent with information proffered by PARADIS. CLARK testified that PARADIS and LANDSKRONER had received copies of the complaints before the *Jones v. City* filing in order to facilitate preparation of a comprehensive complaint covering all causes of action. My review of the *Jones v. City* complaint indicates that it was indeed drafted to incorporate the causes of action in the existing complaints.

[29] "High importance" is a feature on an e-mail client that a sender can select to have a message stand out to the receiver.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

decline to discuss billing matters or provide the presentation because of the active litigation.

e. KIESEL had been working with CLARK and Feuer on the plan to present the "case(s)" to the media on Friday, March 6, 2015.

f. TOM and DORNY should determine whether to provide any of this information to then-LADWP General Manager Marcie Edwards or LADWP Board President LEVINE.

64. I believe that SOLOMON's aforementioned email shows the City Attorney's Office's knowledge and approval of the plan to coordinate the filings of two cases involving the LADWP billing situation, namely the *LADWP v. PwC complaint* that the City filed days later and "the consumer law suit" that had also been discussed. Since all available evidence appears to indicate that the City Attorney's Office's initial plan to facilitate a *Jones v. PwC* ratepayer lawsuit was abandoned by late February (after the toll-and-dismiss strategy fell apart and the City's external counsel circulated a memorandum articulating ethical concerns about the City's Special Counsel representing a ratepayer against PwC), I believe that this March 2015 email stating SOLOMON's assumption that a consumer ratepayer lawsuit would soon be forthcoming is a reference to the alternate plan to have a consumer sue LADWP via a white knight plaintiff's counsel. I further believe that SOLOMON's statement that CLARK and Feuer were working with KIESEL on "a plan to present the case(s) to the media" indicates that the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

City Attorney's Office was involved in the White Knight litigation strategy at the highest levels.

65. On March 5, 2015, TOM sent an email to CLARK, PETERS, BROWN, SOLOMON, DORNY, PARADIS, and KIESEL, among others, to request a meeting "to ensure that everyone is up to date on the status of the activities related to the DWP customer billing lawsuits" and to make a clear plan for those activities. TOM further provided a proposed agenda for the meeting and noted the LANCC meeting discussed in SOLOMON's above-referenced email.

66. On March 6, 2015, the City filed the complaint in *City v. PwC*, as forecast in SOLOMON's above-referenced email.

f. The Filing of Jones v. City, and Reaction by City Attorney's Office

67. On March 26, 2015, PARADIS introduced Cleveland-based attorney JACK LANDSKRONER to Jones via email, advising Jones that LANDSKRONER was an expert in municipal lawsuits who should join their legal team.[30] Jones retained LANDSKRONER on that date.

68. On April 1, 2015, LANDSKRONER filed a class-action lawsuit against the City with Jones as the lead plaintiff ("*Jones v. City*"). The complaint was signed by LANDSKRONER and Los Angeles-based attorney MICHAEL LIBMAN (serving as local

[30] Jones understood, at that time and throughout the course of his lawsuit against the City, that he was represented by both PARADIS and LANDSKRONER. PARADIS did not at any time (a) advise his plaintiff client Jones that PARADIS was also representing the defendant City on this matter, (b) advise Jones that he referred LANDSKRONER to Jones, at least in part, because LANDSKRONER was expected to be more compliant with the defendant City's interests (i.e., serve as the "white knight" counsel), or (c) seek to withdraw as Jones's counsel during the Jones's suit against PARADIS's other client, the City.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

counsel) as attorneys for plaintiff Jones. The complaint contained detailed nonpublic information, such as the numbers of ratepayers receiving certain types of utility services, which, as detailed above, PARADIS had obtained from the City in the course of his work as Special Counsel and provided to LANDSKRONER.[31] As noted above, personnel from the City Attorney's Office, including CLARK, were fully aware that the Jones complaint was going to be filed and settled before either happened.

69. On April 1, 2015, KIESEL forwarded to PARADIS a conformed copy of the filed complaint and asked what to do about service. PARADIS replied that LIBMAN should serve it, but noted that "Landskroner already emailed a courtesy copy to Richard Tom tonight (per Richard's [TOM]'s request to me [PARADIS])."

70. On April 2, 2015, SOLOMON forwarded a notification of the *Jones v. City* filing to TOM and DORNY, stating "I believe this is the expected new class action lawsuit."

71. On April 3, 2015, PETERS sent an email to SOLOMON, DORNY, TOM, CLARK, PARADIS, and KIESEL, stating, "FYI, an attorney named Michael Libman has filed the case listed below, which is described in [the electronic court record] as 'class action for overbilling.'" Later that day, KIESEL emailed PETERS separately and stated, "on the new class case you mentioned I

[31] The nonpublic nature of that information and the advantages it conferred to the Jones complaint over the other class-action lawsuits have been noted on the record by counsel for the other plaintiffs.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

want to give you the background on that case . . . I am aware of it. ☺ [smiley face emoji]" At his deposition, KIESEL testified that he used the smiley emoji in his response because he understood PETERS's email to be a "CYA email".[32] KIESEL further testified that everyone knew that the *Jones v. City* case was going to be filed, so the actual filing was obviously no surprise to anyone.

72. I believe that to the extent that PETERS's above email could be read to suggest a lack of prior awareness that the *Jones v. City* complaint would be filed, it shows his intent to mask the City's White Knight collusive litigation scheme, as corroborated by KIESEL's reply email. I believe that the City Attorney's Office's advance knowledge of the *Jones v. City* complaint, which CLARK testified to in his first day of deposition testimony, is further evidenced by PARADIS's April 1, 2015 email stating that TOM had already requested a courtesy copy of the complaint and had received it from LANDSKRONER, and by SOLOMON's April 2, 2015 description of the *Jones v. City* complaint as "the expected new class action lawsuit."

73. On April 21, 2015, SOLOMON sent an email to CLARK, PETERS, BROWN, TOM, DORNY, PARADIS, KIESEL, TUFARO, and others, indicating the following:

a. The class counsel in one of the other class actions called to discuss the possibility of amending his

[32] I understand "CYA" to be a commonly used acronym for "cover your ass," meaning a mechanism undertaken to protect oneself.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

complaint following the recent filing of the *Jones v. City* complaint.

b. There was an April 30, 2015 deadline for plaintiffs to file amended complaints.

c. "Considering the direction we intend to take, we have instructed" outside counsel for the City in the other overbilling class actions to return the call and to file a joint report with a briefing schedule by the April 30 deadline.

d. **"Finally, we think it is in our best interest to have the Libman/Landskroner Firms appear on April 30 and establish their active participation in the pending matters, and possible lead position, and will ask [outside counsel] to convey that message to them.** We will keep you advised."

74. The following day, SOLOMON replied-all to his above-referenced email with the subject line "CORRECTION RE EMAIL OF APRIL 21, 2015" (capitals in original). The text indicated that SOLOMON's correction was that he had given an inaccurate date for the next court hearing. SOLOMON otherwise affirmed the content of his earlier message indicating that the City was seeking to direct the attorneys representing Jones, the plaintiff who had sued the City, to act in a way that was in the City's best interest stating: **"We continue to believe that the Libman/Landskroner Firms need to appear on MAY 22 and establish their active participation in the pending matters, and possible lead position. [Outside counsel] will convey that message to them."**

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

75. I believe that these two emails from SOLOMON to CLARK, PETERS, BROWN, TOM, DORNY, PARADIS, KIESEL, TUFARO, and others shortly after the filing of the *Jones v. City* complaint, demonstrate the City Attorney's Office's direction of LANDSKRONER and LIBMAN, who ostensibly represented the class suing the City. I understand SOLOMON's statement that "it is in our [the City Attorney's Office's] best interest" to mean that the City Attorney's Office preferred LIBMAN/LANDSKRONER to serve as lead counsel because they were the "white knight" counsel, and placing them at the helm of the class action cases was part of the City Attorney's Office's strategy to benefit from this overbilling litigation. I further believe that the transmittal of these two emails to CLARK, PETERS, BROWN, and others at the City Attorney's Office shows that this was not a furtive scheme secretly coordinated by rogue actors or a single employee at the City Attorney's Office, but rather that the strategy was directed and approved by the City Attorney's Office more broadly.

g. Settlement of Jones v. City

76. On April 2, 2015, one day after the *Jones v. City* complaint was filed, LANDSKRONER sent a detailed settlement proposal to the City. PARADIS had prepared the settlement demand and emailed it to LANDSKRONER on March 24, 2015. According to CLARK in his first day of deposition, this immediate settlement overture was expected by the City Attorney's Office, which understood that after LANDSKRONER took

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

over in the last week of March 2015, he was going to file a lawsuit and then immediately reach out to settle the case.[33]

77. Following LANDSKRONER's transmittal of the settlement proposal that PARADIS had drafted, settlement negotiations quickly ensued in the *Jones v. City* case. The parties engaged in a mediation process, and PARADIS attended mediation sessions on behalf of the City notwithstanding that 1) PARADIS did not represent the City in the *Jones v. City* case, and 2) members of the City Attorney's Office responsible for overseeing the *Jones v. City* case knew that PARADIS represented or had represented Jones.

78. The terms of the settlement agreement, which received final approval from Judge Berle on July 20, 2017, were consistent with those originally desired by the City Attorney's Office. Specifically, the final settlement called for 100% reimbursement of overcharged ratepayers (as determined by LADWP and the City); a $20,000,000 remediation of the LADWP billing system; appointment of an independent monitor to oversee the remediation process;[34] and a release sufficiently broad to cover the claims alleged by the other class-action plaintiffs. The

[33] As noted above, CLARK subsequently recanted similar testimony from the first day of his deposition and gave conflicting testimony on subsequent days; however, this statement was not specifically identified as incorrect in his errata.

[34] According to PARADIS, he has largely controlled PAUL BENDER, the "independent monitor," including drafting many or all of BENDER's reports, at the direction of CLARK and others at the City Attorney's Office and with the oversight of WRIGHT. According to WRIGHT, BENDER confirmed to WRIGHT and LADWP Chief Administrative Officer DONNA STEVENER that PARADIS wrote most of BENDER's "independent monitoring" reports to the court.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

plaintiffs' attorneys were awarded approximately $19,000,000, of which more than $10,000,000 was paid to LANDSKRONER.

79. LANDSKRONER's fees were based on billing records reflecting work allegedly performed beginning in November 2014, four months *before* he ever met or was retained by his client (and before PARADIS ever contacted Jones). LIBMAN's fees, which totaled approximately $1,300,000, were based on billing records indicating work beginning in 2013, *before* Jones had even received the inflated LADWP bill leading him to seek an attorney. In my review of evidence in this case, I have not yet seen anything reflecting any substantive work that LIBMAN performed on this case. Based on LIBMAN's receipt of a seven-figure attorney's fee for a case on which he did little or no actual work, and based on information that PETERS took "referral" fees from other plaintiffs' firms with cases before the City[35] and further evidence that PETERS and KIESEL were involved in other dual representation schemes involving the City Attorney's Office[36], I believe LIBMAN may have provided an illegal kickback to a Special Counsel or official at the City/City Attorney's Office in return for his lucrative fee for his minor role in this case.

80. According to CLARK, the City was not concerned about ensuring that the attorneys' fees reflected hours that they actually worked in connection with the case. CLARK further

[35] According to media reports and deposition testimony, these allegations were the basis for PETERS's abrupt resignation from the City Attorney's Office in March 2019.

[36] This evidence is further described below.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

testified that the City agreed to the eight-figure attorneys' fee figure without having seen the hours that the attorneys worked.

81. On November 10, 2017, LANDSKRONER covertly paid $2,175,000 of his earnings from the *Jones v. LADWP* settlement fees to PARADIS as a "referral fee." LANDSKRONER made this payment using a sham real estate investment company, S.M.A. PROPERTY HOLDINGS, LLC, which PARADIS and LANDSKRONER had set up for that purpose.[37] I believe that this may have constituted an illegal kickback to PARADIS, who at that time represented the City as Special Counsel in the LADWP v. PwC litigation.

82. I believe that the above facts constitute probable cause to believe that evidence of the criminal schemes and Target Offenses, including conspiracy, wire fraud, federal program bribery, deprivation of honest services, and money laundering will be found in the Target Accounts and premises referenced above.

2. The City's Filing of Selected Documents

83. As further noted herein, in late April 2019, the City filed approximately two dozen emails that it alleged had just been discovered in a .pst file[38] on a hard drive, later revealed to belong to PETERS. The City's filing represented that none of the newly discovered emails were sent to or from a City employee

[37] This information was proffered by both PARADIS and LANDSKRONER and corroborated by bank records and other documentation that I have reviewed.

[38] A .pst file is a personal folder file in Microsoft Outlook. "PST" stands for personal storage.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

or officer, and it was accompanied by a media statement in which the City Attorney denounced Special Counsel, PARADIS and KIESEL, and decried their "reprehensible breach of ethics" of which the City was ostensibly unaware. Subsequently, other emails beyond those selected by the City to fit its narrative of Special Counsel acting as rogue elements —— including many to and from City employees and officials as described herein —— were also revealed to be in the .pst file.

84. At day two of his deposition in the days after the City's filing of selected emails, CLARK testified to his understanding, learned through counsel, that PETERS "had never seen the documents before, and was outraged" when he learned about them. CLARK also testified that to his knowledge, no emails on the .pst file were sent to or from City employees or officials. CLARK further testified that he himself was "outraged, angry, disgusted" upon reading the emails that the City had selected for release. As detailed herein, KIESEL subsequently revealed documents indicating that many of the emails from the same .pst file but which that the City had elected not to release in its filing were sent to or from City officials and employees, including CLARK and PETERS.

85. Later, after metadata for the .pst file showed that PETERS had downloaded the contents of the .pst file from a Dropbox link and saved them to his hard drive, PETERS gave sworn testimony acknowledging that he had done so, but stating that he had no recollection of doing so or of reading the emails.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

86. Based on this chronology and review of the aforementioned court filing, the relevant deposition testimony, and the later-revealed emails, I believe that the City's filing contained false or misleading statements designed to erroneously portray PARADIS and KIESEL as rogue actors who secretly engaged in unethical or unlawful conduct without the City's knowledge when in fact, as described herein, PARADIS's and KIESEL's unethical and/or illegal conduct with respect to the collusive litigation scheme described herein was known by several officials at the City Attorney's Office.

3. Hush Money to Conceal Collusive Litigation Practices[39]

87. PARADIS proffered information indicating that in 2017, he and KIESEL paid $800,000 to a former KIESEL employee to buy her silence about purported fraudulent dual representation by KIESEL, PARADIS, and PETERS, who was then Chief of Civil Litigation at the City Attorney's Office.

88. Specifically, in approximately July of 2017, KIESEL fired his secretary, Julissa Salgueiro, who had worked for both KIESEL and PETERS when they were law partners. Thereafter, Salgueiro threatened to publicly reveal that KIESEL and PETERS were secretly engaging in collusive litigation practices in the LADWP litigation, as well as one or more other cases, unless

[39] The information in this subsection was proffered by PARADIS and was partially corroborated by communications between and among PARADIS, KIESEL, and Salgueiro, and others, and by the settlement agreement entered into by these parties (following a privilege review by filter attorneys, the prosecution team reviewed unprivileged portions of these materials).

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

KIESEL paid Salgueiro $1,000,000. KIESEL initially offered to pay Salgueiro $300,000, but she rejected that offer.

89. In October 2017, Salgueiro told PARADIS in a text message, which I have reviewed, that she had left a message for CLARK related to this matter, and that CLARK had not responded. According to PARADIS, CLARK was angry after Salgueiro reached out, and CLARK told PETERS to "take care of" the problem, which PARADIS understood to mean giving Salgueiro whatever it took to keep her quiet. At a hearing on December 4, 2017, Salgueiro approached counsel for PwC in the *LADWP v. PwC* lawsuit, [redacted] of Gibson Dunn, in the presence of KIESEL and PETERS, and offered to provide [redacted] with information that he would find interesting.[40] This action quickly spurred renewed discussions between KIESEL, PARADIS, and Salgueiro, which ultimately resulted in an agreement that KIESEL would pay $800,000 to Salgueiro to buy her silence.

90. PARADIS agreed to pay half of the hush money payment, and he wired a total of $400,000 to KIESEL in or around late December of 2017.[41] The terms were memorialized in a confidential settlement agreement, which was prepared by a private attorney named [redacted]. The settlement agreement, which I have reviewed, stated that Salgueiro had "alleged legal claims and alleged violations of the law" by

[40] [redacted] confirmed to the government that the described incident took place (he was not certain of the hearing date but believed it to be in that general time frame).

[41] I have reviewed wire transfer records that corroborate PARADIS's payments to KIESEL.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Kiesel's law firm, which Kiesel's law firm denied. It further stated that Kiesel's law firm alleged that Salgueiro had taken certain records from the firm, and that Salgueiro denied any impropriety in connection with those records.[42]

B. The Manipulation of the Court-Appointed "Independent Monitor"

91. The *Jones v. LADWP* settlement negotiation included a provision by which the CC&B billing system remediation efforts would be overseen by an independent monitor appointed by the court. This monitor was required to make periodic reports to the court as to the progress of the remediation and to provide objective oversight so that the ratepayers would be treated fairly and obtain a central benefit of the settlement – fair and correct billing practices. The court appointed PAUL BENDER as the independent monitor.

92. In proffer sessions with the government, PARADIS advised that he had, contrary to the intent of the settlement, effectively controlled BENDER's work as the "independent monitor." PARADIS stated that he had done so at the direction of CLARK and with the knowledge of WRIGHT and others at LADWP. In particular, PARADIS stated that he regularly wrote BENDER's purportedly independent reports to the court, and that on some occasions BENDER did not substantively edit those reports before filing them with the court.

[42] The FBI has not yet interviewed Salgueiro regarding these topics.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

93. In a proffer session, WRIGHT stated that BENDER had previously told WRIGHT and LADWP Chief Administrative Officer DONNA STEVENER that PARADIS had written BENDER's reports and that BENDER sometimes submitted them without editing.

94. At my direction, PARADIS engaged in recorded communications with BENDER during the spring of 2019, wherein BENDER asked PARADIS to draft an additional "independent" report that BENDER was scheduled to submit to the court soon. After PARADIS deflected multiple such requests, BENDER ultimately wrote the report himself and submitted it to the court.

95. PARADIS further advised me that during BENDER's tenure as independent monitor, PARADIS treated BENDER to meals, sporting events, and other entertainment, and that neither PARADIS nor BENDER had reported these gifts or benefits to the court because it would reveal that BENDER was in fact not independent.

96. On May 31, 2019, in response to a court order, BENDER filed a sworn declaration with the court falsely averring that he did not have, and had never had, any professional or personal relationships with PAUL PARADIS. Based on an email that I have reviewed, it appears that BENDER sent PARADIS a draft of this declaration on April 18, 2019. Based on PARADIS's statements, recordings of BENDER, and the referenced email, BENDER clearly appeared to have both a personal and professional relationship with PARADIS.

C. No-Bid LADWP Contracts Awarded to Attorney PARADIS and Quid Pro Quo Established with City Officials

1. 2015 and 2016 No-Bid Contract for $6,000,000

97. In 2015 and 2016, during the *Jones v. City* settlement negotiations in which PARADIS was participating during the mediation on behalf of the City, and after PARADIS had selected the City's white knight plaintiff's counsel (LANDSKRONER) who later covertly paid PARADIS a $2.175 million dollar kickback, PARADIS's two-member law firm also received from LADWP two no-bid contracts totaling over $6,000,000 for project management services relating to remediation of the CC&B billing system.[43] .

2. 2017 No-Bid Contract for $30,000,000

98. On March 29, 2017, PARADIS registered the AVENTADOR company for the purpose of pursuing a separate $30 million no-bid contract from LADWP, which ostensibly covered further work to remediate the CC&B system.[44]

99. In May 2017, PAUL BENDER —— the aforementioned court-appointed "independent monitor" who was effectively controlled by PARADIS —— reported to the court that LADWP lacked well-qualified information technology project management personnel,

---

[43] In proffer sessions, PARADIS claimed he did not pay any bribes or kickbacks to obtain either the no-bid contract or the extension thereof. WRIGHT also stated in a proffer session that he was not aware of any bribes or kickbacks in connection with that contract or the extension.

[44] The facts of AVENTADOR's incorporation were provided by PARADIS in a proffer and are reflected in records maintained by the California Secretary of State.

As noted below, the facts indicate that the primary purpose of this contract was different than that reflected in the contract itself and the LADWP Board's public materials about the contract.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

and also that it lacked the capability to successfully manage implementation projects; thus, BENDER maintained that LADWP "would need to contract" for these personnel.[45] At the LADWP Board meeting where the AVENTADOR contract was approved, WRIGHT also expounded on this alleged lack of any internal LADWP options to perform the necessary functions and thus the need to approve the AVENTADOR contract.

a. WRIGHT's Acceptance of Bribe in Exchange for Supporting AVENTADOR Contract

100. In the months before the contract was awarded, to obtain support for AVENTADOR's single-source bid for this $30 million contract, PARADIS secretly offered the LADWP General Manager, DAVID WRIGHT, a future post-retirement position as CEO of AVENTADOR, with an annual salary of $1 million and various associated benefits and perks.[46] WRIGHT secretly accepted this

---

[45] This information is derived from a draft LADWP Board report dated July 10, 2019. I obtained this document from [redacted] who advised that the document had been drafted by [redacted], LADWP's Director of Communications, Media, and Community Affairs, with input from others at LADWP.

[46] In a consensually recorded conversation, WRIGHT previously stated that he intended to retire from LADWP in 2020. In subsequent consensually recorded conversations, WRIGHT advised that he had prepared a resignation letter and informed the Mayor's Office that he would retire in October 2019. WRIGHT was seeking an arrangement with the City that would permit him, upon retirement, to be hired as a contractor to report to an offsite location (not requiring him to actually produce work) and provide transitional services to the yet to be determined LADPW General Manager. In early July 2019, LEVINE advised WRIGHT that the Mayor's office had decided to officially transition the role of LADWP General Manager from WRIGHT to a successor on July 23, 2019.

In a consensually recorded conversation, WRIGHT, a public official representing the largest municipality utility in the country, referred to PARADIS, a plaintiff's counsel who had

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

offer.[47] I believe this secret arrangement to constitute bribery of a public official because it established a quid pro quo, namely, assisting PARADIS's receipt of a lucrative City contract in exchange for WRIGHT's agreement to a lucrative future salary.[48]

b. Bribes to FUNDERBURK in Exchange for Support for AVENTADOR Contract

101. According to PARADIS, during the months preceding the LADWP Board's vote on the $30 million no-bid contract, PARADIS

---

represented a class plaintiff in a high profile lawsuit against WRIGHT's agency, as his "ATM" and requested that PARADIS begin paying WRIGHT in August 2019, despite WRIGHT's intention not to retire from the City until October 2019.

[47] In a proffer session, PARADIS described his agreement with WRIGHT as to WRIGHT's future employment with and financial interest in AVENTADOR. WRIGHT confirmed their agreement in multiple consensually recorded conversations with PARADIS. After initial denials and partial denials, WRIGHT also admitted in proffer sessions with the government that he had agreed to accept a future job with AVENTADOR for an annual salary of $1 million.

In addition to WRIGHT's financial interest in AVENTADOR, PARADIS and WRIGHT planned to engage in another business venture that would solicit lucrative contracts from LADWP. Specifically, PARADIS and WRIGHT agreed to partner with an Israeli company called CYBERGYM to open cybersecurity training facilities in Los Angeles and elsewhere to serve personnel from LADWP and other utility companies. PARADIS's affiliation with this company is overt, but WRIGHT, as current LADWP General Manager, endeavored to hide his role, likely because City ethics rules forbid former City officials from lobbying City officials for a period of one year (and for life if they substantially and personally worked on the project while in the City).

As described in more detail herein, PARADIS, WRIGHT, LEVINE, and other LADWP employees and officials traveled to Israel in 2018 to meet with individuals related to CYBERGYM and other prospective Israeli vendors seeking to do business with LADWP.

[48] As LADWP General Manager, WRIGHT did not have a direct role in voting on the contract, but he did utilize his official capacity as General Manager to influence LADWP Board members to vote in favor.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

also courted support from LADWP Board Vice President, attorney WILLIAM FUNDERBURK, who, in turn, solicited financial benefits from PARADIS before the vote.[49] I believe this arrangement to similarly constitute a quid pro quo relationship between PARADIS and FUNDERBURK.

102. Specifically, on May 31, 2017, FUNDERBURK asked PARADIS to provide legal services on behalf of a class-action defendant that FUNDERBURK was representing. PARADIS agreed to assist because he knew that FUNDERBURK was set to vote on the $30 million no-bid contract the following week, and he wanted FUNDERBURK to vote in his favor. FUNDERBURK e-mailed PARADIS the necessary documents, and PARADIS wrote a brief and sent it back to FUNDERBURK. PARADIS never billed FUNDERBURK or FUNDERBURK's client, nor did FUNDERBURK ever reimburse PARADIS for his legal services. Between May 31, 2017, and August 6, 2017, PARADIS performed "free" legal work for FUNDERBURK and FUNDERBURK's client because of FUNDERBURK's influence over the $30 million no-bid contract and potential future contracts.

103. Additionally, in October 2016, during PARADIS's initial preparations to seek the contract the following year, FUNDERBURK invited PARADIS to an award ceremony at which FUNDERBURK was being honored, telling PARADIS that FUNDERBURK expected PARADIS's full support. On the guidance of WRIGHT, who advised PARADIS that he needed to donate because FUNDERBURK would soon be voting on PARADIS's contract, PARADIS donated

[49] PARADIS proffered the information herein regarding benefits that he provided to FUNDERBURK in exchange for FUNDERBURK's support of his contract.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

$5,000 to the organization hosting FUNDERBURK's award function.

c. Behind-the-Scenes Coordination by WRIGHT, LEVINE, and FUNDERBURK in Support of AVENTADOR Contract

104. On June 4, 2017, two days before the LADWP Board approved the AVENTADOR contract, WRIGHT sent a text message to LEVINE with FUNDERBURK's contact information. LEVINE responded, "Left a detailed vm [voicemail]. Will call again." That same day, LEVINE left a voicemail for WRIGHT that said, "I just reached BILL [FUNDERBURK], **I do not believe BILL [FUNDERBURK] will end up being a problem**; however, the issue is diligence. He said why don't we have like a committee, an oversight committee to monitor the progress. I think that is probably a good idea, but I told him I want to run that idea by you and not sign off on anything. I was going to go with you, period. But, that sounded like a reasonable suggestion, so I wanted to hear your thoughts about it."[50] Based on my training, experience, and knowledge of the investigation, I believe that LEVINE referencing that "BILL will not end up being a problem" meant that LEVINE and WRIGHT were coordinating efforts to ensure the $30 million AVENTADOR contract for PARADIS was approved. FUNDERBURK, being the Vice-President, needed to "not be a problem" leading into the LADWP Board meeting.

105. At the LADWP Board meeting on June 6, 2017,[51] both

[50] This voice-mail was seized from WRIGHT's Phone pursuant to the April 18, 2019 search warrant authorized by the Honorable Magistrate Judge Jacqueline Choolijan.

[51] This meeting was audio/video recorded by the City, and I have reviewed relevant parts of this recording.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

WRIGHT and LADWP Board President (and Gibson Dunn attorney) LEVINE strongly argued in favor of awarding the $30 million no-bid contract to AVENTADOR, underscoring that the need for AVENTADOR's billing-system remediation services was so imminent that there was not sufficient time to engage in the standard competitive bidding process usually required for LADWP contracts of that size.[52] In addition, a LADWP Ratepayer Advocate, Frederick Pickel, was asked if he had any questions or input, to which Pickel replied with an inquiry about how oversight would be provided. WRIGHT suggested that a subcommittee be formed to evaluate the work being completed, and LEVINE and FUNDERBURK were selected to perform that role. According to the above-described June 4, 2017 voicemail message from LEVINE to WRIGHT, which I have reviewed, these comments appeared to be staged in order to make the process appear more legitimate. Following the enthusiastic recommendations of WRIGHT and LEVINE, all the Board members (including FUNDERBURK) voted in favor of awarding the $30 million contract to AVENTADOR.[53] Based on the context of the

[52] In this Board meeting, video footage of which is publicly available on LADWP's website, WRIGHT described the urgent need to award this no-bid contract to AVENTADOR based on the negotiated terms of the pending settlement agreement, which required the City to remediate the CC&B system. LEVINE enthusiastically concurred, noting that LADWP had no choice but to award the no-bid contract to AVENTADOR. As discussed further below, the representations made by WRIGHT and LEVINE do not appear to be a fair or accurate description of the choice the LADWP Board had to make when awarding this $30 million dollar contract and instead appear to be pre-textual reasons to get the contract approved expeditiously and with little scrutiny.

[53] The Los Angeles City Council has the prerogative to review a contract of this size. According to PARADIS, WRIGHT asked certain members of City Council not to review the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

communications, the recording of the meeting, the interviews I conducted, and my knowledge of the investigation, I believe WRIGHT and LEVINE coordinated together and/or with FUNDERBURK for the AVENTADOR contract approval. This is relevant evidence because of PARADIS's quid pro quo relationships with WRIGHT and FUNDERBURK, and I am seeking to determine who else (a) was aware of the illicit relationships and (b) was set to financially benefit from the AVENTADOR contract approval.

3. WRIGHT Advocated For and Praised AVENTADOR in an Effort to Gain Support for Future Contracts

106. On May 12, 2018, in a text message, WRIGHT told LEVINE, "MEL[TON LEVINE], here's a short message I sent [redacted][54] that's entirely plausible from meetings that we attended over the entire trip.[55] Just wanted you to know… We provide rebates for facility energy management systems. Some of the light bulbs that could work with them have light sensors or motion sensors in them. Hackers could go through the light bulbs to hack their facility's entire IT systems. Now think if that energy management system services a hospital. It could actually kill patients! And on top of how horrible that is, we would likely be pulled into the lawsuit." LEVINE replied, "Yikes!!!!!" Based on my training, experience, and knowledge of

AVENTADOR contract. However, WRIGHT denied this allegation to me.

[54] [redacted] is the Chief Operating Officer for LADWP and has been designated by the Mayor of Los Angeles as the next General Manager of LADWP after WRIGHT's impending retirement.

[55] Based on the timing of the text message and my knowledge of the investigation, I believe that this was a reference to the May 2018 Israel trip attended by PARADIS, WRIGHT, and LEVINE, along with other LADWP officials.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

the investigation, I believe WRIGHT informed LEVINE about his message to [redacted] in an effort to plant seeds related to the need for cyber security. I believe that although the cyber vulnerabilities and necessity for cyber security measures may indeed exist, WRIGHT was zealously advocating for cyber awareness and security services at least in part because of his illicit quid pro quo relationship with PARADIS, namely, WRIGHT's self-interest in his future lucrative employment with AVENTADOR, PARADIS's company.

107. On August 17, 2018, WRIGHT sent a text message to LEVINE and LADWP Board Commissioner Christina Noonan, "we have experienced a phishing attack that has resulted in hackers obtaining staff credentials and gaining access into our systems. We don't know yet to what extent. AVENTADOR staff have been working 24/7 to contain the situation. Nothing on our systems has been compromised or information released that we are aware of. But his [PARADIS's] dozen staff are mostly from the NSA or DOE and are **the best in the nation**. I will fill you in as we know more." Noonan replied, "Just checking in on this situation. Is AVENTADOR pre-approved under our cyber insurance policy? Any of this 24/7 cost will need to go against our deductible. Also, **I suggest communication relating to this matter, particularly with AVENTADOR, go through our legal counsel so that the Department secures attorney/client privilege which will be beneficial**. All of this presumes we have noticed our insurance carriers." Based on my knowledge of the investigation, I believe that WRIGHT glorified the team as being

"the best in the nation" to further praise AVENTADOR, a company in which WRIGHT secretly had a strong financial interest. In addition, I believe Noonan's comments that communication regarding AVENTADOR should be cloaked in attorney/client privilege to be consistent with LADWP's pattern of behavior to conceal aspects of the AVENTADOR contract by copying lawyers on routine non-legal communications and marking them as privileged.

108. Later that day, WRIGHT provided an update regarding the situation and stated, "We have 10 former staff from the NSA and DOE working 24/7 throughout the weekend and next week on the most highly exposed areas of our SCADA operating systems. (Our contractor, AVENTADOR owned by PAUL PARADIS, hired almost all of the DOE's cyber team over the last six months to work for him, so we have the some of the best experts related to these hacking efforts in the world working on this.). Biggest worry is that several months of planned system fixes now have to be expedited into just a few weeks. We can tell the hackers keep trying to attack us but we are on it. (As perspective, **if we called the Federal government for help, they would contact the DOE who would have assigned the staff AVENTADOR already hired to come out to help us**.)." LEVINE replied, "Wow. Thanks Dave. Hang in there. If you want to talk over the weekend or Monday let us know." Based on my knowledge of the investigation, I believe WRIGHT was again advocating for LADWP's continued reliance on AVENTADOR and excusing the need to contact the Federal government regarding the issues. WRIGHT's effusive adulation portrays AVENTADOR and PARADIS as saviors to the City, a

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

depiction that appears unwarranted by the facts and in any event omits WRIGHT's covert financial entanglement with AVENTADOR.[56] In addition, I have reviewed text messages between PARADIS, WRIGHT, and LEVINE in which PARADIS echoes WRIGHT's sentiments about AVENTADOR's expertise and necessity, yet omits reference to WRIGHT's financial interest in AVENTADOR.

109. On August 23, 2018, WRIGHT sent a text message to LEVINE, "no need to call back unless you want more info. Cyber attack has been contained. Mayor briefed by PAUL [PARADIS] and I. It was sophisticated. But PAUL's [PARADIS] **elite team of experts** handled it and prioritized fixes. **Staff is now becoming very accepting of AVENTADOR staff** and excited about getting some training from the experts. PAUL [PARADIS] is charging us for this time, but not overcharging. We are so messed up here that **I will likely suggest a two year extension and an increase to his contract.** But that's six months away. I want to brief the board again at the next meeting." LEVINE replied, "Thanks DAVE [WRIGHT]. Just received. Great news. Please get back to me today if possible with the names of the Israeli companies we are

[56] In October 2016, AVENTADOR performed penetration testing at the Los Angeles International Airport ("LAX") to test cyber vulnerabilities. The FBI received notice from LAX regarding the intrusion. Cyber agents with the FBI subsequently conducted an investigation that lead to the execution of a search warrant for [redacted], an AVENTADOR employee. [redacted] stated that he was authorized to conduct the penetration test and that AVENTADOR had a contact with the City. Representatives from AVENTADOR (now ARDENT) have yet to produce said contract. Based on my interviews with PARADIS, no such contract existed regarding penetration testing at LAX; however, PARADIS maintains that the testing was verbally authorized by City officials. Based on my discussions with FBI cyber agents, they described AVENTADOR's work as "amateur."

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

considering using so I can promptly get back to the guy st [at] DHS Rep. Schiff put us together with. Thanks." WRIGHT then responded, "PAUL [PARADIS] is sending via text. **We don't want to do via LADWP email.**" PARADIS then sent a text message to WRIGHT and LEVINE with the Israeli companies' information and stated, "I sent this as a text rather than email for security and public record disclosure reasons." LEVINE then responded, "Great. Thanks. This is what I need and a good way to send. Will get back to you after I hear back." Based on the context of the communication, it appears as though WRIGHT was once again praising AVENTADOR heavily and laying the groundwork to advocate for an extension for AVENTADOR while utilizing personal email, which would not be subject to City monitoring. To my knowledge, WRIGHT does not have any formal cyber training or knowledge to be able to distinguish the experts in the field nor be able to provide the LADWP Board a true and accurate assessment of AVENTADOR's work, qualifications, or necessity. I believe that WRIGHT praised and advocated for AVENTADOR so heavily based on his quid pro quo relationship with PARADIS, namely, his financial stake in AVENTADOR contracts.

4. Clear Warnings to LADWP and LEVINE About the AVENTADOR Contract and PARADIS

110. On June 1, 2017, LADWP Director of Supply Chain Services [redacted] sent an email to WRIGHT and LADWP Chief Administrative Officer STEVENER advising that she still lacked necessary information to perform a complete cost-reasonableness analysis on the AVENTADOR contract. Her email

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

further confirmed her position, which she had apparently conveyed in a prior discussion, that **the rates proposed by AVENTADOR "are not fair and reasonable."** [redacted]'s email noted that the single-source nature of the contract made it difficult to determine the cost reasonableness, but that her office had reviewed rates of other comparable recent contracts and found them to be *significantly lower* than those proposed by AVENTADOR.

111. On June 5, 2017, the day before the vote on the $30 million no-bid AVENTADOR contract, [redacted] sent a memo to WRIGHT and STEVENER. [redacted]'s memo again warned that AVENTADOR's proposed contract rates were substantially higher than those of other similarly situated LADWP contractors, and it laid out data for four recent contracts along with the proposed AVENTADOR rates. The memo further noted that nearly all of AVENTADOR's high-rate workers planned to work full time, unlike other contracting firms who typically bill the highest-rate workers for fewer hours per week.[57]

112. During that time frame, STEVENER apparently performed her own rate analysis. A media report indicates that the data on which STEVENER relied showed AVENTADOR's rates to be higher in nearly every job classification than six other companies, with the exception of a law firm.[58]

---

[57] A draft Board report dated July 10, 2019 —— which WRIGHT provided with the explanation that it was being drafted by LADWP media relations personnel, LEVINE, and other LADWP officials to address fallout from media and poli[redacted]ficials regarding the AVENTADOR contract —— implies that [redacted]s concerns about AVENTADOR's rates were not provided to the LADWP Board before the vote.

[58] I have not seen a copy of this data.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

113. In May and June 2018, LEVINE engaged in detailed written communication with an LADWP supplier of CC&B remediation services ("the supplier") about contracting work by the supplier and future contracting opportunities. On July 6, 2018, the supplier sent LEVINE a lengthy email detailing the manner in which PARADIS failed to follow the contract terms in administering the contract, edged the supplier out of its contracting duties, and transferred contract work to another supplier favored by PARADIS. The email further stated:

> We believe that it is no coincidence that Aventador Utility Solutions, LLC, an entity controlled by Paul Paradis, was granted a $30M no-bid contract by LADWP on June 6, 2017 to provide IT project management services at the same time that Paul [PARADIS] was pushing [the supplier] —— a potential competitor —— out the door. We also believe that it is no coincidence that retired LADWP senior management staff are currently working for Aventador at LADWP under lucrative contracts —— **the quid pro quo may not be explicit, but the message is certainly clear**.

114. Having received this explicit and detailed warning about potential illicit relationships by PARADIS related to the AVENTADOR contract, LEVINE forwarded the email chain to PARADIS and WRIGHT and asked for their guidance and assistance in responding. I do not know whether LEVINE undertook to investigate the complaints beyond sending them to PARADIS and WRIGHT.

115. On February 25, 2019, LEVINE received an e-mail from an entity identified as [redacted] bringing to his attention "the questionable actions/practices" of PARADIS at LADWP. The email explained that PARADIS was hired to handle the LADWP

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

litigation and then became involved with other contracts unrelated to his initial role. It further stated that PARADIS "has been able to get many DWP contracts **leveraging his relationship with General Manager [WRIGHT]** and a few other senior management team members." The email also alleged, **"We have tried so many times to bring this to [WRIGHT's] attention, but we haven't seen any action yet."**

116. Upon receipt of this complaint about PARADIS's chain of contracts with LADWP, which specifically stated that many similar complaints about PARADIS had been directed to WRIGHT and had gone unaddressed, LEVINE's response was to forward the email to WRIGHT and asked whether he knew what these concerns were about. WRIGHT then forwarded the email to PARADIS and asked for PARADIS to draft a response to the complainant.

117. The above-described emails suggest that LEVINE's primary method of responding to complaints and warnings, from at least two sources, that PARADIS's and WRIGHT's conduct raised red flags for possible bribery, was to merely send the complaints to PARADIS and WRIGHT —— the very subject of those complaints —— to deal with as they saw fit. Particularly in light of evidence, described herein, indicating that PARADIS did in fact obtain a $30 million no-bid contract by bribing WRIGHT and at least one other LADWP Board Commissioner, LEVINE's conduct raises questions about his motivations for either turning a blind eye to these legitimate complaints or seeking to undermine them by turning them over to PARADIS and WRIGHT to provide responses.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

D. Alleged Falsification of Regulatory Paperwork by LADWP Employees

1. Underreporting and Failure to Report Cybersecurity Issues

118. The above-described LADWP contract awarded to AVENTADOR purported —— according to its own terms and to the related LADWP Board materials and proceedings —— to cover services related to remediation of the CC&B system, as required by the terms of the settlement agreement in *Jones v. City*. However, evidence suggests that this $30 million single-source contract, which General Manager WRIGHT and Board President LEVINE advertised to the LADWP Board as urgent because it was mandated by the court-ordered settlement agreement, was in truth to address an entirely unrelated matter, that is, it was primarily intended to cover services related to assessing and improving cybersecurity for the City's power grid and other critical infrastructure.[59]

119. PARADIS alleges that in order to conceal and avoid responsibility for certain cybersecurity vulnerabilities related to critical infrastructure, LADWP employees falsified mandatory federal regulatory documents,[60] including by regularly self-reporting minor violations in order to avoid the discovery of

[59] The information in this section was proffered by PARADIS and has been corroborated in part by: 1) the aforementioned consensually recorded conversations with WRIGHT; 2) separate consensually recorded conversations with an AVENTADOR employee; and 3) an AVENTADOR work plan and other documents reflecting AVENTADOR'S cybersecurity work for the City, which PARADIS provided to the government.

[60] These include documents mandated by the Federal Energy Regulatory Commission ("FERC") under a compliance regime known as "NERC-CIP" (North American Electric Reliability Corporation - Critical Infrastructure Protection).

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

much more significant violations, which would carry substantial fines (in some cases, millions of dollars). Based on my interviews with PARADIS and my knowledge of the investigation, including review of recordings on this topic, LADWP management was under the impression that if they self-reported certain violations, federal regulatory agencies would be less likely to inquire into or investigate other possible violations because LADWP would appear to be already policing itself.

120. In separate consensually recorded conversations with both the current and former Chief Information Security Officers for LADWP (STEPHEN KWOK and DAVID ALEXANDER, respectively), PARADIS confirmed both LADWP's pattern of self-reporting of minor violations to conceal far more significant problems and the fact that members of LADWP management (including WRIGHT) and the LADWP Board (including LEVINE and Cynthia McClain-Hill) were aware of the unethical and potentially illegal practice.

121. DAVID ALEXANDER also informed PARADIS in a consensually recorded conversation that LADWP falsified paper records to avoid significant fines that might be imposed by NERC and FERC. For example, NERC-CIP standards require, among other things, the deployment of a patch management process to monitor and address software vulnerabilities, which includes adhering to a security patch evaluation timeline to ensure that all patches are up-to-date. In an April 2019 consensually recorded conversation with PARADIS, ALEXANDER said that a comparison of LADWP's paper records to its computers would show that LADWP claimed it applied patches in a timely fashion when, in fact, it

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

did not. ALEXANDER's proposed solution to the problem, which he disclosed to PARADIS, was to simply dispose of all the old computers evidencing delayed patching, and replace them with new computers that had no evidence of any patching issues.

122. In another consensually recorded conversation between PARADIS and ALEXANDER in May 2019, ALEXANDER told PARADIS that he had asked [redacted], the head of CIP compliance at LADWP, for all the self-reports that LADWP had submitted to NERC. ALEXANDER told PARADIS that after [redacted] emailed a link to ALEXANDER with the relevant documents, ALEXANDER emailed "them" – presumably referring to [redacted]'s group -- to take his permissions away, thereby indicating that ALEXANDER was receiving and sending these emails through **ALEXANDER'S LADWP ACCOUNT**. In addition, ALEXANDER told PARADIS he had asked [redacted], LADWP's point of contact for NERC, for additional documents relating to LADWP's NERC compliance.

123. According to PARADIS, LADWP was likely aware of its failure to comply with NERC-CIP standards as early as 2008. Based on a Critical Cyber Asset Vulnerability Assessment Report prepared for LADWP in November 2008, LADWP was informed of a number of weaknesses in its network security, including overly permissive access list statements ("ACLs"), outdated routers and switches, and passwords stored in clear text. In a 2010 NERC Vulnerability Assessment conducted for LADWP by a different vendor, it was determined that insecure ACLs were still an issue, several of the same routers and switches still had vulnerabilities, and weak passwords were cited as an issue of

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

high severity. Additionally, LADWP was cited as having internal network security that was "lax in non-patched and inadequately configured devices, which could either lead to compromise of SCADA data or a denial of service/availability."

124. In a consensually recorded conversation on May 15, 2019, WRIGHT told PARADIS that there had been a report issued 10-15 years ago (referring to the 2010 NERC Vulnerability Assessment) about "how fucked up the IT efforts were at DWP," and that "nothing has been done since then." On May 16, 2019, while in the process of assisting WRIGHT in creating a Power Point presentation regarding the history and oversight of the AVENTADOR contract, PARADIS provided WRIGHT with a written document stating that "LADWP does not have a comprehensive, systematic network security scanning and testing program and LADWP is therefore largely blind to cyber vulnerabilities and insider threats." PARADIS also wrote that 2,409 LADWP computers are "completely unaccounted for and unable to be located."

125. During a consensually recorded meeting between PARADIS and ALEXANDER in May 2019, PARADIS obtained an internal LADWP spreadsheet titled "CIP Self-Report and Issue Tracker" shows that since 2016, 10 of the 16 potential self-reporting incidents involved LADWP's Energy Control Center. But when PARADIS asked WRIGHT during their recorded conversation on May 26, 2019, about allotting funds in the next cybersecurity contract to address the issues at the Energy Control Center, WRIGHT rejected the idea, stating that they needed to avoid doing anything with the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Energy Control Center for at least the first 60 days of the contract, so as to avoid the scrutiny of others. As detailed below, PARADIS, WRIGHT, KWOK, and ALEXANDER were actively orchestrating a plan to award ARDENT a new multi-million dollar cybersecurity contract in September 2019 – even before the relevant Request for Proposals has been drafted.

126. Notably, when KWOK debriefed PARADIS in a consensually recorded conversation about a meeting he had had in March 2019 with Deputy Mayor "[redacted]", KWOK said that when a question was raised about whether the cybersecurity work at issue was deferrable, KWOK responded, "No, none of this stuff is deferrable. It's critical, unless you want the lights to go off, or the water to go off . . . It could happen any day."[61]

E. Alleged Circumvention of LADWP's Contracting Process

1. Manipulation of the SCPPA Bidding Process

127. According to PARADIS, LADWP management and members of the Board (including WRIGHT, LEVINE, and McClain-Hill) successfully manipulated LADWP's contracting processes to ensure that AVENTADOR's successor company, ARDENT UTILITY SOLUTIONS, LLC ("ARDENT"),[62] was awarded a lucrative contract to continue AVENTADOR's cybersecurity work without engaging in the required competitive bidding process (the "ARDENT contract"). According

[61] Based on the consensually recorded conversations between PARADIS and KWOK (and summaries thereof) that I have reviewed, it appears that KWOK was the person at LADWP with whom ARDENT interfaced the most regarding their work at the utility.

[62] Despite a sham sale in March 2019, PARADIS appears to still effectively control this company.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to information proffered by PARADIS, LADWP routinely uses the Southern California Public Power Authority ("SCPPA")[63] to circumvent LADWP's standard 12-18 month competitive bidding process, and did so for the ARDENT contract.[64]

128. On January 8, 2019, WRIGHT sent a text message to LEVINE, "Cyber and IT will always need external staff (I think [redacted] – Business Manager, IBEW Local 18][65] already supports this), we are increasing staff everywhere in the department as fast as reasonable. Need to get more supportive on outsourcing as we have hired a net increase of couple thousand staff in the last few years. We support greater workforce development but LADWP needs to have a greater role in screening them for base line qualifications."

129. The SCPPA website shows that in February 2019, SCPPA issued a Request for Proposals for Cybersecurity Services.

130. According to media reports of a statement issued by LADWP, the LADWP Board, on or about March 12, 2019, ordered AVENTADOR's $30 million contract terminated "in order to eliminate any potential conflict or the appearance of a conflict of interest" after allegations that PARADIS improperly

---

[63] According to the SCPPA website, SCPPA is "a Joint Powers Authority, created in 1980, for the purpose of providing joint planning, financing, construction, and operation of transmission and generation projects."

[64] According to the SCPPA website, WRIGHT is the Secretary of SCPPA and a current member of the SCPPA Board of Directors.

[65] IBEW Local 18 is a labor union. According to IBEW Local 18's website, Local 18 is an "affiliate of the International Brotherhood of Electrical Workers (IBEW). Although our name says "electrical workers," our members come from hundreds of different job classifications."

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

represented both Jones and the City in relation to LADWP's overbilling issues.

131. I have seen text messages between WRIGHT, McClain-Hill, and LEVINE from March 14, 2019, in which McClain-Hill asks, "is the contract termination moving forward," to which WRIGHT responds that the contract was assumed **with PAUL [PARADIS] no longer connected**." McClain-Hill then goes on to say, "The goal was not to simply save the existing contract, but to facilitate payment under the existing contract until we put a new contract in place . . . with AVENTADOR or some other entity." WRIGHT responds, "Yes. That is all in process." And LEVINE says, "All good."

132. On March 14, 2019, LEVINE sent a text message to WRIGHT, "Ok. I need to talk with Dakota [Smith – Los Angeles Times Reporter] again in the next few minutes. Pretty much told her what we are doing to keep the cyber employees. She questioned if that is consistent with board instruction to cancel AVENTADOR contract.[66] Joe [Brajevich – LADWP General Counsel] gave me a good response to that." Based on the context of the communication it appears as though Smith inquired into the retention of City cyber employees and the fate of the AVENTADOR employees post cancellation. The formation of ARDENT,

[66] According to PARADIS, after his dual role in the *Jones v. City* litigation came under scrutiny as described herein, in order to keep AVENTADOR employees working on the City contract, PARADIS submitted to pressure to sell AVENTADOR and have no part in any subsequent companies that form. PARADIS sold AVENTADOR below market value and has in fact remained an integral part of ARDENT (the new company). Based on consensually recorded conversations, WRIGHT and LEVINE are aware of PARADIS' continued involvement.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a subsequent awarded contract discussed below, do not appear to me to be consistent with the LADWP Board's demand.

133. On March 26, 2019, WRIGHT sent a text message to LEVINE, "I have to share at some point that [we are] deliberately vague on our public descriptions as we were worried about publicly communicating our specific cyber vulnerabilities. And we discussed this in closed session and in our meetings with other city staff. Will try to mention it in general in the meeting tomorrow morning if it fits into the discussion." LEVINE replied, "Good. Radio silence from CYNTHIA [MCCLAIN-HILL] after calling and emailing."

134. On March 27, 2019, WRIGHT sent a text message to LEVINE, "Check LADWP email. Excellent summary document regarding cyber we will discuss at tomorrow's meeting." LEVINE replied, "Can you send it to my other email?"[67]

135. According to the California Secretary of State website, AVENTADOR filed an amendment to change its name to ARDENT on March 29, 2019.

136. On April 1, 2019, in a consensually recorded conversation, KWOK told PARADIS that there was really "**no competition**" for ARDENT as far as the SCPPA selection process was concerned, but referred to "political maneuvering" in describing the efforts to get ARDENT another contract with LADWP.

[67] Based on my interviews of PARADIS, LEVINE utilized his Gibson Dunn email to conduct City business, not his LADWP email.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

137. On April 5, 2019, in a consensually recorded conversation, LEVINE and McClain-Hill confirmed to PARADIS that ARDENT would be the primary vendor (out of 28 candidates) for the LADWP's cybersecurity services contract, *despite the fact that SCPPA was not scheduled to vote on the contract until a meeting on April 18, 2019* —— almost two weeks later.

138. That same day, in a consensually recorded conversation, DAVID ALEXANDER informed PARADIS that he had driven the SCPPA process that resulted in the approval of ARDENT. Specifically, ALEXANDER said LADWP had been told by the Mayor's office that they couldn't give another sole source contract to ARDENT, so LADWP used the SCPPA bidding process to "get to [LADWP's] desired outcome in an apparently completely transparent process." In fact, ALEXANDER said, "that was me driving it. That was me and Jim [Compton] texting each other. That was me and Jim conversing with each other on our cell phones."

139. Because ALEXANDER was the Vice-Chair of the SCPPA Cyber Security Working Group, he was able to work with Compton, who was the Chair of the SCPPA Cyber Security Working Group, to get Compton "somebody he wanted," and "[Compton] got me somebody I wanted." According to ALEXANDER, Compton wanted part of the contract to go to Dragos, Inc. The third vendor that ALEXANDER and Compton chose was Archer Energy Solutions, LLC.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

140. On April 23, 2019, the LADWP Board approved a 60-day contract of $3,600,000 for ARDENT, Dragos, Inc., and Archer Energy Solutions, LLC.[68]

2. Continuing Manipulation of the LADWP Bidding Process

141. Since at least May 2019, PARADIS has been working with ALEXANDER and KWOK -- at WRIGHT's direction -- on the issuance of another Request for Proposal ("RFP") for Cybersecurity Consulting Services. Unlike the prior cybersecurity contract, which went through the SCPPA process, this contract is proceeding through LADWP's own bidding process and– based on communications between PARADIS, WRIGHT, ALEXANDER, and KWOK – appears to be an $82.5 million, three-year contract.

142. On May 21, 2019, in a consensually recorded conversation, PARADIS met with KWOK to discuss the RFP. Included in the discussion was the evaluation criterion for who would be selected. KWOK told PARADIS that he spoke to ALEXANDER about how they could control the evaluation team to ensure that they could guarantee that those entities they wanted to hire were certain of being selected.

[68] The Board's action is confirmed in public materials on the LADWP website. According to PARADIS and confirmed in a consensually recorded conversation with WRIGHT on April 21, 2019, the original plan for a larger contract to ARDENT was tabled after the Mayor's office exerted pressure on LADWP to avoid such a large contract with ARDENT due to the potential for negative publicity related to ARDENT, a successive company to AVENTADOR, being awarded another large contract. PARADIS reported that LADWP planned that the majority of the $3.6M 60-day contract would go to ARDENT, and that the contract would thereafter be extended or expanded.

143. On May 24, 2019, **KWOK's PERSONAL ACCOUNT** sent PARADIS a timeline for the RFP, which was designed to meet a "Sept 24 timeline" for the recommendation of an award to the LADWP Board. The attached timeline provided that the RFP would be released on June 17, 2019, with the solicitation period ending on July 8, 2019.

144. That same day, PARADIS submitted his redline of the draft RFP to ALEXANDER and KWOK, at WRIGHT's direction. On May 29, 2019, PARADIS sent another version of the RFP to ALEXANDER and KWOK, which he said included all of WRIGHT's comments. In doing so, PARADIS did not communicate with ALEXANDER and KWOK through their email addresses at LADWP, but instead used **ALEXANDER's PERSONAL ACCOUNT**, [redacted], and **KWOK's PERSONAL ACCOUNT**, [redacted].

145. In that same e-mail, PARADIS said WRIGHT had instructed him to inform KWOK and ALEXANDER of the way in which the $82.5 million would be spent over the course of the three years of the contract. This financial breakdown included a $15 million allotment for "Cybersecurity Laboratory Training Services," which – as WRIGHT told PARADIS in a consensually recorded conversation on May 26, 2019 – would be for CYBERGYM.[69]

[69] On May 26, 2019, WRIGHT stated to PARADIS that LEVINE knew that PARADIS could have, but did not, report LEVINE for having improperly intervened in the debarment process (described in a subsequent section) involving PwC despite being recused, and was appreciative of PARADIS concealing that fact. WRIGHT suggested that PARADIS could use LEVINE as a "front" ownership regarding CYBERGYM.

146. In another email on May 29, 2019, PARADIS emailed **ALEXANDER's PERSONAL ACCOUNT** and **KWOK's PERSONAL ACCOUNT** to tell them that WRIGHT had decided that he, STEVENER, ALEXANDER, and KWOK would be among the seven people making up the evaluation committee for the RFP.

147. According to the website for the Los Angeles Business Assistance Virtual Network, LADWP issued an RFP for Cybersecurity Consulting Services on June 17, 2019, with a deadline of July 10, 2019. According to PARADIS, ARDENT submitted a bid for the contract.

148. I believe this behind-the-scenes manipulation of City contracting processes appears to be consistent with related unethical and/or illegal behavior by LADWP officials designed to circumvent legal and regulatory constraints to benefit favored parties.

F. Alleged Conspiracy and Falsification of Records by Attorney Members of the LADWP Board, LADWP Attorneys, and Members of the City Attorney's Office[70]

1. The City's Contemplated Actions to Debar PwC

149. In June 2016, while representing the City in its litigation against PwC, PARADIS proposed debarring[71] PwC in the

[70] PARADIS proffered the information in this section and provided the government with his correspondence with LEVINE, WRIGHT, FUNDERBURK, Brajevich, and others. While the version seen by the prosecution team to date was heavily redacted by the government's filter attorneys, it generally corroborates PARADIS's account, as detailed below.

[71] Debarment is the state of being excluded from enjoying certain possessions, rights, privileges, or practices and the act of prevention by legal means. For example, companies can be

wake of salacious public allegations that PwC employees had misspent City money on personal entertainment (including prostitutes and alcohol) in Las Vegas. According to PARADIS, in a closed session on June 21, 2016, the LADWP Board agreed with PARADIS and voted 4-0 in favor of debarring PwC, with Board President LEVINE recusing himself from the discussion and vote due to a conflict of interest.[72] Based on LADWP's minutes of the public board meeting on that same date, it appears that the four other board commissioners at the time were FUNDERBURK, Michael Fleming, Christina Noonan, and Jill Banks Barad.

150. PARADIS further reported that a press release touting the debarment was drafted and circulated among the staff of the City Attorney's Office. According to PARADIS, LEVINE, City Attorney Michael Feuer, former Chief of Civil Litigation PETERS, LADWP General Counsel Joseph Brajevich, and others thereafter embarked on a furtive and successful campaign to influence the other LADWP Board members to secretly change their votes, which ultimately resulted in the PwC debarment issue being dropped.

---

debarred from contracts due to allegations of fraud, mismanagement, and similar improprieties.

This initiative to debar PwC came in the wake of public allegations that PwC managers overbilled the City and then spent the money on prostitutes, luxury bottle service liquor, and entertainment in Las Vegas. See https://www.latimes.com/local/lanow/la-me-ln-dwp-billing-20160630-snap-story.html.

[72] According to multiple sources, including an email chain between LEVINE and a City ethics advisor which I have reviewed, LEVINE is officially recused from all LADWP Board matters involving PwC, because PwC is a prominent and lucrative Gibson Dunn client. (LEVINE is a partner/counsel at Gibson Dunn.)

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

The initial 4-0 vote in favor of debarment was not reflected in Board materials and PwC was not debarred.

151. According to PARADIS, he and his law partner, GINA TUFARO, were called to meet with Feuer and others (including PETERS, Brajevich, and Leela Kapur, Feuer's Chief of Staff) in Feuer's office on June 30, 2016. Feuer was angry about the debarment initiative and informed PARADIS that he (Feuer) was the "team captain" and as such was charged with making the decision as to whether to pursue debarment. PARADIS stated that the Board had already voted and debarment was therefore going to happen, and Feuer said words to the effect that, "We'll see about that."[73] At Feuer's direction, PARADIS made a presentation to LADWP management, including WRIGHT, in favor of debarment, and PETERS gave a contrary presentation against debarment. PARADIS then met with LADWP Board Vice President FUNDERBURK, who told PARADIS that both he and another Board member, Michael Fleming, were committed to debarment and would stand by their votes in favor of debarring PwC. A few days later, FUNDERBURK contacted PARADIS to advise that, in fact, debarment was probably not going to happen. PARADIS went to WRIGHT and threatened to "blow the whistle" —— meaning he would disclose information related to what he believed to be certain illicit City schemes to the public —— if he didn't learn what was going

[73] According to PARADIS, Feuer claimed that the debarment process was "in shambles," and thus that debarment was not a viable option. However, PARADIS stated that the Board voted to debar another entity at the June 21, 2016 meeting, and that the other debarment vote was never challenged.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

on, and obtained WRIGHT's permission to review the emails from the LADWP server during the period of the debarment dispute.

152. After being granted access by WRIGHT to the LADWP email server, PARADIS then printed a large number of emails reflecting communications about debarment and behind-the-scene efforts by LEVINE, Feuer, Brajevich, then-LADWP General Manager Marcie Edwards, and others to reverse the Board's 4-0 vote to debar PwC. The prosecution team has since reviewed redacted versions of some of those emails, as received from the government's filter team. While the text of almost all of the emails is heavily redacted (due in part to the apparent default practice of copying LADWP General Counsel Brajevich on nearly every piece of correspondence), the email traffic is generally consistent with PARADIS's account of the debarment episode.

153. Specifically, the emails indicate that:

- On June 30, 2016, City Attorney Michael Feuer held a scheduled meeting with Brajevich, PETERS, and Kapur, regarding PwC.
- Over the next few days, FUNDERBURK, PETERS, Kapur, Feuer, Brajevich, and others traded numerous emails on the subject of PwC and the debarment issue.
- On July 1, 2016, at the end of an email exchange between FUNDERBURK, WRIGHT, Michael Fleming, Marcie Edwards, Joseph Brajevich, and later, LEVINE, regarding a special board meeting to discuss PwC, Marcie Edwards forwarded the email chain only to FUNDERBURK with the message, **"Please. Trust me and stand down."**

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

- On July 1, 2016, LEVINE and Edwards discussed having Feuer speak with FUNDERBURK.
- On July 1, 2016, notwithstanding his official recusal from PwC debarment matters, LEVINE sent an email to all Board commissioners, Edwards, and Brajevich, with the subject "PWC lawsuit."

154. As stated above, debarment of PwC did not ultimately happen, and the minutes from the June 21, 2016 LADWP Board meeting do not reflect the original alleged 4-0 vote in favor of debarment. Rather, the Board meeting minutes from June 21, 2016, note for this item: "Discussion held – action taken but not a final action that is reportable." Based on my knowledge of the investigation, I believe the minutes may not accurately or fully reflect the events that actually transpired at the meeting.

155. The motivations of LEVINE, Feuer, and other members of the City Attorney's Office in preventing the PwC debarment action from moving forward are presently unclear to me. Also unclear is why LEVINE appears to have been actively involved in the discussion of PwC debarment despite being formally recused from all PwC matters due to his financial ties to Gibson Dunn, and thus to PwC, as a major client of Gibson Dunn.

156. During a proffer session, WRIGHT offered the following opinions, which he stated were based on his experience with the contracting and debarment processes:[74]

[74] I have not yet independently confirmed the accuracy of these opinions.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. If PwC had been debarred in Los Angeles, in addition to being officially foreclosed from seeking contracts with LADWP, PwC would have been required to report that debarment on *all* future bids and RFPs with other agencies, including in other locations throughout the country.

b. That reported fact of debarment would have substantially hindered PwC's ability to obtain future contracts with any government agencies.

c. The prospective debarment thus would have effectively blacklisted PwC far beyond the service area of LADWP, with a substantial impact on PwC's business operations and profitability.

157. Based on the above, I believe it is possible that one motive LEVINE could have had in ensuring that PwC was not debarred, notwithstanding his recusal, was to not significantly financially harm a lucrative client of his law firm.

G. LADWP's Use of a Foreign Broker Known to Receive Kickbacks From Successful Contract Vendors

158. In May 2018, officials and employees of LADWP, including WRIGHT and LEVINE, traveled to Israel along with PARADIS to meet with Israeli companies that provided cyber and physical security for utilities.[75] Most or all of these

[75] PARADIS, TUFARO, and WRIGHT proffered information about the trips recounted in this section, and I have reviewed correspondence, agendas, and travel records confirming the details. It appears that the LADWP officials and employees who participated in the trips obtained approval and funding from LADWP to attend. PARADIS and WRIGHT advised that PARADIS funded all travel expenses for himself and AVENTADOR employees and did not seek reimbursement from LADWP.

companies sought to obtain contracts with LADWP, and several subsequently took steps to establish a business relationship with LADWP. The agenda and the logistics of the trip were arranged by an Israeli broker named BARUCH "BOOKY" OREN, whom LADWP Chief Operating Officer [redacted] introduced to WRIGHT and others at LADWP sometime before May 2018.

159. During the initial May 2018 trip to Israel, one of the companies with which the LADWP delegation met was CYBERGYM, an Israeli company focusing on cybersecurity training for utilities. PARADIS proffered that during the May 2018 trip, CYBERGYM executive [redacted] and PARADIS discussed the possibility of PARADIS investing in CYBERGYM in some capacity. PARADIS and WRIGHT subsequently discussed bringing a CYBERGYM facility to Los Angeles, and according to PARADIS, WRIGHT agreed to commit LADWP to purchase $3 million per year in training at the facility for a period of five years.[76] **PARADIS further advised the government that he and WRIGHT had agreed that WRIGHT would have an ownership interest in CYBERGYM after WRIGHT's retirement, a fact that WRIGHT confirmed in recorded conversations with PARADIS.** I believe that these facts show another instance of WRIGHT accepting a bribe in the form of an undisclosed joint future financial interest with PARADIS, AVENTADOR, and CYBERGYM in exchange for WRIGHT's continued support of AVENTADOR's current and future contracts and CYBERGYM's future contract with LADWP.

[76] PARADIS stated that WRIGHT lacked the authority to formally approve such a commitment.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

160. In the months following the May 2018 Israel trip, PARADIS and [redacted] negotiated a joint venture agreement whereby PARADIS would open a CYBERGYM facility in Los Angeles to provide training to LADWP employees.

161. According to PARADIS, when OREN learned soon after the May 2018 trip that PARADIS and CYBERGYM were engaging in business negotiations, OREN was upset and demanded what PARADIS described as a "kickback" from PARADIS because OREN had brought PARADIS/LADWP and Cybergym together. **PARADIS reported that he declined to pay OREN the "kickback," but that he instead agreed to engage OREN as a paid consultant for $500,000 per year.** For at least the next year, OREN proceeded to send PARADIS monthly invoices for $41,667, which I have reviewed. Each invoice describes OREN's work as "Advisory Services," with no further itemization or explanation. According to PARADIS, he paid OREN for his business connections, because OREN knew a lot of people in the water industry and could arrange meetings at which PARADIS could seek business opportunities. In June 2019, when asked what value OREN had provided over the past year for his $500,000 annual fee, PARADIS stated that OREN had arranged meetings for PARADIS in May and June 2019 with utilities in Tucson, Denver, and Las Vegas. PARADIS further reported that in June 2019, OREN had requested a "success fee" on top of his $41,667 monthly advisory services fee. It is unclear to me, and PARADIS professed not to know, what this "success fee" would be intended to cover.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

162. PARADIS provided the government with his emails with OREN. They include the following emails reflecting the terms of their business agreement:

a. In an email to OREN, PARADIS confirmed the nature of their agreement as a joint venture, whereby all of OREN's U.S. cyber security business would be performed with AVENTADOR. PARADIS also agreed to pay OREN $41,667 per month, with the May 2018 invoice to reflect the commencement of their joint venture on May 14, 2018.

b. OREN replied with three clarifications to the contractual terms that they had discussed and that were articulated in PARADIS's email: 1) **OREN's $500,000 annual compensation was to cover only LADWP matters**, with OREN's additional compensation on other AVENTADOR projects to be discussed as needed; 2) the joint venture agreement would also cover all cyber security business by AVENTADOR with other U.S. utilities; and 3) **OREN "will support the best solution to LADWP," but can still "receive consultant fee from vendors."**

c. PARADIS replied that he would work in the additional provisions specified by OREN and circulate another agreement. I did not see any such further email.

163. Following the LADWP delegation's initial May 2018 visit to Israel facilitated by OREN, and PARADIS's entry into a joint venture with OREN that same month on behalf of AVENTADOR and/or LADWP, PARADIS and OREN worked together to arrange three additional trips to Israel for LADWP and AVENTADOR staff, and one Israeli delegation visit to LADWP, over the next six months.

Via PARADIS and WRIGHT, LADWP pursued memoranda of understanding ("MOUs") with individual Israeli companies that would permit mutual sharing of sensitive information and provide for mutual nondisclosure, and emails indicate that LADWP signed at least one such MOU with an Israeli vendor.

164. During one visit to Israel in the second half of 2018, AVENTADOR employees obtained software samples from several Israeli companies that were seeking to sell products or services to LADWP.[77] With respect to one such transaction, an AVENTADOR employee advised PARADIS in September 2018 that they should not provide detailed information about the LADWP network to an Israeli company that was seeking to market its products to LADWP. In subsequent tests of the software samples provided by the Israeli companies, AVENTADOR employees determined that the software provided by one Israeli company was secretly sending data back to Israel through a backdoor channel, so AVENTADOR decided not to use that company or recommend it to LADWP. To my knowledge, that potential counterintelligence issue was not reported to the federal government.

165. In April 2019 -- following PARADIS's divestment from AVENTADOR and the formation of ARDENT, an entity from which PARADIS is allegedly disconnected – in an email that I have reviewed, PARADIS directed his law firm accountant to pay OREN's

[77] The degree to which AVENTADOR's involvement with these Israeli companies was sanctioned by LADWP, and the extent to which it was done on behalf of LADWP, is unclear to me. As with the rest of this affidavit, the information in this section represents my best understanding based on the facts available to me at this time.

February and March 2019 invoices from ARDENT's operating account. PARADIS's accountant agreed to do so.

166. In a proffer session, WRIGHT advised that LADWP did not pay OREN any money for his services in arranging travel and meeting logistics, and that **it was WRIGHT's understanding that OREN would be compensated in the form of a "success fee" from any Israeli company that was ultimately successful in obtaining a contract with LADWP**.

167. I believe that the arrangement whereby OREN would receive financial compensation from a vendor who successfully obtained a contract with LADWP was properly characterized as a kickback, that many kickbacks are illegal, and that they may also constitute evidence of other bribery or corruption schemes. I further believe that PARADIS's $500,000 annual payments to OREN, which were reportedly solely to compensate OREN for his access to officials at other utilities and businesses and which apparently did not require much or any actual work by OREN, may have been intended to fund unlawful kickbacks or bribes to government officials in order to facilitate other contracts that PARADIS and/or AVENTADOR sought.

H. Obstruction of Justice by WRIGHT[78]

1. <u>WRIGHT's Request That PARADIS Destroy Evidence in His Email Accounts and on His Laptop and Cell Phone</u>

168. On March 28, 2019, PARADIS and WRIGHT exchanged text

[78] The recordings described in the section are some of the consensually recorded conversations with WRIGHT. As previously noted, I have not included every recording between PARADIS and WRIGHT.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Case 2:24-cv-01650-SB Document 28 Filed 06/07/24 Page 430 of 1425 Page ID #:1636

concerned about the AVENTADOR laptop computer (WRIGHT's laptop) that PARADIS had previously given to him. Following a discussion of their options concerning those communications, WRIGHT requested that PARADIS "get his people" to destroy all evidence of their communications on WRIGHT'S phone and all information on WRIGHT's laptop.[79] Specifically, WRIGHT told PARADIS to destroy all his emails from his two AOL email accounts, as well as the corresponding iCloud accounts for them.

171. WRIGHT agreed to provide his phone and laptop to PARADIS in order to have the devices "wiped" clean of incriminating evidence. In addition, WRIGHT told PARADIS that he already shredded all related documents within **WRIGHT's OFFICE** that involved PARADIS and/or LEVINE, and that he planned to do so again the following week.[80] PARADIS agreed to wipe WRIGHT's phone and laptop and delete all emails on the provider's servers. In addition, WRIGHT and PARADIS discussed utilizing the application Confide to communicate as a means to conceal

---

[79] Based on the context of the conversation and my knowledge of this case, I understood this to be a reference to the team of hackers and intelligence agency veterans that PARADIS had recruited and hired to work for AVENTADOR on the above-referenced cybersecurity issues.

[80] Based on WRIGHT confirming that evidence related to the Target Offenses was contained in **WRIGHT's OFFICE**, and that WRIGHT planned to destroy additional evidence the next week, I believe there is probable cause and a search warrant for **WRIGHT's OFFICE** is necessary to identify (1) indicia that evidence was destroyed (shredded paper, labeled but empty labeled folders/cabinets, other evidence of missing items), (2) if WRIGHT failed to destroy everything and there still remains evidence of the Target Offenses and criminal schemes, or (3) if WRIGHT did not destroy the evidence as described and the evidence remains in **WRIGHT's OFFICE**.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

their communications.[81]

172. On March 31, 2019, in a consensually recorded meeting, WRIGHT provided his phone and laptop to PARADIS so that, as he and PARADIS had agreed, PARADIS could wipe the devices to include deleting all text messages and emails. WRIGHT and PARADIS agreed to meet in Santa Monica, California, on April 1, 2019, to return WRIGHT's phone wiped. PARADIS subsequently provided WRIGHT's phone and laptop to the FBI to preserve all evidence on the phone and laptop.

173. On April 1, 2019, in a consensually recorded meeting, PARADIS and WRIGHT discussed further concealing their future communication via "burner"[82] phones. PARADIS and WRIGHT agreed to meet on April 3, 2019, at the Disney Concert Hall in Los Angeles, California, for WRIGHT to pick up a burner phone from PARADIS.

174. On April 3, 2019, I conducted surveillance of PARADIS and WRIGHT's meeting at the Disney Concert Hall. PARADIS was seated at a table in the back corner of the café with a brown paper bag that contained WRIGHT's burner phone (provided to him by the FBI) and WRIGHT's phone. WRIGHT approached PARADIS and provided a head nod which PARADIS understood to mean WRIGHT acknowledged PARADIS' presence. PARADIS subsequently left the bag with the two phones on the table and walked into the men's

[81] Confide is an encrypted messaging application that deletes each communication after it is viewed. PARADIS proffered that WRIGHT had previously asked him to use Confide in connection with the Target Offenses and criminal schemes.

[82] A "burner" phone is typically a difficult to trace phone that provides little to no paper trail back to its user.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Case 2:24-cv-01650-SB Document 28 Filed 06/07/24 Page 433 of 1425 Page ID #:1639
Case 2:24-cv-01650-SB Document 28-1

Case 2:24-cv-01650-SB Document 28 Filed 06/07/24 Page 434 of 1425 Page ID #:1640

Case 2:24-cv-01650-SB Document 28 Filed 06/07/24 Page 435 of 1425 Page ID #:1641

running CIP violations, which thereby made it appear that WRIGHT was acting properly and prudently on behalf of LADWP. WRIGHT verbally acknowledged both items and agreed those items should be concealed in the presentation. In subsequent consensually recorded meetings with WRIGHT, WRIGHT agreed to conceal this information from the Mayor's Office, City Attorney's Office, and LADWP Board.

180. On May 18, 2019, in a consensually recorded meeting, PARADIS met WRIGHT at PARADIS's Rancho Mirage residence. During the meeting PARADIS and WRIGHT discussed the presentation further. WRIGHT stated that he wanted to show PARADIS edits he had made, but that he had forgotten the presentation at his home. WRIGHT therefore requested PARADIS to meet him the following day. WRIGHT discussed an initial presentation that he had with City officials including Deputy Mayor Barbara Romero; staff members of the Mayor's Office; LADWP Director of Communications, Media, and Community Affairs [redacted]; LADWP General Counsel Joseph Brajevich; and LEVINE. According to WRIGHT, the first version of this presentation detailed the events at LADWP that led to the award of the contracts to PARADIS LAW GROUP and AVENTADOR. WRIGHT described the presentation as a thirty-seven page blend of what WRIGHT and PARADIS drafted. WRIGHT stated that the presentation laid out the CC&B billing system problems that led WRIGHT to offer PARADIS the "Project Management" contract to lead the CC&B system remediation effort. In addition, the presentation included PARADIS's role in implementing the requirements of the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Jones class action settlement and in remediation of cyber security issues. WRIGHT stated that he pointed out how many times people in the Mayor's Office, the City Attorney's Office, and the LADWP Board were informed of the circumstances involving these three areas and how they had all approved of PARADIS leading these efforts on a number of occasions. WRIGHT told PARADIS that Romero and the others in the Mayor's Office were quick to change course during his presentation and soon said that they now recalled these events and that these could not be dredged back up again because doing so would potentially hurt the Mayor's public opinion. Romero then said that the presentation should be made to the City Council Energy and Environmental Committee in closed session only and that the presentation needed to be cut down drastically to omit the background facts that led to PARADIS's appointment in the first place.

181. During this same meeting, WRIGHT and PARADIS discussed a cyber contract that would be subject to a request for proposal ("RFP") process and be awarded at the conclusion of ARDENT's current contract. WRIGHT instructed PARADIS to work with KWOK and ALEXANDER to draft the RFP.[86] WRIGHT, however, did not want KWOK or ALEXANDER to know that PARADIS was in communication with

[86] Based on subsequent recorded conversations between PARADIS and KWOK and/or ALEXANDER, the new contract would be directly awarded by LADWP. The contract was expected to be a three-year contract totaling $75 million to $87.5 million.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

WRIGHT because WRIGHT did not feel KWOK would lie under oath[87] for WRIGHT, regarding his communications with PARADIS, and WRIGHT did not trust ALEXANDER.

182. Regarding the Jones case, WRIGHT recalled being a part of a 2015 meeting with the City Attorney's Office and PARADIS in which CLARK directed PARADIS to "flip" Jones to LANDSKRONER so that the City could control the settlement and that CLARK was the one who quarterbacked the strategy and the settlement of the Jones case. In addition, WRIGHT recalled a meeting with CLARK, PARADIS, TUFARO, PETERS, and WRIGHT prior to CLARK's deposition testimony in which this strategy, orchestrated by CLARK, was discussed. WRIGHT said that CLARK is now lying to the court by saying he did not have knowledge of the Jones arrangements.

183. On May 20, 2019, in a consensually recorded conversation, PARADIS met WRIGHT at WRIGHT's son's apartment in downtown Los Angeles. During the meeting, PARADIS and WRIGHT further discussed the presentation for the Energy and Environmental Committee. In PARADIS's presence, WRIGHT spoke to LEVINE. PARADIS overheard WRIGHT and LEVINE discussing strategy regarding what should and should not be included in the closed E & E Committee presentation. After the call with LEVINE, WRIGHT and PARADIS discussed the presentation further and WRIGHT stated that LEVINE was going to request the same presentation in closed session to the LADWP Board.

---

[87] PARADIS believed this to mean KWOK would not lie under oath in the event he was deposed in any civil litigation related to AVENTADOR/ARDENT, or questioned by law enforcement about the same.

184. On May 21, 2019, in a consensually recorded conversation, PARADIS met with KWOK to discuss the RFP. Included in the discussion was the evaluation criterion for who would be selected. KWOK started that he spoke to ALEXANDER about how they could control the evaluation team to ensure that they determine the outcome to guarantee that those entities they wanted to hire were certain of being selected. In a May 29, 2019 text message, WRIGHT instructed PARADIS to instruct KWOK and ALEXANDER to include WRIGHT as an evaluator. I believe WRIGHT wanted to be an evaluator to help ensure ARDENT/NEWCO (in which WRIGHT had a significant financial interest) received this future lucrative contract.

185. On May 26, 2019, PARADIS met with WRIGHT and discussed a LADWP Cyber RFP[88] for additional cyber services. WRIGHT requested that PARADIS send the draft to KWOK and ALEXANDER so that they could in turn "officially" send the REF to WRIGHT for his approval. Based on my review of emails between PARADIS, KWOK, and ALEXANDER regarding the RFP, KWOK and ALEXANDER were aware that PARADIS was drafting the RFP directly with WRIGHT, indicating that the process was fixed and not an arms-length City process, as it should have been.

VI. CONCERNS ABOUT SPOLIATION OF EVIDENCE

186. While some of the evidence sought by the requested warrants could, under other circumstances, be obtained by other

[88] WRIGHT, KWOK, and ALEXANDER requested PARADIS's assistance in drafting the RFP.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

means, specific concerns about spoliation of evidence have compelled the government to seek the instant warrants.

A. Destruction or Concealment of Evidence and False Testimony

187. Certain high-ranking officials at both LADWP and the City Attorney's Office have demonstrated a willingness to destroy evidence, testify falsely under oath, and otherwise obstruct justice. While these officials do not represent their entire offices, they are sufficiently highly placed within those offices to give rise to significant concerns of undue influence or interference should they be asked to simply self-produce evidence that may implicate them in criminal or ethical violations or otherwise put the City Attorney's Office in a bad light. Specific examples, which are further described herein, include:

a. LADWP General Manager DAVID WRIGHT secretly accepted a future executive position at a $1 million annual salary with a company for which he then facilitated a $30 million LADWP contract; he then took actions to have his phone and laptop forensically wiped to conceal evidence of these crimes.

b. LADWP Chief Cyber Risk Officer DAVID ALEXANDER described, in recorded conversations, an elaborate secret plan to identify LADWP computer equipment containing evidence of crimes and regulatory violations that he and other LADWP employees had committed over the past decade, and to destroy

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

that equipment, in an effort to, according to ALEXANDER, avoid "going to jail."

c. As detailed above, Chief Deputy City Attorney JAMES CLARK provided sworn deposition testimony that was internally inconsistent and, in many instances, demonstrably false.

d. At his deposition, CLARK testified that he took investigative notes to prepare, but then destroyed them in the days before the deposition. CLARK then repeatedly testified that he could not recall key facts relevant to his investigation.

e. CLARK and then-Chief of Civil Litigation THOMAS PETERS allegedly knew about and encouraged a substantial financial payment to keep a threatened whistleblower from exposing the City Attorney's Office's conduct of collusive litigation in the LADWP billing matter and at least one other case.

B. The City's April 26, 2019 Filing of Selected Documents

188. Recent conduct by and on behalf of the City Attorney's Office in the ongoing *LADWP v. PwC* litigation undermines the government's confidence in the integrity of any self-production should the government pursue a mechanism other than a search warrant.

a. In late April 2019, the City filed a Notice re Documents in the *City v. PwC* case (the "City's Notice"). The City's Notice attached approximately two dozen emails that it

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

stated had been newly discovered in a .pst file,[89] stating: "The .pst file contains 131 records, including emails among Paul Kiesel, Paul Paradis, Michael Libman and/or Jack Landskroner. (No City employee or officer sent or received any of these emails.)" The City's Notice was paired with a media statement accusing its former Special Counsel [PARADIS and KIESEL] of a "reprehensible breach of ethics."

b. While it was technically true that none of the handful of emails that the City selected to disclose and publicly file were sent to or from City employees, it was subsequently revealed that many of the other 131 documents —— which the City sought to protect as privileged or confidential —— were not only sent to or from City employees but in fact showed members of the City Attorney's Office's active involvement in the collusive litigation that their media statement had described as a "reprehensible breach of ethics."

---

[89] The City's Notice stated that this .pst file had been recovered from a forensically imaged hard drive, which was later revealed to belong to PETERS. At his deposition in the days after the City's filing of selected emails, CLARK testified to his understanding that PETERS "had never seen the documents before, and was outraged" when he learned about them. Later, after metadata for the .pst file showed that PETERS had in fact downloaded the contents from a Dropbox link and saved them to his hard drive, PETERS acknowledged that he had done so, but testified that he had no recollection of doing so or of reading the emails.

CLARK also testified that to his knowledge, no emails on the .pst file were sent to or from City employees or officials. He further testified that he was "outranged, angry, disgusted" upon reading the emails that the City had selected for release. As detailed herein, KIESEL subsequently revealed documents indicating that many of these emails were sent to or from City officials and employees, including CLARK.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

c. The City's disingenuous portrayal of its then-terminated Special Counsel, PARADIS and KIESEL, as rogue actors for engaging in conduct that was, according to testimony and documentary evidence, directed by the City Attorney's Office at the highest levels causes the government concern about relying on those who developed, executed, and sanctioned this strategy to scrupulously produce evidence of that conduct.

C. Attempts to Shield Certain Deposition Testimony

a. In April and May 2019, following PETERS's abrupt walk-out during the middle of his ordered deposition and CLARK's post-testimony issuance of an "errata" seeking to retract or reverse much of his substantive testimony, the court ordered the City to produce CLARK and PETERS to testify again. At those depositions, the City demanded that all parties accept a designation of both witnesses' testimony as "confidential" pursuant to an existing protective order. The protective order provided that a party could designate as non-public any testimony that the party believed in good faith: 1) would risk competitive injury or security breach, 2) was subject to an obligation of confidentiality owed to a third party, 3) implicated the privacy of an individual, or 4) was required to be kept confidential by law.

b. In light of these narrow categories, it is unclear why the City designated as confidential the testimony of these public servants about the manner in which they served the public. This effort to shield from public scrutiny the

activities of its senior public officials related to the collusive litigation further heightens the government's misgivings that the City would be forthcoming with full and complete evidence if confronted with a subpoena or request for voluntary production.

D. The Overall Conduct of the Collusive Litigation

a. Standing alone, I believe the established facts of the collusive litigation paint a picture of fraud on the court and the public. In summary and further described below, the City hand-selected a lawyer for a favored plaintiff on the grounds that this lawyer would be more compliant with the City's interests, as opposed to vigorously advocating for those of their true client, the plaintiff(s); provided substantial non-public LADWP information, along with the existing complaints, to feed a new complaint that would effectively overtake all of the causes of action filed by opposing counsel who were not controlled by the City; directed certain activities of its hand-picked lawyer; quickly settled on the exact terms that the City wanted from the very start; and paid nearly $20 million in taxpayer money to the plaintiffs' lawyers, with the hand-picked lawyer who did nearly no independent work receiving the lion's share.

b. None of these backroom dealings —— which led to at least one participant covertly receiving a multimillion dollar kickback in exchange for facilitating the collusive litigation —— were divulged to the court overseeing the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

litigation, and the City has fought for years to obscure them from public view.

VII. PREMISES INFORMATION

186. I have learned the following information from cooperating witnesses and open-source research:

187. LADWP's main office is located in the John Ferraro Building at 111 N. Hope Street, Los Angeles, California. WRIGHT's office suite is located there, believed to be in or near Office #1603. Additionally, the LADWP Board of Commissioners operates out of space on the 15th floor of that building; the LADWP Board meeting room is labeled 1555H, and with each Commissioner assigned to an office in 1555 in the vicinity of the Board meeting room. The Board secretary is assigned to an office, also in that vicinity, as are each of three Board assistants. There are Board records and files, including draft and final agendas, attachments, filings, video film, meeting minutes, travel arrangements, and other documents reflecting Board business stored in filing cabinets in and around the Board offices and on the LADWP computer system. An assistant to the Board secretary, [redacted], is assigned to an office 1221; [redacted] also assists in maintaining records of Board business.

188. ARDENT operates out of office space in the 111 N. Hope Street building, on the northern end of the 15th floor, facing the Temple/Fremont intersection.

189. The members of the City Attorney's Office assigned to LADWP, including SOLOMON, TOM, and DORNY, work in office space

at 221 N. Figueroa Street, Los Angeles, California. I have received information indicating that SOLOMON, TOM, and DORNY work out of offices on the 10th floor of that building, in or near Suite 1000.

190. In addition to the files and records reflecting LADWP business stored at the above-described building, LADWP also maintains file storage space at 5848 Miramonte Blvd., Los Angeles, California. Certain LADWP records, including documents reflecting matters that are not currently being worked on or for which there is overflow material, are stored there. Additionally, some historical Board records are maintained in a vault in that space.

191. CLARK's office suite is located in City Hall East, at 200 N. Main Street, Los Angeles, California, on the 8th floor. Files and records relating to ongoing and recent cases are stored in storage areas throughout the City Attorney's Office.

VIII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[90]

192. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

---

[90] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

193. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

194. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

IX. BACKGROUND ON E-MAIL AND THE PROVIDER

195. In my training and experience, I have learned that providers of e-mail and/or social media services offer a variety of online services to the public. Providers, like the PROVIDER, allow subscribers to obtain accounts like the SUBJECT ACCOUNTS. Subscribers obtain an account by registering with the provider. During the registration process, providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail or social media account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). Some providers also maintain a record of changes that are made to the information provided in subscriber records, such as to any other e-mail addresses or phone numbers supplied in subscriber records. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of an account.

196. Therefore, the computers of a PROVIDER are likely to contain stored electronic communications and information concerning subscribers and their use of the PROVIDER's services, such as account access information, e-mail or message transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of a SUBJECT ACCOUNT.

197. A subscriber of a PROVIDER can also store with the PROVIDER files in addition to e-mails or other messages, such as address books, contact or buddy lists, calendar data, pictures or videos (other than ones attached to e-mails), notes, and other files, on servers maintained and/or owned by the PROVIDER. In my training and experience, evidence of who was using an account may be found in such information.

198. In my training and experience, e-mail and social media providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail and social media providers often have records of the

Internet Protocol ("IP") address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a SUBJECT ACCOUNT.

199. In my training and experience, e-mail and social media account users will sometimes communicate directly with the service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers of e-mails and social media services typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of a SUBJECT ACCOUNT.

200. I know from my training and experience that the complete contents of an account may be important to establishing the actual user who has dominion and control of that account at a given time. Accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. Given the ease with which accounts may be created under aliases, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of an account,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

investigators often have to rely on circumstantial evidence to show that an individual was the actual user of a particular account. Only by piecing together information contained in the contents of an account may an investigator establish who the actual user of an account was. Often those pieces will come from a time period before the account was used in the criminal activity. Limiting the scope of the search would, in some instances, prevent the government from identifying the true user of the account and, in other instances, may not provide a defendant with sufficient information to identify other users of the account. Therefore, the contents of a given account, including the e-mail addresses or account identifiers and messages sent to that account, often provides important evidence regarding the actual user's dominion and control of that account. For the purpose of searching for content demonstrating the actual user(s) of a SUBJECT ACCOUNT, I am requesting a warrant requiring the PROVIDER to turn over all information associated with a SUBJECT ACCOUNT with the date restriction included in Attachment B for review by the search team.

201. Relatedly, the government must be allowed to determine whether other individuals had access to a SUBJECT ACCOUNT. If the government were constrained to review only a small subsection of an account, that small subsection might give the misleading impression that only a single user had access to the account.

202. I also know based on my training and experience that criminals discussing their criminal activity may use slang,

short forms (abbreviated words or phrases such as "lol" to express "laugh out loud"), or codewords (which require entire strings or series of conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of a message or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and parenthesis :) to convey a smile or agreement) to discuss matters. "Keyword searches" would not account for any of these possibilities, so actual review of the contents of an account by law enforcement personnel with information regarding the identified criminal activity, subject to the search procedures set forth in Attachment B, is necessary to find all relevant evidence within the account.

203. This application seeks a warrant to search all responsive records and information under the control of the PROVIDER, which is subject to the jurisdiction of this court, regardless of where the PROVIDER has chosen to store such information.

204. As set forth in Attachment B, I am requesting a warrant that permits the search team to keep the original production from the PROVIDER, under seal, until the investigation is completed and, if a case is brought, that case

is completed through disposition, trial, appeal, or collateral proceeding.

a. I make that request because I believe it might be impossible for a provider to authenticate information taken from a SUBJECT ACCOUNT as its business record without the original production to examine. Even if the provider kept an original copy at the time of production (against which it could compare against the results of the search at the time of trial), the government cannot compel the provider to keep a copy for the entire pendency of the investigation and/or case. If the original production is destroyed, it may be impossible for the provider to examine a particular document found by the search team and confirm that it was a business record of the provider taken from a SUBJECT ACCOUNT.

b. I also know from my training and experience that many accounts are purged as part of the ordinary course of business by providers. For example, if an account is not accessed within a specified time period, it -- and its contents -- may be deleted. As a consequence, there is a risk that the only record of the contents of an account might be the production that a provider makes to the government, for example, if a defendant is incarcerated and does not (perhaps cannot) access his or her account. Preserving evidence, therefore, would ensure that the government can satisfy its Brady obligations and give the defendant access to evidence that might be used in his or her defense.

X. REQUEST FOR NON-DISCLOSURE

205. Pursuant to 18 U.S.C. § 2705(b), I request that the Court enter an order commanding the PROVIDERS not to notify any person, including the subscribers of the SUBJECT ACCOUNTS, of the existence of the warrant until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date the requested warrant is signed by the magistrate judge, or such later date as may be set by the Court upon application for an extension by the United States. There is reason to believe that such notification will result in: (1) flight from prosecution; (2) destruction of or tampering with evidence; (3) intimidation of potential witnesses; (4) otherwise seriously jeopardizing the investigation; or (5) exposing the identities of confidential sources who have cooperated with the government and in some cases may continue to actively and covertly cooperate.

XI. AFFIDAVIT NOT ATTACHED TO SEARCH WARRANT

206. The affidavit has not been attached to the search warrants because allowing disclosure during the search would give subjects and targets of the investigation an opportunity to destroy evidence, change patterns of behavior, notify confederates, flee from prosecution, or otherwise seriously jeopardize the investigation. In addition, I am aware that "if the face sheet and attachments clearly state that the agents have lawful authority to conduct the search and specify the location to be searched and the items sought, the affidavit

supporting the probable cause determination need not be served at the time of the search." United States v. Celestine, 324 F.3d 1095, 1100, 1101 (9th Cir. 2003).

XII. CONCLUSION

207. Based on the foregoing, I request that the Court issue the requested search warrants.

ANDREW CIVETTI, Special Agent
Federal Bureau of
Investigation

Subscribed to and sworn before
me on July 18, 2019.

HONORABLE PATRICK J. WALSH
UNITED STATES MAGISTRATE JUDGE

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

XIII. Search Warrants Reference Chart

Case No.	No.	Att A	Att A Description	No.
	A-1	Microsoft	1. james.p.clark@lacity.org; 2. thom.peters@lacity.org; 3. david.wright@ladwp.com; 4. marcie.Edwards@ladwp.com; 5. donna.stevener@ladwp.com; 6. richard.brown@ladwp.com; 7. richard.tom@ladwp.com; 8. eskel.solomon@ladwp.com; 9. deborah.dorny@ladwp.com; 10. david.alexander@ladwp.com; 11. [redacted] 12. stephen.kwok@ladwp.com; 13. [redacted] 14. mel.levine@ladwp.com; 15. william.funderburk@ladwp.com; 16. [redacted]; 17. kiesel@kiesellaw.com; 18. [redacted]	B-1
	A-2	Google	19. [redacted]	B-2
	A-3	City Hall East	200 N. Main Street, Los Angeles, California 1. JAMES CLARK's Office 2. File Storage Locations	B-3
	A-4	LADWP	111 N. Hope Street, Los Angeles, California 3. The Office of the General Manager (**WRIGHT's OFFICE**) 4. LADWP Commissioner's Offices (Room #1555) 5. LADWP Board Office, including work space used by LADWP Board Secretary and LADWP Board Assistants (Room #1555) 6. LADWP Board Room (Room #1555-H) 7. LADWP Board file storage space outside LADWP Board Room (15th floor) 8. STEPHEN KWOK's Office (Room #1544) 9. [redacted] Office (Room #1221) 10. DAVID ALEXANDER's Office (Room #251)	B-4

Case No.	No.	Att A	Att A Description	No.
	A-5	City Property 10th Floor	221 N. Figueroa Street, 10th Floor, Los Angeles, California 11. RICHARD TOM's Office 12. DEBROAH DORNEY's Office 13. ESKEL SOLOMON's Office	B-5
	A-6	LADWP Records Retention	14. 5848 Miramonte Boulevard, Los Angeles, California	B-6
	A-7	City Property 15th Floor	221 N. Figueroa Street, 10th Floor, Los Angeles, California 15. AVENTADOR/ARDENT Office's (15th Floor – North side of building)	B-7
	A-8	Kiesel Office	16. 8648 Wilshire Boulevard, Beverly Hills, California	B-8

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AO 93 (Rev. 11/13) Search and Seizure Warrant (USAO CDCA Rev. 04/17)

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information associated with items identified in Attachment A-7 that is within the possession, custody, or control of Aventador/Ardent Offices, 221 N. Figueroa Street, Los Angeles, CA	)	Case No. 2:19-MJ-02913

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-7

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B-7

Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 7/18/19 3:30 p.m.

Patrick J. Walsh

Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh, U.S. Magistrate Judge

Printed name and title

AUSA: Melissa Mills (213) 894-0627

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:19-MJ-02913	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-7 [Aventador/Ardent Offices]

PROPERTY TO BE SEARCHED

The premises to be searched are located at **221 N. Figueroa Street, 15th Floor, Los Angeles, California ("City Property 15th Floor")** and pictured below. Specifically, the following locations within the City Property are to be searched.

1. **Aventador/Ardent Office's** (15th Floor – North side of building)

ATTACHMENT B-7 (Ardent Offices)

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 16 U.S.C. §§ 824o, 825o (Knowing and Willful Violation of Electric Reliability Standards) (the "Target Offenses"), namely:

a. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Formation, incorporation, purchase, or transfer of the company;

ii. Contracts, bids, proposals, or requests for proposal;

iii. Invoices, bills, timesheets, expense reimbursements, daily cash reports, expense reports;

iv. Business development, marketing, or advertising;

v. Board, agency, City Council, or other customer presentations;

vi. Communications with or concerning officials or employees with the City of Los Angeles;

vii. Communications with or concerning PAUL PARADIS, GINA TUFARO, PARADIS LAW GROUP, [redacted], or any other employee or officer of PARADIS LAW GROUP;

viii. AVENTADOR UTILITY SOLUTIONS LLC ("AVENTADOR");

ix. Any future enterprise to be developed from ARDENT UTILITY SOLUTIONS LLC ("ARDENT") or AVENTADOR;

x. Business-related foreign travel by employees or officers of AVENTADOR or ARDENT, or by employees or officials of the City of Los Angeles, between January 1, 2018, through the present; coordination by AVENTADOR, ARDENT, or the City of Los Angeles with foreign governments or entities; memoranda of understanding or other information-sharing agreements with foreign governments or entities; witting or unwitting transfer of proprietary or sensitive information belonging or relating to the City of Los Angeles;

xi. Penetration testing or other intrusions into networks or systems of any entity, whether authorized or unauthorized;

xii. Any physical security or cybersecurity issues, risks, or threats identified at LADWP, including any communications or presentations to LADWP employees, LADWP Board members, or Los Angeles City Council members;

xiii. Any physical security or cybersecurity assessments or surveys performed for or at LADWP, from June 1, 2008, to the present, whether by ARDENT, AVENTADOR, Element

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Digital, Oracle, SDI Presence, LLC, Robert Bigman, West Monroe, or any other cybersecurity vendor;

xiv. Any cybersecurity or physical security risk management, mitigation or remediation relating to cybersecurity or physical security issues identified at LADWP after June 1, 2008;

xv. Any certifications, reports, statements, or other communications to the Western Electricity Coordinating Council ("WECC"), the North American Electric Reliability Corporation ("NERC"), or the Federal Energy Regulatory Commission ("FERC") regarding compliance or failure to comply with NERC Critical Infrastructure Protection ("NERC-CIP") standards;

xvi. Falsification, manipulation, or destruction of records, data, or other information relating to compliance with NERC-CIP standards;

xvii. Destruction or concealment of evidence.

b. Bank records, tax records, and other financial records;

c. Employment and personnel records for all current and former AVENTADOR and ARDENT employees or officers, including work history, performance reviews, evaluations, ethical screens, lodged complaints, disciplinary actions, administrative leave, suspension, and dismissal;

d. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

e. Any digital device and data servers, to include the Los Angeles City server, capable of being used to commit or further the Target Offenses, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such Target Offenses, and forensic copies thereof.

f. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

1. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

2. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

3. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

4. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AO 93 (Rev. 11/13) Search and Seizure Warrant (USAO CDCA Rev. 04/17)

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information associated with items identified in Attachment A-3 that is within the possession, custody, or control of Los Angeles City Hall East building, located at 200 N. Main Street, Los Angeles, CA ("City Hall East")	)	Case No. 2:19-MJ-02914

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-3

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B-3

Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 7/18/19 3:30 p.m.

Patrick J. Walsh

Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh, U.S. Magistrate Judge

Printed name and title

AUSA: Melissa Mills (213) 894-0627

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:19-MJ-02914	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

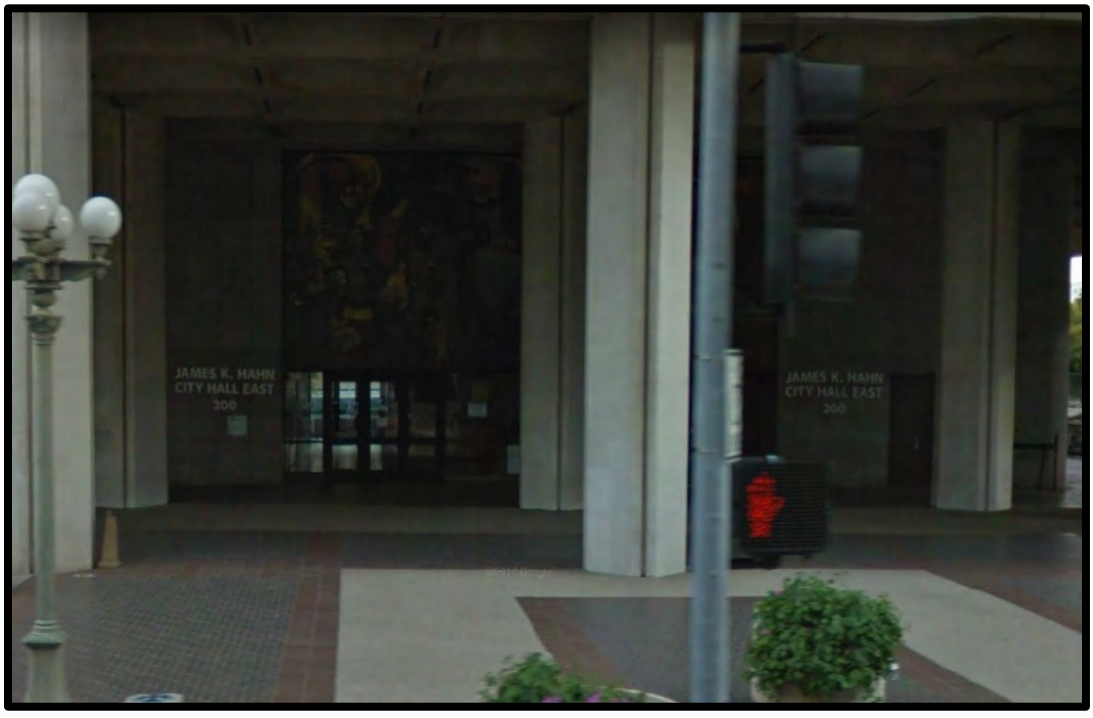
_____
Printed name and title

ATTACHMENT A-3 [City Hall East – City Attorney's Office]

PROPERTY TO BE SEARCHED

The premises to be searched are located at the Los Angeles City Hall East building located at **200 N. Main Street, Los Angeles, California**, ("**City Hall East**") and pictured below. Specifically, the following locations within **City Hall East** are to be searched:

1. **James Clark's Office**
2. **File Storage Locations** [specifically containing records of former employees, and files and records from litigation and other processes related to the Los Angeles Department of Water and Power billing system]



ATTACHMENT B-3 (City Attorney's Office)

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); and 1956 (Money Laundering) (the "Target Offenses"), namely:

a. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Procedures and actions by the City Attorney's Office, LADWP, or the City of Los Angeles, or employees, representatives, or officials thereof, regarding proposed or considered debarment of PricewaterhouseCoopers ("PwC");

ii. Any lawsuit to which the City, or any City employee, official, or representative, was a party and had a legal, representational, and/or financial interest in both sides of the lawsuit;

iii. For the period from January 1, 2014, through the present, any practices, policies, or protocols for retention of special counsel or other outside counsel to represent the City of Los Angeles;

iv. Retention of PAUL PARADIS and PAUL KIESEL, or entities related thereto, to represent the City of Los Angeles;

v. Communications involving or relating to any party to, or counsel for party to, *Jones v. City of Los Angeles* ("the *Jones* matter") or *City of Los Angeles v. PricewaterhouseCoopers* ("the *PwC* matter");

vi. Litigation or contemplated litigation concerning the LADWP Customer Care and Billing ("CC&B") billing system;

vii. Remediation of the LADWP CC&B system;

viii. Communications with any party to or counsel for party to any lawsuits, including but not limited to class action lawsuits, that alleged problems with the LADWP CC&B billing system;

ix. Communications with the independent monitor appointed in the *Jones* matter, PAUL BENDER, or records relating to the consideration and selection of an independent monitor in that case;

x. Financial payments, gifts, services, or other benefits given to, offered to, or solicited by City employees or officials or their staff or family members;

xi. Any business venture in which a City official, employee, or representative had a financial interest, including but not limited to AVENTADOR UTILITY SOLUTIONS, LLC, CYBERGYM, and ARDENT UTILITY SOLUTIONS, LLC;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

xii. Employment and personnel records, including work history, performance reviews, evaluations, ethical screens, lodged complaints, disciplinary actions, administrative leave, suspension, and dismissal, for JAMES P. CLARK, THOMAS PETERS, RICHARD BROWN, RICHARD TOM, ESKEL SOLOMON, and DEBORAH DORNY;

xiii. Bank records, tax records, and other financial records from December 1, 2014, through present, relating to JAMES CLARK or THOMAS PETERS;

xiv. Destruction or concealment of evidence.

b. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

c. Any digital device and data servers, to include the Los Angeles City server, capable of being used to commit or further the Target Offenses, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such Target Offenses, and forensic copies thereof.

d. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

4. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications, work product, or other potentially privileged communications:

Non-Digital Evidence

5. Law enforcement personnel conducting the investigation ("the Investigation Team) may be present at the search, but may not search or review any item prior to it being given to them by

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

the "Privilege Review Team" (previously designated individual(s) not participating in the investigation of the case).

6. The Privilege Review Team will review documents to see whether or not the document appears to contain or refer to communications between an attorney and any person or containing the work product of the attorney ("potentially privileged information"). Those documents not containing or referring to such communications or work product may be turned over to the Investigation Team for review.

7. In consultation with a Privilege Review Team Assistant United States Attorney ("PRTAUSA"), if appropriate, the Privilege Review Team member will then review any document identified as appearing to contain potentially privileged information to confirm that it contains potentially privileged information. If it does not, it may be returned to an Investigation Team member. If a member of the Privilege Review Team confirms that a document contains potentially privileged information, then the member will review only as much of the document as is necessary to determine whether or not the document is within the scope of the warrant. Those documents which contain potentially privileged information but are not within the scope of the warrant will be set aside and will not be subject to further review or seizure absent subsequent authorization. Those documents which contain potentially privileged information and are within the scope of the warrant will be seized and sealed together in an enclosure, the outer portion of which will be marked as containing potentially

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

privileged information. The Privilege Review Team member will also make sure that the locations where the documents containing potentially privileged information were seized have been documented.

8. The seized documents containing potentially privileged information will be delivered to the United States Attorney's Office for further review by a PRTAUSA. If that review reveals that a document does not contain potentially privileged information, or that an exception to the privilege applies, the document may be returned to the Investigation Team. If appropriate based on review of particular documents, the PRTAUSA may apply to the court for a finding with respect to the particular documents that no privilege, or an exception to the privilege, applies.

Digital Evidence

9. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will review only digital device data which has been released by the Privilege Review Team.

10. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

11. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the

digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

12. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

13. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

14. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

15. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

16. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

17. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

18. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

19. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully

search a device because the device or files contained therein is/are encrypted.

20. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

21. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

22. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of: Information associated with accounts identified in Attachment A-2 that is within the possession, custody, or control of Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA	)	Case No. 2:19-MJ-02915

WARRANT PURSUANT TO 18 U.S.C. § 2703

To: Any Authorized Law Enforcement Officer

An application by a federal law enforcement officer requests the production and search of the following data:

See Attachment A-2

The data to be produced and searched, described above, are believed to contain the following:

See Attachment B-2

I find that the affidavit, or any recorded testimony, establishes probable cause to produce and search the data described in Attachment A-2, and to seize the data described in Attachment B-2. Such affidavit is incorporated herein by reference.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE HEREBY COMMANDED to serve this warrant on Google, Inc. at any time within 14 days from the date of its issuance.

GOOGLE, INC. IS HEREBY COMMANDED to produce the information described in Attachment A-2 within 10 calendar days of the date of service of this order. **GOOGLE, INC. IS FURTHER COMMANDED** to comply with the further orders set forth in Attachment B-2, and, pursuant to 18 U.S.C. § 2705(b), shall not notify any person, including the subscriber(s) of the account/s identified in Attachment A-2, of the existence of this warrant.

The officer executing this warrant, or an officer present during the execution, shall prepare an inventory as required by law, and shall promptly return this warrant and the inventory to the United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE FURTHER COMMANDED to perform the search of the data provided by Google, Inc. pursuant to the procedures set forth in Attachment B-2.

Date and time issued: ___7/18/19 3:30 p.m. ___

Patrick J. Walsh

Judge's signature

City and State: _Los Angeles, CA_____

Patrick J. Walsh, U.S. Magistrate Judge

Printed name and title

AUSA: Melissa Mills (213) 894-0627

Return	
Case No: 2:19-MJ-02915	*Date and time warrant served on provider:*
Inventory made in the presence of:	
Inventory of data seized: [Please provide a description of the information produced.]	

Certification
I declare under penalty of perjury that I am an officer involved in the execution of this warrant, and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.
Date: _____ _____ *Executing officer's signature*
_____ *Printed name and title*

ATTACHMENT A-2 [Google]

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the account identified as [redacted] and being used by PAUL BENDER, that is within the possession, custody, or control of Google, Inc., a company that accepts service of legal process at its headquarters located at 1600 Amphitheatre Parkway, Mountain View, California, 94043, regardless of where such information is stored, held, or maintained.

ATTACHMENT B-2 (Google)

ITEMS TO BE SEIZED

I. SEARCH PROCEDURES INCLUDING PRIVILEGE REVIEW PROCEDURE

1. The warrant will be presented to personnel of Microsoft Corporation (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below in Section IV.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.13.a. below), law enforcement agents and/or other individuals assisting law enforcement agents who are not participating in the investigation of the case and who are assigned as the "Privilege Review Team" will review the content records, according to the procedures set forth herein, to determine whether or not any of the content records appears to contain or refer to communications between an attorney, or to contain the work product of an attorney, or between a spouse and any person ("potentially privileged information"). The "Search Team" (law enforcement personnel conducting the investigation

and search and other individuals assisting law enforcement personnel in the search) will review only content records which have been released by the Privilege Review Team. With respect to the non-content information produced by the PROVIDER (see Section II.13.b. below), no privilege review need be performed and the Search Team may review immediately.

5. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for in the content records, to include specific words like names of any identified attorneys or law firms and names of any identified spouses] or their email addresses, and generic words such as "privileged" and "work product". The Privilege Review Team will conduct an initial review of all of the content records by using the privilege key words, and by using search protocols specifically chosen to identify content records containing potentially privileged information. Content records that are not identified by this initial review as potentially privileged may be given to the Search Team.

6. Content records that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Content records determined by this review not to be potentially privileged may be given to the Search Team. Content records determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a Privilege Review Team Assistant United States Attorney ("PRTAUSA"). Content records identified by the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

PRTAUSA after review as not potentially privileged may be given to the Search Team. If, after review, the PRTAUSA determines it to be appropriate, the PRTAUSA may apply to the court for a finding with respect to particular content records that no privilege, or an exception to the privilege, applies. Content records that are the subject of such a finding may be given to the Search Team. Content records identified by the PRTAUSA after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

7. The Search Team will search only the content records that the Privilege Review Team provides to the Search Team at any step listed above in order to locate, extract and seize content records that are within the scope of the search warrant (see Section III below). The Search Team does not have to wait until the entire privilege review is concluded to begin its review for content records within the scope of the search warrant. The Privilege Review Team may also conduct the search for content records within the scope of the search warrant if that is more efficient. The search may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

8. If, while reviewing content records or non-content information, either the Privilege Review Team or the Search Team encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

shall immediately discontinue its search pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

9. The Privilege Review Team and the Search Team will complete the search of non-content information and both stages of the search of the content records discussed herein as soon as is practicable but not to exceed 180 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the records beyond this 180-day period without first obtaining an extension of time order from the Court.

10. Once the Privilege Review Team and the Search Team have completed their review of the non-content information and the content records and the Search Team has created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the Search Team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, neither the Privilege Review Team nor the Search Team will access the data from the sealed original production which fell outside the scope of the items to be seized or was determined to be privileged absent further order of the Court.

11. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant

to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

12. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDER

13. To the extent that the information described in Attachment A is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each TARGET ACCOUNT listed in Attachment A:

a. All contents of all wire and electronic communications associated with the TARGET ACCOUNT, limited to that which occurred on or after January 1, 2015,[2] including:

i. All e-mails, communications, or messages of any kind associated with the TARGET ACCOUNT, including stored or preserved copies of messages sent to and from the account, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information

[2] To the extent it is not reasonably feasible for the PROVIDER to restrict any categories of records based on this date restriction (for example, because a date filter is not available for such data), the PROVIDER shall disclose those records in its possession at the time the warrant is served upon it.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

associated with each e-mail or message, and any related documents or attachments.

ii. All records or other information stored by subscriber(s) of the TARGET ACCOUNT, including address books, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files.

iii. All records pertaining to communications between the PROVIDER and any person regarding the TARGET ACCOUNT, including contacts with support services and records of actions taken.

b. All other records and information, including:

(I) All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), any alternate names, other account names or e-mail addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, **and including any changes made to any subscriber information** or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

information, or types of services used, and including the dates on which such changes occurred, for the TARGET ACCOUNT.

ii. All user connection logs and transactional information of all activity relating to the TARGET ACCOUNT described above in Section II.13.a., including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations, and including specifically the specific product name or service to which the connection was made.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

14. For each TARGET ACCOUNT listed in Attachment A, the search team may seize all information described above in Section II.13.a. that constitutes evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); and 1956 (Money Laundering), namely:

a. Information relating to who created, accessed, or used the TARGET ACCOUNT, including records about their identities and whereabouts.

b. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Litigation or contemplated litigation concerning the LADWP Customer Care and Billing ("CC&B") billing system;

ii. Remediation of the LADWP CC&B system;

iii. Communications involving or related to any party to or counsel for party to *Jones v. City of Los Angeles* ("the *Jones* matter") or *City of Los Angeles v. PricewaterhouseCoopers* ("the *PwC* matter"), or with Superior Court personnel assigned to either matter;

iv. Scope and performance of duties as independent monitor in *Jones* matter;

v. Terms of retention as independent monitor in *Jones* matter, including but not limited to duties, financial compensation, reporting requirements, restrictions on communication with parties or counsel; and negotiations regarding those terms;

vi. Reports prepared or submitted in *Jones* matter;

vii. Financial payments, gifts, services, or other benefits offered or given to or from, or solicited by or from, officials or employees of the City Attorney's Office, other City officials, or any party or counsel to litigation in the *Jones* or *PwC* matters, or staff or family members thereof;

viii. Destruction or concealment of evidence.

c. Bank records, tax records, and other financial records from December 1, 2014, through present.

d. All records and information described above in Section II.13.b.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

IV. PROVIDER PROCEDURES

15. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. The PROVIDER shall send such information to:

[redacted]

16. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

17. IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 2705(b), that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A, of the existence of the warrant, until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date this warrant is signed by the magistrate judge or such later date as may be set by the Court upon application for an extension by the United States. Upon expiration of this order, at least ten business days prior to disclosing the existence of the warrant, the PROVIDER shall notify the filter attorney identified in paragraph 15 above of its intent to so notify.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AO 93 (Rev. 11/13) Search and Seizure Warrant (USAO CDCA Rev. 04/17)

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information associated with items identified in Attachment A-8 that is within the possession, custody, or control of Kiesel Law LLP, 8648 Wilshire Boulevard, Beverly Hills, CA	)	Case No. 2:19-MJ-02917

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-8

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B-8

Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 7/18/19 3:30 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh, U.S. Magistrate Judge
Printed name and title

AUSA: Melissa Mills (213) 894-0627

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:19-MJ-02917	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-8 [Kiesel Law Firm]

PROPERTY TO BE SEARCHED

The premises to be searched is a law firm located at **8648 Wilshire Boulevard, Beverly Hills, California**, which is known as Kiesel Law, LLP ("**Kiesel's Office**") and pictured below.

ATTACHMENT B-8 (Kiesel Law LLP)

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering) (the "Target Offenses"), namely:

a. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Any lawsuit where Kiesel Law LLP (or any predecessor firm owned or operated by PAUL KIESEL) or any of its members, principals, attorneys, or other employee, including but not limited to PAUL KIESEL or THOMAS PETERS, was a party, or counsel to a party, to the lawsuit and had a legal, representational, and/or financial interest in both sides of the lawsuit;

ii. Any lawsuit to which the City, or any City employee, official, or representative, was a party and had a legal, representational, and/or financial interest in both sides of the lawsuit;

iii. Threats to expose litigation practices of Kiesel Law LLP (or any predecessor firm owned or operated by PAUL KIESEL) or its members or employees, or of the City Attorney's Office or employees or officials thereof;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

iv. Negotiations and settlement of complaints by and/or against Julissa Salgueiro;

v. Employment and personnel records, including work history, performance reviews, evaluations, ethical screens, lodged complaints, disciplinary actions, administrative leave, suspension, or dismissal, for THOMAS PETERS or Julissa Salgueiro;

vi. Litigation or contemplated litigation concerning the LADWP Customer Care and Billing ("CC&B") billing system;

vii. Remediation of the CC&B billing system;

viii. Financial payments, gifts, services, or other benefits given to, offered to, or solicited by City employees or officials or their staff or family members;

ix. Destruction or concealment of evidence.

b. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

c. Any digital device and data servers capable of being used to commit or further the Target Offenses, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such Target Offenses, and forensic copies thereof.

d. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

1. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any

privileged attorney-client communications, work product, or other potentially privileged communications:

Non-Digital Evidence

2. Law enforcement personnel conducting the investigation ("the Investigation Team) may be present at the search, but may not search or review any item prior to it being given to them by the "Privilege Review Team" (previously designated individual(s) not participating in the investigation of the case).

3. The Privilege Review Team will review documents to see whether or not the document appears to contain or refer to communications between an attorney and any person or containing the work product of the attorney ("potentially privileged information"). Those documents not containing or referring to such communications or work product may be turned over to the Investigation Team for review.

4. In consultation with a Privilege Review Team Assistant United States Attorney ("PRTAUSA"), if appropriate, the Privilege Review Team member will then review any document identified as appearing to contain potentially privileged information to confirm that it contains potentially privileged information. If it does not, it may be returned to an Investigation Team member. If a member of the Privilege Review Team confirms that a document contains potentially privileged information, then the member will review only as much of the document as is necessary to determine whether or not the document is within the scope of the warrant. Those documents which contain potentially privileged information but are not

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

within the scope of the warrant will be set aside and will not be subject to further review or seizure absent subsequent authorization. Those documents which contain potentially privileged information and are within the scope of the warrant will be seized and sealed together in an enclosure, the outer portion of which will be marked as containing potentially privileged information. The Privilege Review Team member will also make sure that the locations where the documents containing potentially privileged information were seized have been documented.

5. The seized documents containing potentially privileged information will be delivered to the United States Attorney's Office for further review by a PRTAUSA. If that review reveals that a document does not contain potentially privileged information, or that an exception to the privilege applies, the document may be returned to the Investigation Team. If appropriate based on review of particular documents, the PRTAUSA may apply to the court for a finding with respect to the particular documents that no privilege, or an exception to the privilege, applies.

Digital Evidence

6. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will review only digital device data which has been released by the Privilege Review Team.

7. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

8. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

9. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

10. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

11. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, “hidden,” or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

12. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

13. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

14. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

15. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

16. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

17. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

18. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

19. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:19-MJ-02917	Date and time warrant executed: 7/22/2019 9:15am	Copy of warrant and inventory left with: Paul Kiesel

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

See attached

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 7/24/2019

Executing officer's signature

SA Julie Sawyer

Printed name and title

GPO U.S. GOVERNMENT PUBLISHING OFFICE 2015 0-468-495

FD-597 (Rev. 4-13-2015) Page 1 of 1

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property

Case ID: 194B-LA-3082417

On (date) 7/22/2019

item (s) listed below were:
- [x] Collected/Seized
- [ ] Received From
- [ ] Returned To
- [ ] Released To

(Name) KIESEL LAW, LLP

(Street Address) 8648 WILSHIRE BLVD

(City) BEVERLY HILLS, CA 92011

Description of Item (s):

1) -SALGUIERO PERSONNEL FILES
2) - 5 PARADIS CDS
3) - MISC. DOCUMENTS
4) - EMAIL DOCUMENTS
5) - PARADIS DOCUMENTS
6) - SD CARD FROM SERVER

Received By: Paul R. Kiesel (Signature) Received From: (Signature)

Printed Name/Title: Printed Name/Title: SA

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with items identified in Attachment A-5 that is within the possession, custody, or control of Los Angeles Department Water and Power City Attorney Offices, located at 221 N. Figueroa Street, Los Angeles, CA

Case No. 2:19-MJ-02919

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-5

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B-5

Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 7/18/19 3:30 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh, U.S. Magistrate Judge
Printed name and title

AUSA: Melissa Mills (213) 894-0627

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:19-MJ-02919	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-5 [LADWP City Attorney Offices]

PROPERTY TO BE SEARCHED

The premises to be searched are located at **221 N. Figueroa Street, 10th Floor, Los Angeles, California** ("**City Property 10th Floor**") and pictured below. Specifically, the following locations within the **City Property** are to be searched.

1. **Richard Tom's Office (10th floor, in or near Suite 1000)**
2. **Deborah Dorny's Office (10th floor, in or near Suite 1000)**
3. **Eskel Solomon's Office (10th floor, in or near Suite 1000)**

ATTACHMENT B-5 (LADWP City Attorney's Office Detachment)

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering) (the "Target Offenses"), namely:

a. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Los Angeles Department of Water and Power contracts and proposed contracts related to any company owned, operated, or affiliated with PAUL PARADIS, including but not limited to PARADIS LAW GROUP LLC, AVENTADOR UTILITY SOLUTIONS LLC ("AVENTADOR"), ARDENT UTILITY SOLUTIONS LLC ("ARDENT"), and CYBERGYM;

ii. LADWP contracting protocols and processes between January 1, 2015, through the present, including but not limited to any manipulations of contracting processes, and the use of other entities to circumvent the requirement for open-bid contracts;

iii. LADWP use of the Southern California Public Power Authority's ("SCPPA") Request for Proposal ("RFP") process;

iv. Procedures, deliberations, and actions by LADWP, the City Attorney's Office, the City of Los Angeles, or any City employee, official, or representative, regarding proposed or considered debarment of PricewaterhouseCoopers ("PwC");

v. Any lawsuit to which the City, or any City employee, official, or representative, was a party and had a legal, representational, and/or financial interest in both sides of the lawsuit;

vi. For the period from January 1, 2014, through the present, any practices, policies, or protocols for retention of special counsel or other outside counsel to represent the City of Los Angeles in litigation;

vii. Retention of PAUL PARADIS and PAUL KIESEL, or entities related thereto, to represent the City of Los Angeles;

viii. Communications involving or *relating* to any party or to counsel for any party to *Jones v. City of Los Angeles* (the "*Jones* matter") or *City of Los Angeles v. PricewaterhouseCoopers* (the "*PwC* matter");

ix. Litigation or contemplated litigation concerning the LADWP Customer Care and Billing ("CC&B") billing system;

x. Remediation of the CC&B billing system;

xi. Communications with the independent monitor appointed in the *Jones v. City of Los Angeles* litigation, PAUL

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

BENDER, or records relating to the consideration and selection of an independent monitor in that case;

xii. Financial payments, gifts, services, or other benefits given to, offered to, or solicited by City employees or officials or their staff or family members;

xiii. Any business venture in which a City official or employee had a financial interest, including but not limited to AVENTADOR, CYBERGYM, and ARDENT;

xiv. Employment and personnel records, including work history, performance reviews, evaluations, ethical screens, lodged complaints, disciplinary actions, administrative leave, suspension, and dismissal, for RICHARD BROWN, RICHARD TOM, ESKEL SOLOMON, or DEBORAH DORNY;

xv. Any physical security or cybersecurity issues, risks, or threats identified at LADWP, including any communications or presentations to LADWP employees, LADWP Board members, or Los Angeles City Council members;

xvi. For the period from June 1, 2008, through the present, any physical security or cybersecurity assessments or surveys performed for or at LADWP, from June 1, 2008, to the present, whether by ARDENT, AVENTADOR, [redacted] or any other cybersecurity vendor;

xvii. Any cybersecurity or physical security risk management, mitigation or remediation relating to cybersecurity or physical security issues identified at LADWP after June 1, 2008;

xviii. For the period from June 1, 2008, through the present, any certifications, reports, statements, or other communications to the Western Electricity Coordinating Council ("WECC"), the North American Electric Reliability Corporation ("NERC"), or the Federal Energy Regulatory Commission ("FERC") regarding compliance or failure to comply with NERC Critical Infrastructure Protection ("NERC-CIP") standards;

xix. Falsification, manipulation, or destruction of records, data, or other information relating to compliance with NERC-CIP standards;

xx. Destruction or concealment of evidence.

b. Bank records, tax records, and other financial records from December 1, 2014, through present, relating to RICHARD BROWN, RICHARD TOM, ESKEL SOLOMON, or DEBORAH DORNY.

c. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

d. Any digital device and data servers, to include the Los Angeles City server, capable of being used to commit or further the Target Offenses, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such Target Offenses, and forensic copies thereof.

e. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

4. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

privileged attorney-client communications, work product, or other potentially privileged communications:

Non-Digital Evidence

5. Law enforcement personnel conducting the investigation ("the Investigation Team) may be present at the search, but may not search or review any item prior to it being given to them by the "Privilege Review Team" (previously designated individual(s) not participating in the investigation of the case).

6. The Privilege Review Team will review documents to see whether or not the document appears to contain or refer to communications between an attorney and any person or containing the work product of the attorney ("potentially privileged information"). Those documents not containing or referring to such communications or work product may be turned over to the Investigation Team for review.

7. In consultation with a Privilege Review Team Assistant United States Attorney ("PRTAUSA"), if appropriate, the Privilege Review Team member will then review any document identified as appearing to contain potentially privileged information to confirm that it contains potentially privileged information. If it does not, it may be returned to an Investigation Team member. If a member of the Privilege Review Team confirms that a document contains potentially privileged information, then the member will review only as much of the document as is necessary to determine whether or not the document is within the scope of the warrant. Those documents which contain potentially privileged information but are not

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

within the scope of the warrant will be set aside and will not be subject to further review or seizure absent subsequent authorization. Those documents which contain potentially privileged information and are within the scope of the warrant will be seized and sealed together in an enclosure, the outer portion of which will be marked as containing potentially privileged information. The Privilege Review Team member will also make sure that the locations where the documents containing potentially privileged information were seized have been documented.

8. The seized documents containing potentially privileged information will be delivered to the United States Attorney's Office for further review by a PRTAUSA. If that review reveals that a document does not contain potentially privileged information, or that an exception to the privilege applies, the document may be returned to the Investigation Team. If appropriate based on review of particular documents, the PRTAUSA may apply to the court for a finding with respect to the particular documents that no privilege, or an exception to the privilege, applies.

Digital Evidence

9. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will review only digital device data which has been released by the Privilege Review Team.

10. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

11. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

12. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

13. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

14. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, “hidden,” or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

15. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

16. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

17. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

18. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

19. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

20. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

21. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

22. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:19-MJ-02919	Date and time warrant executed: 7/22/19 9:25 A.M	Copy of warrant and inventory left with: JOSEPH BRAJENICH, DEBORAH DORNY, ESKEL SOLOMON

Inventory made in the presence of : ALLEN GROVE

Inventory of the property taken and name of any person(s) seized:

SEE ATTACHED

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 7/24/19

Executing officer's signature

ALLEN GROVE, FBI SPECIAL AGENT

Printed name and title

FD-886 (Rev. 4-13-15)

EVIDENCE COLLECTED ITEM LOG

Print Legibly. More than one line may be used for each item, if necessary.

Date: 07/22/19 **Case ID:**

Location: 221 N. Figueroa Street, 10th Floor Los Angeles, CA

Preparer/Assistants: SA Justin Britto

Personnel (full names and initials):

SA Duncan Suh OST
SA MICHAEL TORBIC
OST MIRANDA BAKER

Item #	Description (e.g., One black Samsung flip phone; Serial #)	Location (e.g., Room)	Specific Location (e.g., Specific area w/in room)	Collected by/ Observed by (First Name and Last Name)	Packaging Method	Comments (if needed)
001	PWC Documents, Emails	ROOM F	On Computer desk by Monitor	SA DUNCAN SUH SA MICHAEL TORBIC	PLASTIC BAG	
002	James Clark Deposition	ROOM F	ON Floor by Computer desk	SA DUNCAN SUH SA MICHAEL TORBIC	PLASTIC BAG	
003	MISC. DOCUMENTS RELATING TO PWC SUIT	Room F	STACKED IN CORNER - RIGHT SIDE OF OPEN SHELVES	SA DUNCAN SUH SA MICHAEL TORBIC	Cardboard Box	
004	MISC. DOCUMENTS RELATING TO PWC SUIT	Room F	STACKED IN CORNER - RIGHT SIDE OF OPEN SHELVES	SA DUNCAN SUH SA MICHAEL TORBIC	CARDBOARD BOX	
005	MISC. DOCUMENTS RELATING TO PWC SUIT	Room F	STACKED IN CORNER - RIGHT SIDE OF OPEN SHELVES	SA MICHAEL TORBIC SA DUNCAN SUH	CARDBOARD BOX	
006	MISC. DOCUMENTS RELATING TO PWC SUIT	ROOM F	STACKED IN CORNER ON TOP OF BANKERS BOXES - RIGHT SIDE OF OPEN SHELVES	SA MICHAEL TORBIC SA DUNCAN SUH	CARDBOARD BOX	
007	MISC. DOCUMENTS RELATING TO ~~PWC~~ LAW SUIT & OUTSIDE EMPLOYMENT	ROOM F	INSIDE OR ON OPEN SHELVES / LOWER CABINETS	SA MICHAEL TORBIC SA DUNCAN SUH	PLASTIC BAG	
008	MISC. DOCUMENTS RELATING TO PWC SUIT	ROOM F	ON ROUND TABLE OR ON FLOOR NEAR TABLE	SA MICHAEL TORBIC SA DUNCAN SUH	PLASTIC BAG	
009	ONE BLACK THINPAD (LENOVO) ~~EMPLOYMENT~~ COLLECTION KIT ESTIB 1093	ROOM F	ON OFFICE DESK - BACK DESK	SA MICHAEL TORBIC SA DUNCAN SUH	PLASTIC BAG	

FD-886 (Rev. 4-13-15)

EVIDENCE COLLECTED ITEM LOG

Print Legibly. More than one line may be used for each item, if necessary.

Date: 07/22/19 **Case ID:**

Location: 221 N. Figueroa Street, 9th/10th Floor Los Angeles, CA –

Preparer/Assistants: SA Justin Britto

Personnel (full names and initials):

SA Mark Coleman
SA Pamela Schwartz
SA Amir Sharif

Item #	Description (e.g., One black Samsung flip phone; Serial #)	Location (e.g., Room)	Specific Location (e.g., Specific area w/in room)	Collected by/ Observed by (First Name and Last Name)	Packaging Method	Comments (if needed)
010	(1) hp Z220 Desktop S/N 2UA3260RDB/LADWP# DWP20041731	Room F	Under Desk below monitor	SA Van Nimitsila SA Michael Torbil	Cardboard Box	
011	LADWP CHAIN OF CUSTODY LOGS LA v. PWC; JONES V. LA, Macias v. LA, Photos of Servers; Litigation Drafts Jones v. LA, claims related to CC&B billing, Jones v. City of LA Declaration Filings.	ROOM D	Desk Drawer – under window	SA Mark Coleman SA Amir Sharif	CARDBOARD Box	
012	LA DWP/Aventador purchase order dated 06/06/2017 • LADWP/Wipro LLC CB/CC&B Agreement; LADWP/PWC CIS Agreement (2011); DWP Performance based Rates (2015); DWP CIS Remediation w/ Paradise Law	Room D	Filing Cabinet near Entry Door	SA Mark Coleman SA Amir Sharif	Paper Bag	
013	LADWC v. PWC Deposition, communications, complaints, court records and attorney/client agreement inside black 3" binder; (4) accordion file folders w/ court records, Cisco interface function design man. progress reports & other doc.	Room D.	Under Desk Near Window	SA Amir Sharif SA Pamela Schwartz	Cardboard Box	
014	Filebox - PWC Materials Jan-Mar 2015 & April 2015; Email From Paridise re: not billing accountiand Jones v. City of LA filing (Nov 2016)	Room D.	Under Desk Near Window	SA Mark Coleman SA Amir Sharif	Cardboard Box	
015	-FINANCIALS Involving Paradis Law Group Emails vendor; court docs. Maciasand Jones.	Room C	First (2) File Cabinets in middle row (Facing door)	SA Mark Coleman SA Duncan ~~Sth~~ Suh	Cardboard Box	
016	Case Doc. of Morsel; Macias, Jones	Room C	First (2) File Cabinets in middle row (Facing Door)	SA Mark Coleman SA Duncan ~~Sth~~ Suh	Cardboard Box	
017	Hof Docs LA v. PWC., Jones v. LA; CC&B Matter; Macias v. LA.	Room C	First (2) File Cabinets in middle row (Facing Door)	SA Mark Coleman SA Duncan Suh	Cardboard Box	
018	Misc. Documents found on [illegible]	Room [illegible]	On Desk Near Computer Monitor	SA Kathleen Kennedy SA Pamela Schwartz	Cardboard Box	

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

FD-886 (Rev. 4-13-15)

EVIDENCE COLLECTED ITEM LOG

Print Legibly. More than one line may be used for each item, if necessary.

Date: 07/22/19 **Case ID:**

Location: 221 N. Figueroa Street, 9th Floor Los Angeles, CA

Preparer/Assistants: SA Justin BRITTO

Personnel (full names and initials):

SA Robert Moody SA Michael Torbil

SA Kathleen Kennedy

SA Van Nimitsinpa (CART)

Item #	Description (e.g., One black Samsung flip phone; Serial #)	Location (e.g., Room)	Specific Location (e.g., Specific area w/in room)	Collected by/ Observed by (First Name and Last Name)	Packaging Method	Comments (if needed)
019	(1) Black WD Elements External Hard Drive S/N WX81AB6PISS3	Room B	On Desk near Computer Monitor	SA Kathleen Kennedy SA Robert Moody	Plastic Bag	
020	Documents containing documents Regarding PWC Suit	Room B	Stacked on Floor in (NE) Corner	SA MICHAEL TORBIL SA Pamela Schwartz	CARDBOARD BOX	
021	Documents containing documents Regarding PWC Suit	Room B	Stacked on Floor in (NE) Corner	SA MICHAEL TORBIL SA Pamela Schwartz	Cardboard Box	
022	~~Misc. Documents found on Computer Desk~~	~~Room B~~	~~On Desk Near Computer Monitor~~	~~SA Kathleen Kennedy SA Pamela Schwartz~~	MS	Duplicate of Item 018
022	(1) Black hp Desktop Computer S/N MXL02400PS DWP20033233 Hp Compact Mini tower	Room D	Under Desk by Window	SA Pamela Schwartz SA Mark Coleman		

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information associated with items identified in Attachment A-6 that is within the possession, custody, or control of Los Angeles Department Water and Power Records Retention Storage Facility, 5848 Miramonte Boulevard, Los Angeles, CA	Case No. 2:19-MJ-02920

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-6

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B-6

Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 7/18/19 3:30 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh, U.S. Magistrate Judge
Printed name and title

AUSA: Melissa Mills (213) 894-0627

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:19-MJ-02920	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-6 [LADWP Records Retention]

PROPERTY TO BE SEARCHED

The premises to be searched is a storage facility located at **5848 Miramonte Boulevard, Los Angeles, California ("LADWP Records Retention")** and pictured below. **LADWP Records Retention** facility is pictured below:

ATTACHMENT B-6 (LADWP Records Retention Facility)

I. ITEMS TO BE SEIZED

1. Evidence of the criminal schemes and evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 666 (Bribery and Kickbacks Concerning Federal Funds), 1341 (Mail Fraud), 1343 (Wire Fraud), 1346 (Deprivation of Honest Services), 1505 (Obstruction of Federal Proceeding), 1510 (Obstruction of Justice), 1951 (Extortion), and 1956 (Money Laundering) (collectively, the "Target Offenses") namely:

a. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Los Angeles Department of Water and Power contracts and proposed contracts related to any company owned, operated, or affiliated with PAUL PARADIS, including but not limited to PARADIS LAW GROUP LLC, AVENTADOR UTILITY SOLUTIONS LLC ("AVENTADOR"), ARDENT UTILITY SOLUTIONS LLC ("ARDENT"), and CYBERGYM;

ii. LADWP contracting protocols and processes, including but not limited to any manipulations of contracting processes, or the use of other entities to circumvent the requirement for open-bid contracts;

iii. Procedures, deliberations, and actions by LADWP, the City Attorney's Office, the City of Los Angeles, or any City employee, official, or representative, regarding proposed or considered debarment of PricewaterhouseCoopers;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

iv. Any business venture in which a City official had a financial interest, including but not limited to AVENTADOR, CYBERGYM, and ARDENT;

v. Any lawsuit to which the City, or any City employee, official, or representative, was a party and had a legal, representational, and/or financial interest in both sides of the lawsuit;

vi. Litigation or contemplated litigation concerning the LADWP Customer Care and Billing ("CC&B") billing system;

vii. Remediation of the CC&B billing system;

viii. Financial payments, gifts, services, or other benefits given to, offered to, or solicited by City employees or officials or their staff or family members;

ix. Official foreign travel by employees or officials of the City of Los Angeles; coordination by the City of Los Angeles with foreign governments or entities between January 1, 2018, through the present; memoranda of understanding or other information-sharing agreements with foreign governments or entities; or witting or unwitting transfer of proprietary or sensitive information belonging or relating to the City of Los Angeles;

x. Any physical security or cybersecurity issues, risks, or threats identified at LADWP, including any communications or presentations to LADWP employees, LADWP Board members, or Los Angeles City Council members;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

xi. Any physical security or cybersecurity assessments or surveys performed for or at LADWP, from June 1, 2008, to the present, whether by ARDENT, AVENTADOR, [redacted] or any other cybersecurity vendor;

xii. Any cybersecurity or physical security risk management, mitigation or remediation relating to cybersecurity or physical security issues identified at LADWP after June 1, 2008;

xiii. Any certifications, reports, statements, or other communications to the Western Electricity Coordinating Council ("WECC"), the North American Electric Reliability Corporation ("NERC"), or the Federal Energy Regulatory Commission ("FERC") regarding compliance or failure to comply with NERC Critical Infrastructure Protection ("NERC-CIP") standards;

xiv. Falsification, manipulation, or destruction of records, data, or other information relating to compliance with NERC-CIP standards;

xv. Destruction or concealment of evidence.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

2. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications, work product, or other potentially privileged communications:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Non-Digital Evidence

3. Law enforcement personnel conducting the investigation ("the Investigation Team) may be present at the search, but may not search or review any item prior to it being given to them by the "Privilege Review Team" (previously designated individual(s) not participating in the investigation of the case).

4. The Privilege Review Team will review documents to see whether or not the document appears to contain or refer to communications between an attorney and any person or containing the work product of the attorney ("potentially privileged information"). Those documents not containing or referring to such communications or work product may be turned over to the Investigation Team for review.

5. In consultation with a Privilege Review Team Assistant United States Attorney ("PRTAUSA"), if appropriate, the Privilege Review Team member will then review any document identified as appearing to contain potentially privileged information to confirm that it contains potentially privileged information. If it does not, it may be returned to an Investigation Team member. If a member of the Privilege Review Team confirms that a document contains potentially privileged information, then the member will review only as much of the document as is necessary to determine whether or not the document is within the scope of the warrant. Those documents which contain potentially privileged information but are not within the scope of the warrant will be set aside and will not be subject to further review or seizure absent subsequent

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

authorization. Those documents which contain potentially privileged information and are within the scope of the warrant will be seized and sealed together in an enclosure, the outer portion of which will be marked as containing potentially privileged information. The Privilege Review Team member will also make sure that the locations where the documents containing potentially privileged information were seized have been documented.

6. The seized documents containing potentially privileged information will be delivered to the United States Attorney's Office for further review by a PRTAUSA. If that review reveals that a document does not contain potentially privileged information, or that an exception to the privilege applies, the document may be returned to the Investigation Team. If appropriate based on review of particular documents, the PRTAUSA may apply to the court for a finding with respect to the particular documents that no privilege, or an exception to the privilege, applies.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:19-MJ-02920	Date and time warrant executed: 7/22/19 9:00AM	Copy of warrant and inventory left with: Angela Tatum

Inventory made in the presence of : Angela Tatum, Records Manager

Inventory of the property taken and name of any person(s) seized:

See attached evidence log.

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 7/22/19

Julianne Mayfield

Executing officer's signature

Julianne Mayfield, Special Agent

Printed name and title

FD-886 (Rev. 4-13-15)

EVIDENCE COLLECTED ITEM LOG

Print Legibly. More than one line may be used for each item, if necessary.

Page 1 of ___

Date: 7/22/19 **Case ID:** LA-3082417

Location: 5846 Miramount Blvd., LA, CA 90001

Preparer/Assistants: ___

Personnel (full names and initials):

Item #	Description (e.g., One black Samsung flip phone; Serial #)	Location (e.g., Room)	Specific Location (e.g., Specific area w/in room)	Collected by/ Observed by (First Name and Last Name)	Packaging Method	Comments (if needed)
1	Compliance records 2010-2013	warehouse	DWP-02 Box Serial 498178	Cara Buchanan Keith Tennyson	Bag	Bag 1 Box 2
2	Contract Record Sheets: Paradis LawGroup, PLLC Cyber Security Contract	Warehouse	DWP Box Serial 505746	Abby Coons Keith Tennyson	Bag	Bag 2 Box 2
3	WECC Compliance violations	Warehouse	DWP Box Serial 510288	Kate Bailey Keith Tennyson	Box	~~Box~~ Item 3 Box 1
4	Cyber Security Agenda & NERC Reliability Standards Compliance	Warehouse	DWP Box Serial 506279	Cara Buchanan Keith Tennyson	Bag	Item 4 Box 2
5	SCPPA, Emerson process mgmt. Contract Records	Warhouse	DWP Box Serial 505741	Young Oh Keith Tennyson	Bag	Item 5 Box 2
6	NOAVS of NERC Reliability Standards.	Warehouse	DWP Box Serial 515222	Abby Coons Keith Tennyson	Bag	Item 6 Box 2
7.	NERC Compliance Issues Federal BLM Land, Aerial maps & hand notes of non compliance	warhouse	DWP Box 513565	Young Oh Keith Tennyson	Bag	Item 7 Box 2
8	Vulnerability Assessment and Penetration testing of Dept-wide IT infrastructure Avantador utility solutions Contract	Warhouse	DWP Box 523 223	Caitlin Bowler Keith Tennyson	Bag	Item 8 Box 2
9	Box 520947 LADWP — Patrice Findley V. whistleblower Privileged	Warehouse	DWP Box 520947	Young Oh Keith Tennyson	Box	Item 9 Box 2

FD-886 (Rev. 4-13-15)

EVIDENCE COLLECTED ITEM LOG

Page ____ of ____

Print Legibly. More than one line may be used for each item, if necessary.

Date: _____ **Case ID:** _____

Location: _____

_____

Preparer/Assistants: _____

Personnel (full names and initials):

Item #	Description (e.g., One black Samsung flip phone; Serial #)	Location (e.g., Room)	Specific Location (e.g., Specific area w/in room)	Collected by/ Observed by (First Name and Last Name)	Packaging Method	Comments (if needed)
10	Contracts records re: NERC Upgrades CCNB System.	Warehouse	DWP Box 523225	Cara Buchanan Keith Tennyson	Bag	Item 10 Box 2
11	Asset Purchase Agreement Action Items and Status for redaction of Exceptions / emails.	Warehouse	DWP Box 515220	Heath Smalley Keith Tennyson	Bag	Item 11 Box 2

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with items identified in Attachment A-4 that is within the possession, custody, or control of Los Angeles Department Water and Power, located at John Ferraro Building, 111 N. Hope Street, Los Angeles, CA

Case No. 2:19-MJ-02922

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-4

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B-4

Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 7/18/19 3:30 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh, U.S. Magistrate Judge
Printed name and title

AUSA: Melissa Mills (213) 894-0627

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:19-MJ-02922	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

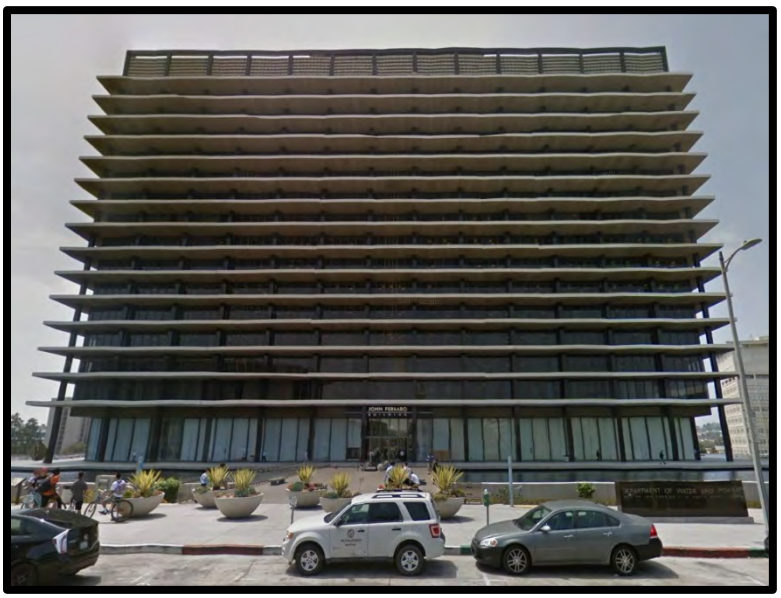
_____
Printed name and title

ATTACHMENT A-4 [Los Angeles Dept. Water and Power]

PROPERTY TO BE SEARCHED

The premises to be searched are located at the John Ferraro Building located at **111 N. Hope Street, Los Angeles, California**, and known as the Los Angeles Department of Water and Power ("LADWP") and pictured below. Specifically, the following locations within LADWP are to be searched:

1. **The Office of the General Manager**
2. **LADWP Commissioner's Offices (Room #1555)**
3. **LADWP Board Office, including work space used by LADWP Board Secretary and LADWP Board Assistants (Room #1555)**
4. **LADWP Board Room (Room #1555-H)**
5. **LADWP Board file storage space outside LADWP Board Room (15th floor)**
6. **Stephen Kwok's Office (Room #1544)**
7. **[redacted]'s Office (Room #1221)**
8. **David Alexander's Office (Room #251)**



ATTACHMENT B-4 (Los Angeles Department of Water and Power)

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 16 U.S.C. §§ 824o, 825o (Knowing and Willful Violation of Electric Reliability Standards) (the "Target Offenses"), namely:

a. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Los Angeles Department of Water and Power contracts and proposed contracts related to any company owned, operated, or affiliated with PAUL PARADIS, including but not limited to PARADIS LAW GROUP LLC, AVENTADOR UTILITY SOLUTIONS LLC ("AVENTADOR"), ARDENT UTILITY SOLUTIONS LLC ("ARDENT"), and CYBERGYM;

ii. LADWP contracting protocols and processes, including but not limited to any manipulations of contracting processes or the use of other entities to circumvent the requirement for open-bid contracts;

iii. LADWP use of the Southern California Public Power Authority's ("SCCPA") Request for Proposal ("RFP") process;

iv. Procedures, deliberations, and actions by LADWP, the City Attorney's Office, the City of Los Angeles, or any City employee, official or representative, regarding proposed or considered debarment of PricewaterhouseCoopers ("PwC");

v. Litigation or contemplated litigation concerning the LADWP Customer Care and Billing ("CC&B") billing system;

vi. Remediation of the LADWP CC&B system;

vii. Financial payments, gifts, services, or other benefits given to, offered to, or solicited by City employees or officials or their staff or family members;

viii. Any business venture in which a City official had a financial interest, including but not limited to AVENTADOR, CYBERGYM, and ARDENT;

ix. Employment and personnel records, including work history, performance reviews, evaluations, ethical screens, lodged complaints, disciplinary actions, administrative leave, suspension, and dismissal, for DAVID WRIGHT, RICHARD BROWN, RICHARD TOM, ESKEL SOLOMON, DEBORAH DORNY, DONNA STEVENER, DAVID ALEXANDER, or STEPHEN KWOK;

x. Official foreign travel by employees, officials, or representatives of LADWP between January 1, 2018, through the present; coordination by LADWP with foreign governments or entities; memoranda of understanding or other information-sharing agreements with foreign governments or entities; or witting or unwitting transfer of proprietary or

sensitive information belonging or relating to LADWP or the City of Los Angeles;

xi. For the period from June 1, 2008, through the present, any physical security or cybersecurity issues, risks, or threats identified at LADWP, including any communications or presentations to LADWP employees, LADWP Board members, or Los Angeles City Council members;

xii. Any physical security or cybersecurity assessments or surveys performed for or at LADWP, from June 1, 2008, to the present, whether by ARDENT, AVENTADOR, [redacted] or any other cybersecurity vendor;

xiii. Any cybersecurity or physical security risk management, mitigation or remediation relating to cybersecurity or physical security issues identified at LADWP after June 1, 2008;

xiv. For the period from June 1, 2008, through the present, any certifications, reports, statements, or other communications to the Western Electricity Coordinating Council ("WECC"), the North American Electric Reliability Corporation ("NERC"), or the Federal Energy Regulatory Commission ("FERC") regarding compliance or failure to comply with NERC Critical Infrastructure Protection ("NERC-CIP") standards;

xv. Falsification, manipulation, or destruction of records, data, or other information relating to compliance with NERC-CIP standards;

xvi. Destruction or concealment of evidence.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. Bank records, tax records, and other financial records from December 1, 2014, through present, relating to DAVID WRIGHT, DAVID ALEXANDER, STEPHEN KWOK, MELTON EDISES LEVINE, or WILLIAM FUNDERBURK.

c. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

d. Any digital device and data servers, to include the Los Angeles City server, capable of being used to commit or further the Target Offenses, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such Target Offenses, and forensic copies thereof.

e. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

4. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications, work product, or other potentially privileged communications:

Non-Digital Evidence

5. Law enforcement personnel conducting the investigation ("the Investigation Team) may be present at the search, but may not search or review any item prior to it being given to them by the "Privilege Review Team" (previously designated individual(s) not participating in the investigation of the case).

6. The Privilege Review Team will review documents to see whether or not the document appears to contain or refer to communications between an attorney and any person or containing the work product of the attorney ("potentially privileged

information"). Those documents not containing or referring to such communications or work product may be turned over to the Investigation Team for review.

7. In consultation with a Privilege Review Team Assistant United States Attorney ("PRTAUSA"), if appropriate, the Privilege Review Team member will then review any document identified as appearing to contain potentially privileged information to confirm that it contains potentially privileged information. If it does not, it may be returned to an Investigation Team member. If a member of the Privilege Review Team confirms that a document contains potentially privileged information, then the member will review only as much of the document as is necessary to determine whether or not the document is within the scope of the warrant. Those documents which contain potentially privileged information but are not within the scope of the warrant will be set aside and will not be subject to further review or seizure absent subsequent authorization. Those documents which contain potentially privileged information and are within the scope of the warrant will be seized and sealed together in an enclosure, the outer portion of which will be marked as containing potentially privileged information. The Privilege Review Team member will also make sure that the locations where the documents containing potentially privileged information were seized have been documented.

8. The seized documents containing potentially privileged information will be delivered to the United States Attorney's

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Office for further review by a PRTAUSA. If that review reveals that a document does not contain potentially privileged information, or that an exception to the privilege applies, the document may be returned to the Investigation Team. If appropriate based on review of particular documents, the PRTAUSA may apply to the court for a finding with respect to the particular documents that no privilege, or an exception to the privilege, applies.

Digital Evidence

9. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will review only digital device data which has been released by the Privilege Review Team.

10. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

11. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

12. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

13. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

14. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

15. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

16. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

17. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

18. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

19. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

20. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

21. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

22. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:19-MJ-02922	Date and time warrant executed: 07/22/2019, 9:20am	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

See Attached

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 07/24/2019

Diamond Outlaw
Executing officer's signature

Diamond Outlaw, Special Agent
Printed name and title

FD-886 (Rev. 4-13-15)

EVIDENCE COLLECTED ITEM LOG

Print Legibly. More than one line may be used for each item, if necessary.

Date: 7/22/2019 **Case ID:** 194B-LA-3882417

Location: 111 N Hope Street Room 251 Los Angeles, CA

Preparer/Assistants:

Personnel (full names and initials): Diamond Outlaw (DO), Travis Bouchard (TB) David Beams (DB) Lindsay Zimmerman (LZ) Alexandra Pham (AP) Ashley Horne (AH) Matthew Bozin (MB) Janine Li (JL) Ryne Intlekofer (RI)

Item #	Description (e.g., One black Samsung flip phone; Serial #)	Location (e.g., Room)	Specific Location (e.g., Specific area w/in room)	Collected by/ Observed by (First Name and Last Name)	Packaging Method	Comments (if needed)
1	Documents from desk, one box	Desk Room 251	Desk in David Alexander's office	Diamond Outlaw Matt Bozin	Cardboard box	
2	One gray/silver Motorola flip phone (Cingular)	Room 251 David Alexander's office	Desk	Diamond Outlaw Matt Bozin	plastic bag	
3	One black/silver motorola flip phone (Verizon)	"	" Desk	Diamond Outlaw Matt Bozin	plastic bag	
4	One blue Siemens phone	"	"	Diamond Outlaw Matt Bozin	plastic bag	
5	One silver 8 GB ipod Serial # CCQFVWMWDCS7	"	"	Diamond Outlaw Matt Bozin	plastic bag	
6	One silver 8GB ipod serial # 9C908SXL2B1	~~Room 251~~	~~David Alexander~~ LZ David Alexander office desk	Diamond Outlaw Matt Bozin	plastic bag	
7	One silver 16 GB ipad OK AP Serial # J3832CWSZ38	Room 251 KS	David Alexander AP office desk	Diamond Outlaw AP Matt Bozin	plastic bag	AP
8	One gold iphone Blue/Black case	on person	on David Alexander	Diamond Outlaw ~~Ryne~~ AP Intlekofer	plastic bag	
9	Black iphone black Speck case	on person	on David Alexander	Diamond Outlaw Ryne Intlekofer	plastic bag	

OK as to 7

FD-886 (Rev. 4-13-15)

EVIDENCE COLLECTED ITEM LOG

Print Legibly. More than one line may be used for each item, if necessary.

Date: 7/22/2019 **Case ID:** 194B-LA-3082417

Location: 111 N Hope Street Room 251 Los Angeles, CA

Preparer/Assistants:

Personnel (full names and initials):

Diamond Outlaw (DO), Travis Bouchard (TB), David Baarns (DB), Lindsey Zimmerman (LZ), Alexandria Pharm (AP), Ashley Horne (AH), Matthew Botzin (MB), Janine Li (JL), Ryne Intlekofer (RI)

Item #	Description (e.g., One black Samsung flip phone; Serial #)	Location (e.g., Room)	Specific Location (e.g., Specific area w/in room)	Collected by/ Observed by (First Name and Last Name)	Packaging Method	Comments (if needed)
10	Cryptex USB Flash-Drive	Desk Room 251	David Alexander's Office Desk	Ashley Horne Diamond Outlaw	Plastic bag	
11	SanDisk USB 3.0 64 GB BN1512246878	Desk Room 251	David Alexander's Office Desk	Janine Li Diamond Outlaw	Plastic bag	
12	Aegis secure key USB 16 GB 1208001748	"	"	Janine Li Diamond Outlaw	Plastic Bag	
13	IBM USB 2G 20120614-AT	"	"	Janine Li Diamond Outlaw	Plastic Bag	
14	USB 02245862 Powered by Yubico	"	"	Janine Li Diamond Outlaw	Plastic Bag	
15	USB Hynix HY27UT088G2M	"	"	Janine Li Diamond Outlaw	Plastic Bag	
16	Blue/ External hard drive Silver NA7RG30S	"	"	Janine Li Diamond Outlaw	Plastic Bag	
17	Black external hard drive WXC1A61F9743	"	"	Janine Li Diamond Outlaw	Plastic Bag	
18	Documents from [illegible]	Filing Cabinet Rm 251	Filing Cabinet Rm 251	Ashley Horne Diamond Outlaw	Brown Bag	

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

FD-886 (Rev. 4-13-15)

EVIDENCE COLLECTED ITEM LOG

Print Legibly. More than one line may be used for each item, if necessary.

Date: 7/22/19 **Case ID:** 194B-LA-3092417

Location: 111 N Hope St. Room 251 Los Angeles, CA

Preparer/Assistants:

Personnel (full names and initials): Diamond Ovlaw (DO), Travis Buchard (TB), David Baarns (DB), Lindsay Zimmerman (LZ), Alexandria Pham (AP), Matthew Bozin (MB) Tarntli (JL) Ryne Illickofer (RI)

Item #	Description *(e.g., One black Samsung flip phone; Serial #)*	Location *(e.g., Room)*	Specific Location *(e.g., Specific area w/in room)*	Collected by/ Observed by *(First Name and Last Name)*	Packaging Method	Comments *(if needed)*
19	DVD-R disk "For David Alexander"	DESK Room 251	DESK, David Alexander's office	Diamond Ovlaw / Matt Bozin	Plastic Bag	

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of: Information associated with accounts identified in Attachment A-1 that is within the possession, custody, or control of Microsoft Corporation, One Microsoft Way, Redmond, WA	))))))	Case No. 2:19-MJ-02923

WARRANT PURSUANT TO 18 U.S.C. § 2703

To: Any Authorized Law Enforcement Officer

An application by a federal law enforcement officer requests the production and search of the following data:

See Attachment A-1

The data to be produced and searched, described above, are believed to contain the following:

See Attachment B-1

I find that the affidavit, or any recorded testimony, establishes probable cause to produce and search the data described in Attachment A-1, and to seize the data described in Attachment B-1. Such affidavit is incorporated herein by reference.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE HEREBY COMMANDED to serve this warrant on Microsoft Corporation at any time within 14 days from the date of its issuance.

MICROSOFT CORPORATION IS HEREBY COMMANDED to produce the information described in Attachment A-1 within 10 calendar days of the date of service of this order. **MICROSOFT CORPORATION IS FURTHER COMMANDED** to comply with the further orders set forth in Attachment B-1, and, pursuant to 18 U.S.C. § 2705(b), shall not notify any person, including the subscriber(s) of the account/s identified in Attachment A-1, of the existence of this warrant.

The officer executing this warrant, or an officer present during the execution, shall prepare an inventory as required by law, and shall promptly return this warrant and the inventory to the United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE FURTHER COMMANDED to perform the search of the data provided by Microsoft Corporation pursuant to the procedures set forth in Attachment B-1.

Date and time issued: 7/18/19 3:30 p.m.

Patrick J. Walsh

Judge's signature

City and State: Los Angeles, CA

Patrick J. Walsh, U.S. Magistrate Judge

Printed name and title

AUSA: Melissa Mills (213) 894-0627

Return	
Case No: 2:19-MJ-02923	*Date and time warrant served on provider:*
Inventory made in the presence of:	
Inventory of data seized: [Please provide a description of the information produced.]	

Certification
I declare under penalty of perjury that I am an officer involved in the execution of this warrant, and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.
Date: _____ _____ *Executing officer's signature*
_____ *Printed name and title*

ATTACHMENT A-1 [Microsoft]

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the accounts identified below that are within the possession, custody, or control of Microsoft Corporation, a company that accepts service of legal process at its headquarters located at One Microsoft Way, Redmond, Washington, 98052-6399, regardless of where such information is stored, held, or maintained.

1. **james.p.clark@lacity.org;**
2. **thom.peters@lacity.org;**
3. **david.wright@ladwp.com;**
4. **marcie.Edwards@ladwp.com;**
5. **donna.stevener@ladwp.com;**
6. **richard.brown@ladwp.com;**
7. **richard.tom@ladwp.com;**
8. **eskel.solomon@ladwp.com;**
9. **deborah.dorny@ladwp.com;**
10. **david.alexander@ladwp.com;**
11. [redacted]
12. **stephen.kwok@ladwp.com;**
13. [redacted]
14. **mel.levine@ladwp.com;**
15. **william.funderburk@ladwp.com;**
16. [redacted];
17. **kiesel@kiesellaw.com;**
18. [redacted].

ATTACHMENT B-1 (Microsoft)

ITEMS TO BE SEIZED

I. SEARCH PROCEDURES INCLUDING PRIVILEGE REVIEW PROCEDURE

1. The warrant will be presented to personnel of Microsoft Corporation (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below in Section IV.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.13.a. below), law enforcement agents and/or other individuals assisting law enforcement agents who are not participating in the investigation of the case and who are assigned as the "Privilege Review Team" will review the content records, according to the procedures set forth herein, to determine whether or not any of the content records appears to contain or refer to communications between an attorney, or to contain the work product of an attorney, or between a spouse and any person ("potentially privileged information"). The "Search Team" (law enforcement personnel conducting the investigation

and search and other individuals assisting law enforcement personnel in the search) will review only content records which have been released by the Privilege Review Team. With respect to the non-content information produced by the PROVIDER (see Section II.13.b. below), no privilege review need be performed and the Search Team may review immediately.

5. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for in the content records, to include specific words like names of any identified attorneys or law firms and names of any identified spouses] or their email addresses, and generic words such as "privileged" and "work product". The Privilege Review Team will conduct an initial review of all of the content records by using the privilege key words, and by using search protocols specifically chosen to identify content records containing potentially privileged information. Content records that are not identified by this initial review as potentially privileged may be given to the Search Team.

6. Content records that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Content records determined by this review not to be potentially privileged may be given to the Search Team. Content records determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a Privilege Review Team Assistant United States Attorney ("PRTAUSA"). Content records identified by the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

PRTAUSA after review as not potentially privileged may be given to the Search Team. If, after review, the PRTAUSA determines it to be appropriate, the PRTAUSA may apply to the court for a finding with respect to particular content records that no privilege, or an exception to the privilege, applies. Content records that are the subject of such a finding may be given to the Search Team. Content records identified by the PRTAUSA after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

7. The Search Team will search only the content records that the Privilege Review Team provides to the Search Team at any step listed above in order to locate, extract and seize content records that are within the scope of the search warrant (see Section III below). The Search Team does not have to wait until the entire privilege review is concluded to begin its review for content records within the scope of the search warrant. The Privilege Review Team may also conduct the search for content records within the scope of the search warrant if that is more efficient. The search may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

8. If, while reviewing content records or non-content information, either the Privilege Review Team or the Search Team encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

shall immediately discontinue its search pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

9. The Privilege Review Team and the Search Team will complete the search of non-content information and both stages of the search of the content records discussed herein as soon as is practicable but not to exceed 180 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the records beyond this 180-day period without first obtaining an extension of time order from the Court.

10. Once the Privilege Review Team and the Search Team have completed their review of the non-content information and the content records and the Search Team has created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the Search Team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, neither the Privilege Review Team nor the Search Team will access the data from the sealed original production which fell outside the scope of the items to be seized or was determined to be privileged absent further order of the Court.

11. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant

to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

12. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDER

13. To the extent that the information described in Attachment A-1 is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each TARGET ACCOUNT listed in Attachment A:

a. All contents of all wire and electronic communications associated with the TARGET ACCOUNT, limited to that which occurred on or after December 1, 2014,[1] including:

i. All e-mails, communications, or messages of any kind associated with the TARGET ACCOUNT, including stored or preserved copies of messages sent to and from the account, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information

[1] To the extent it is not reasonably feasible for the PROVIDER to restrict any categories of records based on this date restriction (for example, because a date filter is not available for such data), the PROVIDER shall disclose those records in its possession at the time the warrant is served upon it.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

associated with each e-mail or message, and any related documents or attachments.

ii. All records or other information stored by subscriber(s) of the TARGET ACCOUNT, including address books, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files.

iii. All records pertaining to communications between the PROVIDER and any person regarding the TARGET ACCOUNT, including contacts with support services and records of actions taken.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), any alternate names, other account names or e-mail addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, **and including any changes made to any subscriber information** or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

services used, and including the dates on which such changes occurred, for the following accounts:

(I) the TARGET ACCOUNT.

ii. All user connection logs and transactional information of all activity relating to the TARGET ACCOUNT described above in Section II.13.a., including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations, and including specifically the specific product name or service to which the connection was made.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

14. For each TARGET ACCOUNT listed in Attachment A, the search team may seize all information described above in Section II.13.a. that constitutes evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 16 U.S.C. §§ 824o, 825o (Knowing and Willful Violation of Electric Reliability Standards), namely:

a. Information relating to who created, accessed, or used the TARGET ACCOUNT, including records about their identities and whereabouts.

b. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Los Angeles Department of Water and Power ("LADWP") contracts and proposed contracts related to any company owned, operated, or affiliated with PAUL PARADIS, including but not limited to PARADIS LAW GROUP LLC, AVENTADOR UTILITY SOLUTIONS LLC ("AVENTADOR"), ARDENT UTILITY SOLUTIONS LLC ("ARDENT"), and CYBERGYM;

ii. LADWP contracting protocols and processes from January 1, 2015, through the present, including but not limited to any manipulations of contracting processes, and the use of other entities to circumvent the requirement for open-bid contracts;

iii. LADWP use of the Southern California Public Power Authority's ("SCPPA") Request for Proposal ("RFP") process;

iv. Procedures, deliberations, and actions by LADWP, the City Attorney's Office, the City of Los Angeles, or any City employee, representative, or official, regarding proposed or considered debarment of PricewaterhouseCoopers ("PwC");

v. Any lawsuit to which the City, or any City employee, official, or representative was a party and had a legal, representational, and/or financial interest in both sides of the lawsuit;

vi. For the period from January 1, 2014, through the present, any practices, policies, or protocols in effect for retention of special counsel or other outside counsel to represent the City of Los Angeles;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

vii. Retention of PAUL PARADIS and PAUL KIESEL, or entities related thereto, to represent the City of Los Angeles;

viii. Communications involving or relating to any party to, or to counsel for any party to, *Jones v. City of Los Angeles* (the "*Jones* matter") or *City of Los Angeles v. PricewaterhouseCoopers* (the "*PwC* matter");

ix. Litigation or contemplated litigation concerning the LADWP Customer Care and Billing ("CC&B") system;

x. Remediation of the LADWP CC&B system;

xi. Communications with the independent monitor appointed in the *Jones v. City of Los Angeles* litigation, PAUL BENDER, or records relating to the consideration and selection of an independent monitor in that case;

xii. Financial payments, gifts, services, or other benefits given to, offered to, or solicited by City employees or officials or their staff or family members;

xiii. Any business venture in which a City official, employee, or representative had a financial interest, including but not limited to AVENTADOR, ARDENT, and CYBERGYM;

xiv. Official foreign travel by officials or employees of the City of Los Angeles between January 1, 2018, through the present, coordination by officials or employees of the City of Los Angeles with foreign governments or enterprises, memoranda of understanding or other information-sharing agreements involving the City of Los Angeles and foreign entities; or witting or unwitting transfer of proprietary or

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

sensitive information belonging or relating to the City of Los Angeles;

xv. From June 1, 2008, through the present, any physical security or cybersecurity issues, risks, or threats identified at LADWP, including any communications or presentations to LADWP employees, LADWP Board members, or Los Angeles City Council members;

xvi. Any physical security or cybersecurity assessments or surveys performed for or at LADWP, from June 1, 2008, to the present, whether by ARDENT, AVENTADOR, [redacted] or any other cybersecurity vendor;

xvii. Any cybersecurity or physical security risk management, mitigation or remediation relating to cybersecurity or physical security issues identified at LADWP after June 1, 2008;

xviii. From June 1, 2008, through the present, any certifications, reports, statements, or other communications to the Western Electricity Coordinating Council ("WECC"), the North American Electric Reliability Corporation ("NERC"), or the Federal Energy Regulatory Commission ("FERC") regarding compliance or failure to comply with NERC Critical Infrastructure Protection ("NERC-CIP") standards;

xix. Falsification, manipulation, or destruction of records, data, or other information relating to compliance with NERC-CIP standards;

xx. Destruction or concealment of evidence.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

c. Bank records, tax records, and other financial records from December 1, 2014, through present, relating to JAMES CLARK, THOMAS PETERS, DAVID WRIGHT, RICHARD BROWN, RICHARD TOM, ESKEL SOLOMON, DEBORAH DORNY, DAVID ALEXANDER, STEPHEN KWOK, MELTON EDISES LEVINE, WILLIAM FUNDERBURK, or PAUL BENDER.

d. All records and information described above in Section II.13.b.

IV. PROVIDER PROCEDURES

15. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. The PROVIDER shall send such information to:

[redacted]

16. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

17. IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 2705(b), that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A, of the existence of the warrant, until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date this warrant is signed by the magistrate judge or such later date as may be set by the Court upon application for an extension by the United States.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Upon expiration of this order, at least ten business days prior to disclosing the existence of the warrant, the PROVIDER shall notify the filter attorney identified in paragraph 15 above of its intent to so notify.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

UNITED STATES DISTRICT COURT

for the

Central District of California

ORIGINAL

CLERK U.S. DISTRICT COURT
JUL 25 2019
CENTRAL DISTRICT OF CALIFORNIA
BY

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
[redacted] Walnut, California

Case No. 2:19-MJ-03045

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 666	Bribery and Kickbacks Concerning Federal Funds
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1505	Obstructing Federal Proceeding
18 U.S.C. § 1510	Obstruction of Justice
16 U.S.C. §§ 824o & 825o	Reliability Standards

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Andrew Civetti, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 7/25/2019

Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh, U.S. Magistrate Judge
Printed name and title

AUSA: Melissa Mills (213) 894-0627

ATTACHMENT A

PROPERTY TO BE SEARCHED

The premises to be searched is located at [redacted], Walnut, California, believed to be the residence of DAVID ALEXANDER ("**ALEXANDER's RESIDENCE**") and pictured below. The residence is a detached four bedroom three bathroom single family home. On the front curb of the residence is painted [redacted]" in black paint on a white background. The numbers "[redacted] are also above the double wide front door.

[redacted]

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1343 (Wire Fraud); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); and 16 U.S.C. §§ 824o, 825o (Knowing and Willful Violation of Electric Reliability Standards) (the "Target Offenses"), namely:

a. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Los Angeles Department of Water and Power ("LADWP") contracts and proposed contracts related to any company owned, operated, or affiliated with PAUL PARADIS, including but not limited to PARADIS LAW GROUP LLC, AVENTADOR UTILITY SOLUTIONS LLC ("AVENTADOR"), ARDENT UTILITY SOLUTIONS LLC ("ARDENT"), and CYBERGYM;

ii. LADWP contracting protocols and processes, including but not limited to any manipulations of contracting processes or the use of other entities to circumvent the requirement for open-bid contracts;

iii. LADWP use of the Southern California Public Power Authority's ("SCCPA") Request for Proposal ("RFP") process;

iv. Financial payments, gifts, services, or other benefits given to, offered to, or solicited by City employees or officials or their staff or family members;

v. Any business venture in which a City official had a financial interest, including but not limited to AVENTADOR and ARDENT;

vi. For the period from June 1, 2008, through the present, any physical security or cybersecurity issues, risks, or threats identified at LADWP, including any communications or presentations to LADWP employees, LADWP Board members, or Los Angeles City Council members;

vii. Any physical security or cybersecurity assessments or surveys performed for or at LADWP, from June 1, 2008, to the present, whether by ARDENT, AVENTADOR, [redacted] or any other cybersecurity vendor;

viii. Any cybersecurity or physical security risk management, mitigation or remediation relating to cybersecurity or physical security issues identified at LADWP after June 1, 2008;

ix. For the period from June 1, 2008, through the present, any certifications, reports, statements, or other communications to the Western Electricity Coordinating Council ("WECC"), the North American Electric Reliability Corporation ("NERC"), or the Federal Energy Regulatory Commission ("FERC") regarding compliance or failure to comply with NERC Critical Infrastructure Protection ("NERC-CIP") standards;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

x. Falsification, manipulation, or destruction of records, data, or other information relating to compliance with NERC-CIP standards;

xi. Destruction or concealment of evidence.

b. Bank records, tax records, and other financial records from December 1, 2014, through present, for ALEXANDER.

c. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

d. Any digital device and data servers, to include and personal/private data servers or data servers of the City of Los Angeles or Los Angeles Department of Water and Power, capable of being used to commit or further the criminal schemes and Target Offenses, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such Target Offenses, and forensic copies thereof.

e. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

outside the scope of the items to be seized absent further order of the Court.

5. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

6. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

Table of Contents

I. INTRODUCTION....1

II. PURPOSE OF AFFIDAVIT....3

III. BACKGROUND ON SUBJECTS....4

IV. OTHER RELEVANT ENTITIES....8

V. STATEMENT OF PROBABLE CAUSE....9

A. Alleged Falsification of Regulatory Paperwork by LADWP Employees....9

1. Underreporting and Failure to Report Cybersecurity Issues....9

B. Alleged Circumvention of LADWP's Contracting Process....14

1. Manipulation of the SCPPA Bidding Process....14

2. Continuing Manipulation of the LADWP Bidding Process....18

C. ALEXANDER and PARADIS Established a Quid-pro-quo to Guarantee Approximately $10-15 million to ARDENT from the Cyber Consulting Contract in Exchange for ALEXANDER's Future Employment with ARDENT, ...21

D. Obstruction of Justice by ALEXANDER....28

E. The FBI Interview of ALEXANDER....31

VII. PREMISES INFORMATION....32

VIII. ....TRAINING AND EXPERIENCE ON DIGITAL DEVICES 33

X. AFFIDAVIT NOT ATTACHED TO SEARCH WARRANT....36

XII. CONCLUSION....36

ATTACHMENT A....1

ATTACHMENT B....1

I. ITEMS TO BE SEIZED....1

II. SEARCH PROCEDURE FOR DIGITAL DEVICES....5

AFFIDAVIT

I, Andrew Civetti, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since September 2015. I am currently assigned to a Public Corruption Squad, where I specialize in the investigation of corrupt public officials, including bribery, fraud against the government, extortion, and money laundering. In addition, I have received training in the investigation of public corruption and other white collar crimes.

2. I am currently one of the agents assigned to an investigation of alleged corrupt activities at the Los Angeles Department of Water and Power ("LADWP") and the Los Angeles City Attorney's Office ("City Attorney's Office") by PAUL PARADIS, JACK LANDSKRONER, PAUL KIESEL, DAVID WRIGHT, MELTON EDISES LEVINE, WILLIAM FUNDERBURK, JAMES CLARK, THOMAS PETERS, RICHARD BROWN, RICHARD TOM, ESKEL SOLOMON, DEBORA DORNY, DONNA STEVENER, DAVID ALEXANDER, STEPHEN KWOK, and PAUL BENDER. As discussed in more detail in previous filings,[1] these activities include the following criminal schemes:

a. Collusive litigation practices related to lawsuits involving the City Attorney's Office and LADWP, which

[1] On July 18, 2019, the Honorable Magistrate Judge Patrick Walsh authorized eight search warrants in the instant investigation. The affidavit in support of those warrants is incorporated herein and can be made available to the Court.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

were fueled in at least one instance by a $2.175 million kickback from plaintiff's attorney JACK LANDSKRONER to attorney PAUL PARADIS, a Special Counsel retained by the City Attorney's Office.

b. An $800,000 hush-money payment to a prospective whistleblower by Special Counsels PARADIS and PAUL KIESEL in exchange for silence as to collusive and potentially fraudulent litigation practices involving PARADIS, KIESEL, and THOMAS PETERS, then the Chief of Civil Litigation at the City Attorney's Office.

c. Offering of bribes by PARADIS, and acceptance of those bribes by LADWP General Manager DAVID WRIGHT and then-LADWP Board Vice President WILLIAM FUNDERBURK, in exchange for supporting at least one $30 million no-bid[2] LADWP contract to PARADIS's company.

d. LADWP's pattern and practice of falsifying records required by the Federal Energy Regulatory Commission ("FERC"), with the knowledge and approval of WRIGHT, LADWP Board President MELTON EDISES LEVINE, ALEXANDER, and other LADWP managers and Board members, in order to conceal and avoid responsibility for cybersecurity vulnerabilities related to the

[2] A "no-bid" contract or "sole source contract" is a contract awarded without competitive bidding. Based on my training and experience, a government entity's award of large and lucrative "no bid" contracts can be (but is not always) an indication that improper and possibly illegal deals were made to secure that contract, or that the vendor was selected for reasons beyond its suitability for the job.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

City's power grid, water supply, and other critical infrastructure.

e. Manipulation of LADWP contract processes by WRIGHT, LEVINE, ALEXANDER, other members of LADWP management and the LADWP Board, and members of the City Attorney's Office.

f. Conspiracy and falsification of records by the President of the LADWP Board, other members of the LADWP Board, LADWP managers, and members of the City Attorney's Office, in order to obscure Board business from public scrutiny.

g. Payments to an Israeli broker to facilitate connections with foreign vendors vying for potential LADWP contracts, with the knowledge that the broker would receive kickbacks from foreign vendors who successfully obtained contracts with LADWP.

3. I am aware that the City receives in excess of $10,000 annually in federal funds through various programs.

II. PURPOSE OF AFFIDAVIT

4. I make this affidavit in support of an application for a search warrant to search the premises of [redacted], Walnut, California, believed to be the residence of DAVID ALEXANDER ("**ALEXANDER's RESIDENCE**"). The location to be searched is described in Attachment A.

5. In connection with the investigation into this matter, the requested search warrant seeks authorization to search the above-referenced premise for the items to be seized described in Attachment B that constitute evidence of the criminal schemes and evidence or fruits of violations of 18 U.S.C. §§ 371

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

(Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1343 (Wire Fraud); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); and 16 U.S.C. §§ 824o, 825o (Knowing and Willful Violation of Electric Reliability Standards) (the "Target Offenses"). Attachments A and B are incorporated herein by reference.

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, information obtained from other agents and witnesses, consensually recorded conversations, and information obtained from the prior related search warrants, as detailed further below. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. BACKGROUND ON SUBJECTS[3]

15. Based on my knowledge of the investigation, below is general background on certain subjects. Although this investigation currently has other subjects, this affidavit focuses on the subjects most relevant to the requested search warrant.

[3] Unless otherwise noted, the e-mail communications described throughout this affidavit involved the accounts identified in this section per individual.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

16. PAUL PARADIS is an attorney and partner at Paradis Law Group, PLLC, operating in New York and Los Angeles. In 2015, PARADIS was appointed as Special Counsel for the City in a civil litigation against PricewaterhouseCoopers ("PwC") regarding an alleged faulty billing system, (Superior Court of California, captioned *City of Los Angeles v. PricewaterhouseCoopers*, Case No. BC574690 ("PwC Case")).

17. On March 15, 2019, I initially interviewed PARADIS, in the presence of his attorney, regarding his involvement in the criminal schemes and Target Offenses detailed herein pursuant to a proffer agreement.[4] I have subsequently interviewed PARADIS on numerous occasions.[5] PARADIS has no criminal record and has agreed to assist the government in exchange for favorable consideration in a potential future prosecution of him related to his conduct in this matter. At my direction, PARADIS has conducted multiple consensual recordings with certain subjects,

[4] Under the terms of the proffer sessions discussed herein, the government is allowed to make derivative use of the information provided to it. The government agrees only not to use the information against the provider of the information in the government's case-in-chief against that person, provided the person is entirely truthful in proffer sessions.

[5] Where possible at this early stage of the investigation, I have attempted to corroborate PARADIS's proffer statements with independent evidence. However, these efforts are presently complicated by the fact that many of the relevant communications may implicate attorney-client privilege or attorney work product. The FBI and the U.S. Attorney's Office are working to resolve these issues through a combination of filter reviews, requests for waivers, and on June 26, 2019, a request for a judicial determination on the crime/fraud exception was filed with the Court and remains pending before the Court. On July 24, 2019, a supplemental filing detailing the government's seizures of new potentially privileged information was filed with the Court.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

including WRIGHT, LEVINE, KWOK, and ALEXANDER, in the investigation, some of which are detailed herein.[6]

18. DAVID WRIGHT is the former General Manager of the LADWP. WRIGHT originally joined LADWP in February 2015 as the Senior Assistant General Manager and then became Chief Operating Officer before being appointed as General Manager in September 2016. According to LADWP's website, WRIGHT spearheaded major LADWP initiatives to restore customer trust in the utility, and to create a clean energy future and a sustainable water supply for Los Angeles. On or around July 23, 2019, WRIGHT was terminated.

a. On April 18, 2019, the Honorable Jacqueline Chooljian, United States Magistrate Judge, authorized search warrants for WRIGHT's phone, WRIGHT's laptop, two of WRIGHT's email addresses, and two of WRIGHT's Apple iCloud accounts (collectively, the "April 2019 search warrants"). On June 4, 2019, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized search warrants for two of WRIGHT's residences, WRIGHT's office at LADWP,[7] WRIGHT's cellular phone, and a burner cellular phone that the FBI had surreptitiously provided to WRIGHT; on June 18, 2019, Judge Walsh authorized a subsequent search warrant for WRIGHT's Riverside residence

[6] As of July 23, 2019, PARADIS has conducted at least fifty hours' worth of recordings with numerous relevant persons in the investigation. I received debriefings from PARADIS regarding each of these recordings; however, due to the high volume, I have not yet listened to each part of every recording.

[7] For operational reasons, this warrant was not executed.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

(collectively, the "June 2019 search warrants"). The April 2019 and June 2019 search warrants and their supporting affidavits are incorporated herein by reference, and copies can be made available for the Court.

b. On June 6, 2019, I interviewed WRIGHT after he waived his Miranda rights. I have since interviewed WRIGHT on several occasions, in the presence of his attorney and pursuant to a proffer agreement, regarding his involvement in the criminal schemes and the Target Offenses described herein.

c. WRIGHT has no criminal record and has agreed to assist the government in exchange for favorable consideration in a potential future prosecution of him related to his conduct in this matter. At my direction, WRIGHT has conducted multiple consensual recordings with certain subjects, including LEVINE, in the investigation, some of which are detailed herein.

16. DAVID ALEXANDER was previously the Chief Information Security Officer ("CISO") at LADWP. In approximately March 2019, he was promoted from that position to the Chief Cyber Risk Officer.

a. Based on review of email communications, I know that ALEXANDER used David.Alexander@ladwp.com ("ALEXANDER's LADWP Account") and [redacted] ("ALEXANDER's Personal Email") for relevant communications detailed below.[8]

[8] On July 18, 2019, the Honorable Magistrate Judge Patrick Walsh authorized a search warrant for these accounts. That warrant has been served, but data has not yet been received from the provider.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. Based on my review of DMV records and FBI surveillance, I believe ALEXANDER resides at [redacted], Walnut, California ("**ALEXANDER's RESIDENCE**").

c. On July 24, 2019, I interviewed ALEXANDER regarding his involvement in the criminal schemes and the Target Offenses described herein.

17. STEPHEN KWOK is the current CISO of LADWP.

a. Based on review of email communications, I know that KWOK used Stephen.kwok@ladwp.com ("KWOK's City Account") and [redacted] ("KWOK's Personal Account") for relevant communications detailed below.

IV. OTHER RELEVANT ENTITIES

30. LOS ANGELES DEPARTMENT OF WATER AND POWER ("LADWP") is, according to its website, the nation's largest municipal utility, with a $7.5 billion annual budget for water, power and combined services. LADWP is responsible for a Power System that provides over 26 million megawatt-hours of electricity per year to over 1.5 million electric services, and a Water System that delivers 160 billion gallons of water per year to 681,000 services in the City. LADWP has a workforce of approximately 10,000 employees. As the user, owner, or operator of a bulk-power system, the LADWP is required to follow the reliability standards approved by the Federal Power Commission.

31. AVENTADOR UTILITY SOLUTIONS, LLC ("AVENTADOR") is a cybersecurity company incorporated by PARADIS on or about March 29, 2017. Around March 2019, AVENTADOR was sold at below-market

value to another owner and changed its name to ARDENT CYBER SOLUTIONS, LLC ("ARDENT").

V. STATEMENT OF PROBABLE CAUSE

A. Alleged Falsification of Regulatory Paperwork by LADWP Employees

1. Underreporting and Failure to Report Cybersecurity Issues

32. In June 2017, LADWP awarded a $30 million contract to AVENTADOR for services related to the remediation of LADWP's Customer Care and Billing ("CC&B") system, as required by the terms of the settlement agreement in *Jones v. City*.[9] Within a year after the award of this $30 million single-source contract, which General Manager WRIGHT and Board President LEVINE advertised to the LADWP Board as urgent because it was mandated by the court-ordered settlement agreement, the primary focus of the contract had shifted to cover services related to assessing and improving cybersecurity for the City's power grid and other critical infrastructure.[10]

33. PARADIS alleges that in order to conceal and avoid responsibility for certain cybersecurity vulnerabilities related

[9] As detailed in my affidavit in support of the eight search warrants approved by Judge Walsh on July 18, 2019, *Jones v. City* is a class-action lawsuit that arose out of widespread billing errors resulting from the implementation of a new CC&B system at LADWP.

[10] The information in this section was proffered by PARADIS and has been corroborated in part by: 1) consensually recorded conversations with WRIGHT; 2) separate consensually recorded conversations with an AVENTADOR employee; and 3) an AVENTADOR work plan and other documents reflecting AVENTADOR'S cybersecurity work for the City, which PARADIS provided to the government.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to critical infrastructure, LADWP employees falsified mandatory federal regulatory documents,[11] including by regularly self-reporting minor violations in order to avoid the discovery of much more significant violations, which would carry substantial fines (in some cases, millions of dollars). Based on my interviews with PARADIS and my knowledge of the investigation, including review of recordings on this topic, LADWP management was under the impression that if they self-reported certain violations, federal regulatory agencies would be less likely to inquire into or investigate other possible violations because LADWP would appear to be already policing itself.

34. In separate consensually recorded conversations with both the current and former Chief Information Security Officers for LADWP (STEPHEN KWOK and DAVID ALEXANDER, respectively), PARADIS confirmed both LADWP's pattern of self-reporting of minor violations to conceal far more significant problems and the fact that members of LADWP management (including WRIGHT) and the LADWP Board (including LEVINE and Cynthia McClain-Hill) were aware of the unethical and potentially illegal practice.

35. ALEXANDER also informed PARADIS in a consensually recorded conversation that LADWP falsified paper records to avoid significant fines that might be imposed by NERC and FERC. For example, NERC-CIP standards require, among other things, the

[11] These include documents mandated by the Federal Energy Regulatory Commission ("FERC") under a compliance regime known as "NERC-CIP" (North American Electric Reliability Corporation - Critical Infrastructure Protection).

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

deployment of a patch management process to monitor and address software vulnerabilities, which includes adhering to a security patch evaluation timeline to ensure that all patches are up-to-date. In an April 2019 consensually recorded conversation with PARADIS, ALEXANDER said that a comparison of LADWP's paper records to its computers would show that LADWP claimed it applied patches in a timely fashion when, in fact, it did not. ALEXANDER's proposed solution to the problem, which he disclosed to PARADIS, was to simply dispose of all the old computers evidencing delayed patching, and replace them with new computers that had no evidence of any patching issues.

36. In another consensually recorded conversation between PARADIS and ALEXANDER in May 2019, ALEXANDER told PARADIS that he had asked [redacted], the head of CIP compliance at LADWP, for all the self-reports that LADWP had submitted to NERC. ALEXANDER told PARADIS that after [redacted] emailed a link to ALEXANDER with the relevant documents, ALEXANDER emailed "them" – presumably referring to [redacted]'s group -- to take his permissions away, thereby indicating that ALEXANDER was receiving and sending these emails through ALEXANDER'S LADWP Account. In addition, ALEXANDER told PARADIS he had asked [redacted], LADWP's point of contact for NERC, for additional documents relating to LADWP's NERC compliance.

37. According to PARADIS, LADWP was likely aware of its failure to comply with NERC-CIP standards as early as 2008. Based on a Critical Cyber Asset Vulnerability Assessment Report prepared for LADWP in November 2008, LADWP was informed of a

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

number of weaknesses in its network security, including overly permissive access list statements ("ACLs"), outdated routers and switches, and passwords stored in clear text. In a 2010 NERC Vulnerability Assessment conducted for LADWP by a different vendor, it was determined that insecure ACLs were still an issue, several of the same routers and switches still had vulnerabilities, and weak passwords were cited as an issue of high severity. Additionally, LADWP was cited as having internal network security that was "lax in non-patched and inadequately configured devices, which could either lead to compromise of SCADA data or a denial of service/availability."

38. In a consensually recorded conversation on May 15, 2019, WRIGHT told PARADIS that there had been a report issued 10-15 years ago (referring to the 2010 NERC Vulnerability Assessment) about "how fucked up the IT efforts were at DWP," and that "nothing has been done since then."

39. On May 16, 2019, while in the process of assisting WRIGHT in creating a Power Point presentation regarding the history and oversight of the AVENTADOR contract, PARADIS provided WRIGHT with a written document stating that "LADWP does not have a comprehensive, systematic network security scanning and testing program and LADWP is therefore largely blind to cyber vulnerabilities and insider threats." PARADIS also wrote that 2,409 LADWP computers are "completely unaccounted for and unable to be located."

40. During a consensually recorded meeting between PARADIS and ALEXANDER in May 2019, PARADIS obtained an internal LADWP

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

spreadsheet titled "CIP Self-Report and Issue Tracker" shows that since 2016, 10 of the 16 potential self-reporting incidents involved LADWP's Energy Control Center. But when PARADIS asked WRIGHT during their recorded conversation on May 26, 2019, about allotting funds in the next cybersecurity contract to address the issues at the Energy Control Center, WRIGHT rejected the idea, stating that they needed to avoid doing anything with the Energy Control Center for at least the first 60 days of the contract, so as to avoid the scrutiny of others. As detailed below, PARADIS, WRIGHT, KWOK, and ALEXANDER were actively orchestrating a plan to award ARDENT a new multi-million dollar cybersecurity contract in September 2019 – even before the relevant Request for Proposals ("RFP") was drafted.

41. Notably, when KWOK debriefed PARADIS in a consensually recorded conversation about a meeting he had had in March 2019 with Deputy Mayor "[redacted]", KWOK said that when a question was raised about whether the cybersecurity work at issue was deferrable, KWOK responded, "No, none of this stuff is deferrable. It's critical, unless you want the lights to go off, or the water to go off . . . It could happen any day."[12]

[12] Based on the consensually recorded conversations between PARADIS and KWOK (and summaries thereof) that I have reviewed, it appears that KWOK was the person at LADWP with whom ARDENT interfaced the most regarding their work at the utility.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

B. Alleged Circumvention of LADWP's Contracting Process

1. Manipulation of the SCPPA Bidding Process

42. According to PARADIS, LADWP management and members of the Board (including WRIGHT, LEVINE, and Cynthia McClain-Hill) successfully manipulated LADWP's contracting processes to ensure that AVENTADOR's successor company, ARDENT UTILITY SOLUTIONS, LLC ("ARDENT"),[13] was awarded a lucrative contract to continue AVENTADOR's cybersecurity work without engaging in the required competitive bidding process (the "ARDENT contract"). According to information proffered by PARADIS, LADWP routinely uses the Southern California Public Power Authority ("SCPPA")[14] to circumvent LADWP's standard 12-18 month competitive bidding process, and did so for the ARDENT contract.[15]

43. On January 8, 2019, WRIGHT sent a text message to LEVINE, "Cyber and IT will always need external staff (I think [redacted] – Business Manager, IBEW Local 18][16] already supports this), we are increasing staff everywhere in the department as fast as reasonable. Need to get more supportive on outsourcing as we have hired a net increase of couple thousand

[13] Despite a sham sale in March 2019, PARADIS appears to still effectively control this company.

[14] According to the SCPPA website, SCPPA is "a Joint Powers Authority, created in 1980, for the purpose of providing joint planning, financing, construction, and operation of transmission and generation projects."

[15] According to the SCPPA website, WRIGHT is the Secretary of SCPPA and a current member of the SCPPA Board of Directors.

[16] IBEW Local 18 is a labor union. According to IBEW Local 18's website, Local 18 is an "affiliate of the International Brotherhood of Electrical Workers (IBEW). Although our name says "electrical workers," our members come from hundreds of different job classifications."

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

staff in the last few years. We support greater workforce development but LADWP needs to have a greater role in screening them for base line qualifications."

44. The SCPPA website shows that in February 2019, SCPPA issued a RFP for Cybersecurity Services ("Cyber Services Contract").

45. According to media reports of a statement issued by LADWP, the LADWP Board, on or about March 12, 2019, ordered AVENTADOR's $30 million contract terminated "in order to eliminate any potential conflict or the appearance of a conflict of interest" after allegations that PARADIS improperly represented both Jones and the City in relation to LADWP's overbilling issues.

46. I have seen text messages between WRIGHT, McClain-Hill, and LEVINE from March 14, 2019, in which McClain-Hill asks, "is the contract termination moving forward," to which WRIGHT responds that "the contract was assumed **with PAUL [PARADIS] no longer connected**." McClain-Hill then goes on to say, "The goal was not to simply save the existing contract, but to facilitate payment under the existing contract until we put a new contract in place . . . with AVENTADOR or some other entity." WRIGHT responds, "Yes. That is all in process." And LEVINE says, "All good."

47. On March 14, 2019, LEVINE sent a text message to WRIGHT, "Ok. I need to talk with Dakota [Smith – Los Angeles Times Reporter] again in the next few minutes. Pretty much told her what we are doing to keep the cyber employees. She

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

questioned if that is consistent with board instruction to cancel AVENTADOR contract.[17] Joe [Brajevich – LADWP General Counsel] gave me a good response to that." Based on the context of the communication it appears as though Smith inquired into the retention of City cyber employees and the fate of the AVENTADOR employees post cancellation. The formation of ARDENT, a subsequent awarded contract discussed below, do not appear to me to be consistent with the LADWP Board's demand.

48. On March 26, 2019, WRIGHT sent a text message to LEVINE, "I have to share at some point that [we are] deliberately vague on our public descriptions as we were worried about publicly communicating our specific cyber vulnerabilities. And we discussed this in closed session and in our meetings with other city staff. Will try to mention it in general in the meeting tomorrow morning if it fits into the discussion." LEVINE replied, "Good. Radio silence from Cynthia [McClain-Hill] after calling and emailing."

49. On March 27, 2019, WRIGHT sent a text message to LEVINE, "Check LADWP email. Excellent summary document regarding

[17] According to PARADIS, after his dual role in the *Jones v. City* litigation came under scrutiny as described herein, in order to keep AVENTADOR employees working on the City contract, PARADIS submitted to pressure to sell AVENTADOR and have no part in any subsequent companies that form. PARADIS sold AVENTADOR below market value and has in fact remained an integral part of ARDENT (the new company). Based on consensually recorded conversations, WRIGHT and LEVINE are aware of PARADIS' continued involvement.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

cyber we will discuss at tomorrow's meeting." LEVINE replied, "Can you send it to my other email?"[18]

50. According to the California Secretary of State website, AVENTADOR filed an amendment to change its name to ARDENT on March 29, 2019.

51. On April 1, 2019, in a consensually recorded conversation, KWOK told PARADIS that there was really "**no competition**" for ARDENT as far as the SCPPA selection process (Cyber Services Contract) was concerned, but referred to "political maneuvering" in describing the efforts to get ARDENT another contract with LADWP.

52. On April 5, 2019, in a consensually recorded conversation, LEVINE and McClain-Hill confirmed to PARADIS that ARDENT would be the primary vendor (out of 28 candidates) for the LADWP's Cyber Services Contract, *despite the fact that SCPPA was not scheduled to vote on the contract until a meeting on April 18, 2019* —— almost two weeks later.

53. That same day, in a consensually recorded conversation, ALEXANDER informed PARADIS that he had driven the SCPPA process that resulted in the approval of ARDENT. Specifically, ALEXANDER said LADWP had been told by the Mayor's office that they couldn't give another sole source contract to ARDENT, so LADWP used the SCPPA bidding process to "get to [LADWP's] desired outcome in an apparently completely

[18] Based on my interviews of PARADIS, LEVINE utilized his Gibson Dunn email to conduct City business, not his LADWP email.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

transparent process." In fact, ALEXANDER said, "that was me driving it. That was me and Jim [Compton] texting each other. That was me and Jim conversing with each other on our cell phones."

54. Because ALEXANDER was the Vice-Chair of the SCPPA Cyber Security Working Group, he was able to work with Compton, who was the Chair of the SCPPA Cyber Security Working Group, to get Compton "somebody he wanted," and "[Compton] got me somebody I wanted." According to ALEXANDER, Compton wanted part of the contract to go to Dragos, Inc. The third vendor that ALEXANDER and Compton chose was Archer Energy Solutions, LLC.

55. On April 23, 2019, the LADWP Board approved a 60-day contract of $3,600,000 for ARDENT, Dragos, Inc., and Archer Energy Solutions, LLC.[19]

2. Continuing Manipulation of the LADWP Bidding Process

56. Since at least May 2019, PARADIS has been working with ALEXANDER and KWOK -- at WRIGHT's direction -- on the issuance of another RFP for Cybersecurity Consulting ("Cyber Consulting Contract"). Unlike the Cyber Services Contract, which went through the SCPPA process, the Cyber Consulting Contract was

[19] The Board's action is confirmed in public materials on the LADWP website. According to PARADIS and confirmed in a consensually recorded conversation with WRIGHT on April 21, 2019, the original plan for a larger contract to ARDENT was tabled after the Mayor's office exerted pressure on LADWP to avoid such a large contract with ARDENT due to the potential for negative publicity related to ARDENT, a successive company to AVENTADOR, being awarded another large contract. PARADIS reported that LADWP planned that the majority of the $3.6M 60-day contract would go to ARDENT, and that the contract would thereafter be extended or expanded.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

proceeding through LADWP's own bidding process and – based on communications between PARADIS, WRIGHT, ALEXANDER, and KWOK – appears to be a $82.5 million, three-year contract.

57. On May 21, 2019, in a consensually recorded conversation, PARADIS met with KWOK to discuss the RFP for the Cyber Consulting Contract. Included in the discussion was the evaluation criterion for who would be selected. KWOK told PARADIS that he spoke to ALEXANDER about how they could control the evaluation team to ensure that they could guarantee that those entities they wanted to hire were certain of being selected.

58. On May 24, 2019, KWOK's Personal Account sent PARADIS a timeline for the RFP, which was designed to meet a "Sept 24 timeline" for the recommendation of an award to the LADWP Board. The attached timeline provided that the RFP would be released on June 17, 2019, with the solicitation period ending on July 8, 2019.

59. That same day, PARADIS submitted his redline of the draft RFP to ALEXANDER and KWOK, at WRIGHT's direction. On May 29, 2019, PARADIS sent another version of the RFP to ALEXANDER and KWOK, which he said included all of WRIGHT's comments. In doing so, PARADIS did not communicate with ALEXANDER and KWOK through their email addresses at LADWP, but instead used ALEXANDER's Personal Account, [redacted][20] and KWOK's

[20] Based on consensually recorded conversation described below, ALEXANDER maintained this e-mail account on a private server located at **ALEXANDER's RESIDENCE**.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Personal Account, [redacted]

60. In that same e-mail, PARADIS said WRIGHT had instructed him to inform KWOK and ALEXANDER of the way in which the $82.5 million would be spent over the course of the three years of the contract. This financial breakdown included a $15 million allotment for "Cybersecurity Laboratory Training Services," which – as WRIGHT told PARADIS in a consensually recorded conversation on May 26, 2019 – would be for CYBERGYM.[21] [22]

61. In another email on May 29, 2019, PARADIS emailed ALEXANDER's Personal Account and KWOK's Personal Account to tell them that WRIGHT had decided that he, ALEXANDER, and KWOK would be among the seven people making up the evaluation committee for the RFP.

62. According to the website for the Los Angeles Business Assistance Virtual Network, LADWP issued an RFP for Cybersecurity Consulting Services on June 17, 2019, with a

---

[21] CYBERGYM, according to its website, conducts cyber-warfare readiness training for government and private enterprises. CYBERGYM was an additional venture that PARADIS orchestrated with WRIGHT as an additional benefit to WRIGHT, post-retirement.

[22] On May 26, 2019, WRIGHT stated to PARADIS that LEVINE knew that PARADIS could have, but did not, report LEVINE for having improperly intervened in the debarment process (described in a subsequent section) involving PwC despite being recused, and was appreciative of PARADIS concealing that fact. WRIGHT suggested that PARADIS could use LEVINE as a "front" ownership regarding CYBERGYM.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

deadline of July 10, 2019. According to PARADIS, ARDENT submitted a bid for the contract.

63. I believe this behind-the-scenes manipulation of City contracting processes appears to be consistent with related unethical and/or illegal behavior by LADWP officials designed to circumvent legal and regulatory constraints to benefit favored parties.

C. ALEXANDER and PARADIS Established a Quid-pro-quo to Guarantee Approximately $10-15 million to ARDENT from the Cyber Consulting Contract in Exchange for ALEXANDER's Future Employment with ARDENT[23,24]

64. On July 15, 2019, ALEXANDER sent a text message to PARADIS that said, "Update: Louis [Carr] and Flora [Chang] have been provided with "cliff notes" on my proposal thoughts. They both appreciate the info. It's printed and I asked for them back. I am reaching out." Based on my knowledge of the investigation, I believe the "cliff notes" to be a reference to ALEXANDER supporting ARDENT and possibly providing instruction to Carr and Chang to also support ARDENT. I understand Carr and

---

[23] The recordings described in the section are some of the consensually recorded conversations with ALEXANDER conducted by PARADI or WRIGHT. As previously noted, I have not included every recording between ALEXANDER and PARADIS or WRIGHT.

[24] I have not yet listened to the recordings referenced in this section given the volume of recordings and my other work responsibilities. The information outlined in this section was provided by PARADIS in his debrief to me after PARADIS conducted the consensual recordings. The debriefs included PARADIS' account of the substance of the recording at that time. However, based on my review of other recordings conducted by PARADIS, the debriefs he provided at that time related to those recordings, and other evidence I have obtained in the investigation, PARADIS' debriefs appear to be consistent with the recordings conducted.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Chang were ultimately added to the evaluation committee for the Cyber Consulting Contract RFP described above.

65. On July 16, 2019, in a consensually recorded meeting, PARADIS and ALEXANDER discussed the following:

a. ALEXANDER informed PARADIS that LADWP received fifteen responses to the Cyber Consulting Contract RFP and the purpose was to establish a "bench" of cyber consultants that could be called upon to perform four basic cyber services.

b. LADWP, for the first time to ALEXANDER's knowledge, required that each of the five evaluators of the RFP -- including himself -- sign an agreement that the evaluators would not speak to one another about their scores or grading of the RFP responses.

c. Despite having signed the agreement, ALEXANDER said he prepared a single color-coded grading score sheet that reflected his scores for each of the potential companies and shared the scoring grid with Carr and Chang to influence them to give ARDENT a high score.[25] ALEXANDER said Carr and Chang understood that the goal was to have ARDENT score high enough to be one of the top three scores and be awarded a portion of the contract.

d. ALEXANDER was not concerned with Carr and Chang disclosing ALEXANDER's violation of the signed agreement because Carr and Chang were "playing ball" to help ALEXANDER get ARDENT

[25] Based on the text messages and consensually recorded conversation, I believe ALEXANDER's "cliff notes" to be the color-coded scoring guide provided to Carr and Chang.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

hired.

e. ALEXANDER was working "behind the scenes" to help manage the contracting process through LADWP's Supply Chain Service Department to ensure ARDENT was hired.

f. ALEXANDER stated that he had arranged multi-million dollar contracts to PARADIS so what could PARADIS do for ALEXANDER.

g. PARADIS told ALEXANDER the lunch was to thank ALEXANDER for the help already provided and inquired as to ALEXANDER's future employment plans, given that WRIGHT had announced his retirement. ALEXANDER described three options -- one being the Business and Operations Manager for ARDENT.

h. PARADIS asked what ALEXANDER wanted for a salary, and ALEXANDER said he would think about it and get back to PARADIS. ALEXANDER requested that medical benefits be included. ALEXANDER also requested that part of his payment come in the form of a new car, specifically a Mercedes-Benz AMG S63.[26]

i. ALEXANDER and PARADIS originally agreed that ALEXANDER's start date with ARDENT would be September 1, 2019; however, ALEXANDER stated that it had to be October 1, 2019, because the LADWP Board meeting to approve the three-year contract that was the subject of the discussed Cyber Consulting Contract RFP was going to be voted on by the LADWP Board in late September. ALEXANDER needed to stay on to guide the process

[26] According to Mercedes-Benz's website, the AMG S63 cost approximately $170,000.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

with the LADWP Board to ensure ARDENT was hired.

j. ALEXANDER had long-standing knowledge of the extensive LADWP NERC-CIP violations and fraudulent regulatory reporting. ALEXANDER said that if the FBI ever learned of these facts there would be "serious criminal issues" for a number of officials, including ALEXANDER. ALEXANDER stated that if the FBI found out about these violations, he and several others "would be going to jail."

66. Based on the consensually recorded conversations, my training, experience, and knowledge of the investigation, I believe ALEXANDER was requesting some type of payment for his work on ensuring ARDENT received the Cyber Consulting Contract. Based on PARADIS' understanding, it appeared as though ALEXANDER was suggesting that because he had assisted ARDENT by influencing other evaluators, he should be rewarded with future employment and a new car.

67. After the meeting, the following text messages were exchanged between ALEXANDER and PARADIS:

ALEXANDER:	"Who is your CFO currently?"
PARADIS:	"A guy I have known in NYC for over 12 years. Why are you asking?
ALEXANDER:	"Role and responsibility for my new job. I'm scoping."
PARADIS:	"You wont have any CFO responsibility. Your duties will be what we discussed, namely operations and business management."
ALEXANDER:	"So I am thinking essentially a Chief Administrative Officer…"

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

PARADIS: "I agree completely[.]"

"[Link to Mercedes-Benz AMG S63] Remember what I said about the colors at lunch?"

ALEXANDER: "Yup. So that darker silver it is."

PARADIS: "You don't like the white with red calipers?"

ALEXANDER: "It's sharp, as well. My comfort is in that darker color, but actually would pick completely black last (heat in the car)…"

PARADIS: "Black on Black gets very hot in the sun. No question about it."

"How did your discussion with your wife go? Is she on board for you to start as ARDENT CAO in October?"

ALEXANDER: "We did tal[k]. She seems supportive. She agrees that I need to confirm my retirement and processes to activate it later.

Additionally, I still need to define my role and value to ARDENT.

We (you and I) will discuss more very soon."

PARADIS: "Ball is in your court – I was very blunt and direct with you at lunch.

I think you would be a great addition to the team. You have already been extremely helpful to ARDENT and demonstrated your value numerous times – including most recently with the both the SCPAA RFP and the current LADWP RFP.

I look forward to discussing further with you very soon."

70. On July 17, 2019, the following text messages were exchanged between ALEXANDER and PARADIS:

ALEXANDER: "I understand that and appreciate it. I'm also thinking of ongoing value. :) Remember,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

you asked me to define the future state for me and ARDENT on a new job. ;) Side note: do either WRIGHT or [redacted] know you and I are talking about this? I ask because, as an exec, I owe them notice and off boarding. I dont exactly want to leave them in a major lurch."

"Dude. Just finished my conversation with the retirement group. Not good at all. We need to talk to discuss options, when you have the chance."

PARADIS: "In a meeting right now and cant talk, but I will call you later. When you say "not good at all" what do you mean?"

ALEXANDER: "Thx[.] The loss… I'll explain when we talk[.]"

71. On July 17, 2019, in a consensually recorded meeting, PARADIS and ALEXANDER discussed the following:

a. After the RFP for the Cyber Consulting Contract concluded and the contract was awarded, ALEXANDER could guarantee that ARDENT would be provided a task order for training and another category of cyber consulting.

b. ALEXANDER could not guarantee, but would attempt to influence others, to ensure ARDENT received a task order for a portion of the remediation.

c. Between these various categories, ALEXANDER could guarantee PARADIS approximately $10-15 million for ARDENT. These guarantees were to show ALEXANDER's worth for his future employment with ARDENT.

d. ALEXANDER was concerned that retiring early would

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

affect his pension. PARADIS agreed to make up the difference in addition to ALEXANDER's salary, if ALEXANDER could guarantee the above as described.

e. ALEXANDER requested an ARDENT email address to communicate with PARADIS.[27] PARADIS offered an ARDENT laptop that ALEXANDER agreed to receive.

72. Based on the consensually recorded conversation, the text messages, and my knowledge of the investigation, I believe that ALEXANDER and PARADIS established a quid-pro-quo involving ALEXANDER guaranteeing $10-15 million of the Cyber Consulting Contract in exchange for future employment with ARDENT. It is my understanding that even after an LADWP contract is awarded to a particular company, no payment is actually received by that company unless a task order is assigned to it. So if multiple companies have been awarded a contract from the LADWP, both the work and any payment for that work is divided based on task order. Here, ALEXANDER guaranteed PARADIS that at least $10-15 million of the $82.5 million Cyber Consulting Contract would be awarded to ARDENT.

73. On July 19, 2019, ALEXANDER sent a text message to PARADIS that said, "Do you still plan to bring the equipment [ARDENT laptop] over today?" On or around that same day, in a

[27] I believe that ALEXANDER requested an e-mail address from ARDENT to conceal his communications with PARADIS.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

consensually recorded conversation, ALEXANDER requested that his ARDENT e-mail address be FrankieWalnut@ardent.com because his middle name was "Frankie" and he lived in "Walnut." According to PARADIS, ALEXANDER did not want his actual name associated with the e-mail account.

74. On July 18, 2019, Judge Walsh issued eight search warrants authorizing the government to search 19 email accounts and six premises, including ALEXANDER's office at LADWP. During execution of those search warrants at LADWP on July 22, 2019, ALEXANDER sent a text message to PARADIS that said, "There is a federal search warrant being administered here at DWP. They are in 251, Donna's office and ARDENT work space. Not sure if it includes WRIGHT's office." Based on my training, experience, and knowledge of the investigation, I believe ALEXANDER informed PARADIS of the FBI searches as a "heads up" and as an attempt to discuss the investigation.

D. Obstruction of Justice by ALEXANDER[28]

75. On July 23, 2019, a day after the FBI searches,

[28] I have not yet listened to the recordings referenced in this section given the volume of recordings and my other work responsibilities. The information outlined in this section was provided by WRIGHT and PARADIS in their debriefs to me after they conducted the referenced consensual recordings. The debriefs included WRIGHT's and/or PARADIS' account of the substance of the recording at that time. However, based on my review of other recordings conducted by WRIGHT and/or PARADIS, the debriefs they provided at that time related to those recordings, and other evidence I have obtained in the investigation, WRIGHT's and PARADIS' debriefs appear to be consistent with the recordings conducted.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

ALEXANDER sent a Confide[29] message to WRIGHT. At my direction, WRIGHT did not open this message due to not being able to capture the content without notifying ALEXANDER. ALEXANDER subsequently sent a text message to WRIGHT that said, "If you have a moment, I think we should talk."

76. In two consensually recorded calls, ALEXANDER told WRIGHT that he was "concerned" and "worried" that the FBI had imaged[30] ALEXANDER's phone. ALEXANDER stated that he was "concerned" because of text messages ALEXANDER had had with PARADIS over the past month. ALEXANDER described these messages to involve providing information regarding the SCPPA manipulation and the recent Cyber Consulting Contract RFP and coordinating with PARADIS to favor ARDENT. ALEXANDER was unsure whether PARADIS had a financial interest in ARDENT, but that it was clear that PARADIS was involved with ARDENT's operations and contracts. ALEXANDER stated that he personally did not have any financial arrangement with PARADIS, nor any arrangements for future employment with ARDENT or PARADIS. ALEXENDER told WRIGHT that he also communicated with PARADIS via ALEXANDER's Personal

---

[29] Confide is an encrypted instant messaging application for most major operating systems. It was first released in 2013 on iOS, and is known for its self-destructing messaging system that deletes messages immediately after reading. The platform offers both free and paid features for individuals and businesses.

[30] ALEXANDER's phone was consensually provided during the execution of the search warrant executed at LADWP on July 22, 2019. Due to technical difficulties, however, the FBI was unable to image the phone. I reviewed ALEXANDER's phone on-scene, and photographed relevant information pursuant to Attachment B-4. ALEXANDER's phone was subsequently returned to ALEXANDER that same day.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Account that was saved on a private server located in **ALEXANDER's RESIDENCE**. In addition, ALEXANDER prepared the draft RFP's at **ALEXANDER's RESIDENCE** and sent them to PARADIS utilizing ALEXANDER's Personal Account. ALEXANDER was not worried about these communications because he deleted the accounts the prior night, July 22, 2019, after ALEXANDER's Office was searched and ALEXANDER's phone was reviewed. ALEXANDER stated that only PARADIS, WRIGHT, and he were aware of the RFP coordination, SCPPA manipulation, and e-mail server located at **ALEXANDER's RESIDENCE**.

77. On July 23, 2019, in a consensual recording, ALEXANDER also told PARADIS that he was concerned about the FBI imaging his phone and their communications. ALEXANDER said he had been deleting some of the messages, but he believed the FBI could still recover the data. ALEXANDER said he wanted to disclose to the new General Manager his conduct with PARADIS and that he may get fired. ALEXANDER also said that he could "talk his way out of anything with the FBI" by stating that his actions were to help address cybersecurity and were best for the City.

78. In subsequent consensually recorded calls, ALEXANDER told PARADIS that he spoke to the new General Manager and disclosed his conduct. ALEXANDER was unaware whether he would be fired based on the conversation. ALEXANDER also said that he did not have a concern about the e-mails from ALEXANDER's Personal Account because he had gotten rid of them and "no one [the FBI] had come to [**ALEXANDER's RESIDENCE**] for that server."

79. Based on my training, experience, and knowledge of the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

investigation, I believe that ALEXANDER's deletion of his Personal Account from the server at **ALEXANDER's RESIDENCE** constitutes a violation of 18 U.S.C. § 1510 (Obstruction of Justice).

E. The FBI Interview of ALEXANDER

80. On July 24, 2019, the FBI received information from the City Attorney's Office and LADWP that ALEXANDER reported to them that he coordinated with PARADIS information related to the Cyber Consulting Contract RFP. ALEXANDER disclosed that he had text messages between himself and PARADIS describing their interactions. ALEXANDER provided the City Attorney's Office and LADWP screenshots of these text messages along with his personal annotation of the meaning of the text messages and a summary of ALEXANDER's interactions with PARADIS. The City Attorney's Office and LADWP subsequently provided ALEXANDER's document. Based on my review of the document, the consensual recordings, e-mails from ALEXANDER's Personal Account, and my knowledge of the investigation, I believe ALEXANDER provided material false statements and omitted material information from this document and his disclosure to the City.

81. On July 24, 2019, I conducted a voluntary interview of ALEXANDER. ALEXANDER stated that he prepared the document and that the annotations and screenshots were a true and accurate account of the events. During the interview I believe that ALEXANDER provided numerous demonstrable false statements and omissions in an effort to minimize his criminal conduct.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

ALEXANDER did confirm his use of ALEXANDER's Personal Account and the private server located in ALEXANDER's RESIDENCE. In addition, ALEXANDER admitted to deleting e-mails throughout his interactions with PARADIS; however, based on the consensual recording with WRIGHT, ALEXANDER in fact deleted the e-mails after the FBI conducted the searches on July 22, 2019. ALEXANDER also admitted that he assisted PARADIS in preparing ARDENT's RFP response to the Cyber Consulting Contract which ALEXANDER characterized as being "inappropriate."

82. On July 25, 2019, ALEXANDER sent me an email stating, "Upon further reflection last evening, there are additional points I would like to bring up." I have not had the opportunity to meet with ALEXANDER or receive the "additional points."

VII. PREMISES INFORMATION

83. Based on the consensual recordings with ALEXANDER, I understand that ALEXANDER is housing a private server at ALEXANDER's RESIDENCE. In addition, based on the preparation of the RFP and utilization of the server at **ALEXANDER's RESIDENCE**, I believe that **ALEXANDER's RESIDENCE** may have evidence of the criminal schemes and Target Offenses. I believe the requested warrant is necessary to determine whether 1) ALEXANDER did in fact delete the accounts on the server and therefore obstructed justice, 2) if ALEXANDER only deleted some of the data and there is additional evidence still present, or 3) ALEXANDER did not delete the data and evidence still remains on the server located

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

in **ALEXANDER's RESIDENCE**. In addition to the server, based on ALEXANDER preparing documents for PARADIS and utilizing ALEXANDER's Personal Account, the server being housed at ALEXANDER's RESIDENCE, and the appearance that ALEXANDER wanted to conceal his interactions with PARADIS from others at LADWP, I believe there may be documents, records, digital devices, etc. present in **ALEXANDER's RESIDENCE**. This evidence may include the items to be seized described in Attachment B.

VIII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[31]

84. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the

[31] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

85. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

86. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

X. AFFIDAVIT NOT ATTACHED TO SEARCH WARRANT

87. The affidavit has not been attached to the search warrants because allowing disclosure during the search would give subjects and targets of the investigation an opportunity to destroy evidence, change patterns of behavior, notify confederates, flee from prosecution, or otherwise seriously jeopardize the investigation. In addition, I am aware that "if the face sheet and attachments clearly state that the agents have lawful authority to conduct the search and specify the location to be searched and the items sought, the affidavit supporting the probable cause determination need not be served at the time of the search." United States v. Celestine, 324 F.3d 1095, 1100, 1101 (9th Cir. 2003).

XII. CONCLUSION

88. Based on the foregoing, I request that the Court issue the requested search warrants.

ANDREW CIVETTI, Special Agent
Federal Bureau of
Investigation

Subscribed to and sworn before
me on July 25, 2019.

HONORABLE PATRICK J. WALSH
UNITED STATES MAGISTRATE JUDGE

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AO 93 (Rev. 11/13) Search and Seizure Warrant (USAO CDCA Rev. 04/17)

UNITED STATES DISTRICT COURT

for the

Central District of California

COPY

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
[redacted] Walnut, California

Case No. 2:19-MJ-03045

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 7/25/19 7:30 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh, U.S. Magistrate Judge
Printed name and title

AUSA: Melissa Mills (213) 894-0627

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:19-MJ-03045	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

PROPERTY TO BE SEARCHED

The premises to be searched is located at [redacted], Walnut, California, believed to be the residence of DAVID ALEXANDER ("**ALEXANDER's RESIDENCE**") and pictured below. The residence is a detached four bedroom three bathroom single family home. On the front curb of the residence is painted [redacted] in black paint on a white background. The numbers [redacted] are also above the double wide front door.

[redacted]

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1343 (Wire Fraud); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); and 16 U.S.C. §§ 824o, 825o (Knowing and Willful Violation of Electric Reliability Standards) (the "Target Offenses"), namely:

a. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Los Angeles Department of Water and Power ("LADWP") contracts and proposed contracts related to any company owned, operated, or affiliated with PAUL PARADIS, including but not limited to PARADIS LAW GROUP LLC, AVENTADOR UTILITY SOLUTIONS LLC ("AVENTADOR"), ARDENT UTILITY SOLUTIONS LLC ("ARDENT"), and CYBERGYM;

ii. LADWP contracting protocols and processes, including but not limited to any manipulations of contracting processes or the use of other entities to circumvent the requirement for open-bid contracts;

iii. LADWP use of the Southern California Public Power Authority's ("SCCPA") Request for Proposal ("RFP") process;

iv. Financial payments, gifts, services, or other benefits given to, offered to, or solicited by City employees or officials or their staff or family members;

v. Any business venture in which a City official had a financial interest, including but not limited to AVENTADOR and ARDENT;

vi. For the period from June 1, 2008, through the present, any physical security or cybersecurity issues, risks, or threats identified at LADWP, including any communications or presentations to LADWP employees, LADWP Board members, or Los Angeles City Council members;

vii. Any physical security or cybersecurity assessments or surveys performed for or at LADWP, from June 1, 2008, to the present, whether by ARDENT, AVENTADOR, [redacted] or any other cybersecurity vendor;

viii. Any cybersecurity or physical security risk management, mitigation or remediation relating to cybersecurity or physical security issues identified at LADWP after June 1, 2008;

ix. For the period from June 1, 2008, through the present, any certifications, reports, statements, or other communications to the Western Electricity Coordinating Council ("WECC"), the North American Electric Reliability Corporation ("NERC"), or the Federal Energy Regulatory Commission ("FERC") regarding compliance or failure to comply with NERC Critical Infrastructure Protection ("NERC-CIP") standards;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

x. Falsification, manipulation, or destruction of records, data, or other information relating to compliance with NERC-CIP standards;

xi. Destruction or concealment of evidence.

b. Bank records, tax records, and other financial records from December 1, 2014, through present, for ALEXANDER.

c. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

d. Any digital device and data servers, to include and personal/private data servers or data servers of the City of Los Angeles or Los Angeles Department of Water and Power, capable of being used to commit or further the criminal schemes and Target Offenses, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such Target Offenses, and forensic copies thereof.

e. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

outside the scope of the items to be seized absent further order of the Court.

5. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

6. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

UNITED STATES DISTRICT COURT

for the

Central District of California

ORIGINAL

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

THOMAS PETERS, date of birth [redacted] 1966

Case No. 2:19-MJ-03814

CENTRAL DIST. OF CALIF. BY DEPUTY SEP 12 2019

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-2

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 666	Bribery and Kickbacks Concerning Federal Funds
18 U.S.C. §1001	False Official Statements
18 U.S.C. §1341	Mail Fraud
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1346	Deprivation of Honest Services
18 U.S.C. § 1505	Obstructing Federal Proceeding
18 U.S.C. § 1510	Obstruction of Justice
18 U.S.C. § 1621	Perjury
18 U.S.C. § 1951	Extortion
18 U.S.C. § 1956	Money Laundering
16 U.S.C. §§ 824o & 825o	Reliability Standards

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Andrew Civetti, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 9/12/19

Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh, U.S. Magistrate Judge

Printed name and title

AUSA: Melissa Mills (213) 894-0627

ATTACHMENT A-2

PERSON TO BE SEARCHED

The person to be searched is **THOMAS PETERS**, date of birth [redacted] 1966, as pictured below:

ATTACHMENT B

I. CELL PHONE ITEMS TO BE SEIZED

1. Law enforcement personnel are authorized to seize the cellular telephone with telephone number [redacted] (the **"TARGET PHONE"** or the "digital device").

2. During the execution of this search warrant, law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of THOMAS PETERS onto the Touch ID sensor of the **TARGET PHONE**, or hold the **TARGET PHONE** in front of PETERS's face to activate the Face ID sensor, in order to gain access to the contents of any such device as authorized by this warrant. The government may not use more force than is reasonable to obtain this access.

3. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the Electronically Stored Information ("ESI") and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review and seize the ESI contained on the **TARGET PHONE** for evidence of the criminal schemes and evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False Official Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); and 1346 (Deprivation of Honest Services);

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1621 (Perjury); 1951 (Extortion); 1956 (Money Laundering); 16 U.S.C. §§ 824o, 825o (Electric Reliability Standards) (collectively, the "Target Offenses"), occurring after December 1, 2015, namely:

a. Evidence of who accessed or used the digital device, including records about their identities and whereabouts.

b. Communications with or referencing: PAUL KIESEL, PAUL PARADIS, GINA TUFARO, JACK LANDSKRONER, JAMES CLARK, Michael Feuer, or Julissa Salgueiro.

c. Records, documents, programs, applications, or materials referencing:

i. PETERS's bank accounts, credit card accounts, tax returns and records, other financial accounts, and wire transfer records;

ii. PETERS's calendar or date book, including calendars or date books stored on digital devices;

iii. Any lawsuit where the City was a party to the lawsuit and appears to have had a legal, representational, and/or financial interest in both sides of the lawsuit, including Jones v. City of Los Angeles;

iv. The litigation of City of Los Angeles v. PricewaterhouseCoopers, including the initial filing of the action, and any discovery, depositions, or filings therein;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

v. Any litigation or contemplated litigation relating to the LADWP Customer Care and Billing system, or the resolution of such litigation;

vi. Financial payments, gifts, services, or other benefits given or offered to officials at LADWP or the City Attorney's Office or their staff or family members, or solicited by officials at LADWP or the City Attorney's Office or their staff or family members;

vii. Efforts to conceal the City Attorney's Office's business practices or members thereof, including but not limited to knowledge or direction of payments made or benefits given to individuals or entities in an effort to discourage their revelation of those practices;

viii. Negotiations or agreements relating to hush money payments offered to or solicited by any individual or entity to conceal business practices by the City Attorney's Office or members thereof, and communications relating thereto;

ix. Obstruction of justice, perjury, or false official statements.

d. Any **TARGET PHONE** which is itself or which contains evidence, contraband, fruits, or instrumentalities of the criminal schemes and evidence of the Target Offenses, and forensic copies thereof.

e. With respect to any **TARGET PHONE** used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

i. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations;

ii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

iii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications or other text or written communications sent to or received from any digital device;

iv. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

v. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

vi. evidence of the attachment of other devices;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

vii. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

viii. evidence of the times the device was used;

ix. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

x. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

xi. records of or information about Internet Protocol addresses used by the device;

xii. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

5. The Privilege Review Team will review the identified digital device as set forth herein. The Search Team will review only digital device data which has been released by the Privilege Review Team.

6. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

7. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

8. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

9. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

10. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

11. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

12. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

13. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

14. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

15. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

16. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

17. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

18. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Table of Contents

I. INTRODUCTION.....1

II. PURPOSE OF AFFIDAVIT.....2

III. STATEMENT OF PROBABLE CAUSE.....4

A. Information Proffered By PAUL KIESEL.....4

B. Text Messages Between PETERS and KIESEL.....8

C. KIESEL's Diary Entry.....12

D. [redacted].....13

E. Recorded Telephone Conversation with PETERS.....14

IV. TRAINING AND EXPERIENCE ON DIGITAL DEVICES.....18

V. AFFIDAVIT NOT ATTACHED TO SEARCH WARRANT.....20

VI. CONCLUSION.....21

ATTACHMENT A-1.....1

ATTACHMENT A-2.....1

ATTACHMENT B.....1

I. CELL PHONE ITEMS TO BE SEIZED.....1

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION.....6

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AFFIDAVIT

I, Andrew Civetti, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since September 2015. I am currently assigned to a Public Corruption Squad, where I specialize in the investigation of corrupt public officials, including bribery, fraud against the government, extortion, and money laundering. In addition, I have received training in the investigation of public corruption and other white collar crimes.

2. I am currently one of the agents assigned to an investigation of alleged corrupt activities at the Los Angeles Department of Water and Power ("LADWP") and the Los Angeles City Attorney's Office ("City Attorney's Office"). As discussed in more detail herein, these activities include the following criminal schemes, among others:

a. Collusive litigation practices related to lawsuits involving the City Attorney's Office and LADWP, which were fueled in at least one instance by a $2.175 million kickback from plaintiff's attorney JACK LANDSKRONER to attorney PAUL PARADIS, a Special Counsel retained by the City Attorney's Office.

b. An $800,000 hush-money payment to a prospective whistleblower by Special Counsels PARADIS and PAUL KIESEL in exchange for silence as to collusive and potentially fraudulent

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

litigation practices involving PARADIS, KIESEL, and THOMAS PETERS, then the Chief of Civil Litigation at the City Attorney's Office, among others.

3. I am aware that the City receives in excess of $10,000 annually in federal funds through various programs.

II. PURPOSE OF AFFIDAVIT

4. This affidavit is made in support of applications to search for a cellular telephone, telephone number [redacted], located in the following residence, or alternatively on the persons of THOMAS PETERS (the "**TARGET PHONE**"):

a. [redacted], Pacific Palisades, CA 90272, described in more detail in Attachment A-1 (**"PETERS' RESIDENCE"**);

b. THOMAS PETERS, described in more detail in Attachment A-2.

5. In connection with the investigation into this matter, the requested search warrants seek authorization to search **PETERS' RESIDENCE**, or alternatively the person of PETERS, for the **TARGET PHONE** described in Attachment B, and any data on the **TARGET PHONE** that constitutes evidence of the criminal schemes identified below and evidence or fruits of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False Official Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); and 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1621 (Perjury); 1951 (Extortion); 1956 (Money Laundering); 16 U.S.C. §§ 824o, 825o (Electric

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Reliability Standards) (collectively, the "Target Offenses"), and any **TARGET PHONE** that is itself an instrumentality of the criminal schemes and Target Offenses, as also set forth in Attachment B. Attachments A-1, A-2, and B are incorporated herein by reference.

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, information obtained from other agents and witnesses, consensually recorded conversations, and information obtained from the prior related search warrants, as detailed further below. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

7. On July 18, 2019, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized two search warrants (19-MJ-2915 and 19-MJ-2923) for the seizure of information associated with nineteen e-mail accounts from two Internet Service Providers, and six search warrants (19-MJ-2913, 19-MJ-2914, 19-MJ-2917, 19-MJ-2919, 19-MJ-2920, and 19-MJ-2922) for the premises of sixteen locations (collectively, the "July 2019 search warrants"). All of the July 2019 search warrants were supported by a single omnibus affidavit (the "omnibus affidavit"). The July 2019 search warrants and their supporting

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

omnibus affidavit are incorporated herein by reference, and copies can be made available for the Court.[1]

III. STATEMENT OF PROBABLE CAUSE

8. The FBI is conducting an ongoing investigation into the City Attorney's Office and LADWP, including into suspected bribery-fueled collusive litigation relating to an LADWP billing system, and an $800,000 hush-money payment made in order to conceal those collusive litigation practices. Background facts relating to these and other facets of the investigation are further detailed in the omnibus affidavit referenced above and incorporated herein. The case numbers associated with the search warrants supported by my omnibus affidavit are outlined above.

A. Information Proffered By PAUL KIESEL

9. The government has conducted voluntary interviews with attorney PAUL KIESEL, who was at relevant times a Special

[1] In addition, on April 18, 2019, the Honorable Jacqueline Chooljian, United States Magistrate Judge, authorized search warrants relating to then-General Manager of the Los Angeles Department of Water and Power's then General Manager, DAVID WRIGHT. Specifically, these warrants authorized search warrants for WRIGHT's phone, WRIGHT's laptop, two of WRIGHT's email addresses, and two of WRIGHT's Apple iCloud accounts (collectively, the "April 2019 search warrants"). On June 4, 2019, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized search warrants for two of WRIGHT's residences, WRIGHT's office, WRIGHT's cellular phone, and a burner cellular phone that the FBI had surreptitiously provided to WRIGHT, as well as for an e-mail account used by Deputy Los Angeles City Attorney JAMES CLARK; on June 18, 2019, Judge Walsh authorized a subsequent search warrant for WRIGHT's Riverside residence (collectively, the "June 2019 search warrants"). The April 2019 and June 2019 search warrants and their supporting affidavits are also incorporated herein by reference, and copies can be made available for the Court.

Counsel for the City Attorney's Office on litigation relating to the LADWP billing system.[2] KIESEL advised the government as follows:

a. In 2017, KIESEL was approached by Julissa Salgueiro, an employee that his law firm had recently terminated, who told him that she had taken certain documents from the firm showing the City's entanglement in the representation of an adverse party that had sued the City in the LADWP billing system litigation.

b. Salgueiro initially demanded $1,500,000 from KIESEL, or she would take the materials public.

c. KIESEL was not initially concerned about Salgueiro taking the materials public, because although they might be "embarrassing" to the City, he did not believe that they reflected any wrongdoing.

d. KIESEL met with Salgueiro in late October 2017 in a meeting coordinated by PAUL PARADIS, another Special Counsel for the City Attorney's Office on the same matter, who was serving as a mediator between Salgueiro and KIESEL. At that time, Salgueiro demanded $900,000, in an offer that she said would remain open for 24 hours. KIESEL agreed to think about it and then countered with an offer of $60,000.

e. KIESEL thereafter received a text from Salgueiro that she would see him in CCW[3] on December 4, 2017, which KIESEL

[2] Interviews with KIESEL, which I attended, were conducted in the presence of KIESEL's attorney.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

interpreted as a threat to publicize her information at the next-scheduled hearing in *City of Los Angeles v. PwC*, which was scheduled for that date in the Central Civil West courthouse.[4]

f. After Salgueiro's threat, KIESEL received a text from PETERS demanding that KIESEL come to see him immediately. KIESEL left a court proceeding in Orange County to drive to PETERS's office at City Hall East in Los Angeles, where he and PARADIS met with PETERS. During that meeting, PETERS was very angry and told KIESEL to make the problem go away or he (KIESEL) would be fired.

g. KIESEL perceived that the threat of firing was coming from above PETERS —— namely, from either Deputy City Attorney JAMES CLARK or City Attorney Michael Feuer —— but he could not articulate a specific basis for that perception.[5]

h. KIESEL recalled that Salgueiro had attempted to contact Feuer and CLARK, and had left documents for CLARK. KIESEL recalled that CLARK was aware of this contact, but it was KIESEL's understanding that CLARK may not have fully understood

---

[3] Central Civil West was at the time a Superior Court courthouse in Los Angeles, where the judge presiding over the *City of Los Angeles v. PwC* litigation was located.

[4] As noted in the omnibus affidavit, these facts are substantially corroborated by text messages with Salgueiro reviewed by the government and information proffered by PARADIS, including an October 31, 2017 text message from Salgueiro reading, "I'll c u both Dec. 4 at 2pm at CCW.". I believe these messages are further corroborated by other newly obtained evidence described herein.

[5] [redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

the situation, and that CLARK delegated handling of the issue to PETERS.[6]

i. KIESEL did not want to lose his job as Special Counsel for the City, particularly after investing substantial time and resources into the case of *City of Los Angeles v. PwC* over approximately three years without any compensation (the Special Counsel contract provided for compensation for KIESEL and PARADIS only on a contingency-fee basis).

j. KIESEL subsequently met with PETERS again, and PETERS had calmed down. PETERS indicated that he would not terminate the contract, and that they would see what happened.

k. After Salgueiro approached PwC's counsel in court on December 4, 2017, KIESEL renewed his efforts to negotiate a settlement, again using PARADIS as a mediator.

l. KIESEL and Salgueiro agreed to a settlement by which KIESEL would pay Salgueiro $800,000, and Salgueiro would return the documents that she had threatened to expose and remain silent about their contents. After the agreement was formalized, KIESEL paid Salgueiro $800,000, and PARADIS paid KIESEL $400,000.

[6] As described in the omnibus affidavit, I have reviewed related text messages between Salgueiro and PARADIS, including a message from Salgueiro on October 10, 2017, advising that she left a written message with CLARK's assistant but had not heard back, and asking whether she should drop off a set of documents with a note.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

m. KIESEL did not get any money from the *Jones* matter and was not aware of any bribes or kickbacks paid to others in connection with those matters.[7]

B. Text Messages Between PETERS and KIESEL

10. KIESEL voluntarily provided the government with a download of text messages from his phone between KIESEL and PETERS, which I have reviewed. KIESEL advised that he exchanged these messages with PETERS using [redacted] (the **TARGET PHONE**).[8]

11. The text messages provided by KIESEL reflect the following pertinent conversation from October 17, 2017:

> PETERS: Paul - something has come up in DWP. **It is crucial I meet with you and Paradis today in my office. When can you come?** Thanks.
>
> KIESEL: I am on my way to court in OC. Can you call me Thom on my cell. I might be back late afternoon.
>
> PETERS: What time this afternoon works? **This is imperative.**
>
> KIESEL: Depends on the MSC today. Starts at 9. Will report. Can you talk?

---

[7] KIESEL advised that he paid PETERS a referral fee on one separate case after PETERS joined the City Attorney's Office. Specifically, PETERS referred a case in 2013, PETERS joined the City Attorney's Office in 2014, and in August 2015, KIESEL paid a referral fee of $29,560.24 in connection with the case, which did not involve the City of Los Angeles.

[8] No phone number is listed on the download that KIESEL provided, but KIESEL's provision of the **TARGET PHONE** number is consistent with the cell number for PETERS that the government obtained in a voluntary search of PARADIS's phone and from database checks. The most recent text messages that KIESEL provided with PETERS were from March 2019, just before KIESEL was fired as Special Counsel. This is consistent with information proffered by KIESEL that he has had no contact with PETERS since that time.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

PETERS: **I need to see you.**

KIESEL: Understood. Need to discuss timing I am at MSC for 5 cases in OC before judge Sanders. Could go well into the afternoon but if this is urgent I will have to arrange coverage here.

PETERS: **It is urgent.**

KIESEL: Okay. What time? Can you meet at noon? I will leave OC now. Let me know.

PETERS: Thank you.

12. I believe that these text messages corroborate the information proffered by KIESEL, described herein, that in mid-October 2017, PETERS demanded to see KIESEL immediately, requiring KIESEL to leave a court proceeding in Orange County to drive to PETERS's office in City Hall East. As noted above, KIESEL proffered that at the meeting, PETERS threatened to fire KIESEL if KIESEL did not settle with Salgueiro to prevent her from going public with the documents. KIESEL further advised that since he was working on a contingency-fee basis, he had not been paid for his years of work as Special Counsel and thus was motivated to follow PETERS's instruction to pay Salgueiro in order to continue KIESEL's Special Counsel contract in pursuit of eventual compensation.

13. The text messages also reflect the following pertinent conversation from December 4, 2017, at the times indicated in brackets herein:

KIESEL: I am parked on the north west corner of 1st and Los Angeles Street. [12:13 p.m.]

PETERS: I'm with Paradis. Can u come to my office now to meet? [3:06 p.m.]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

L. Yes. [redacted] is at the elevator engaging J so [redacted] and I are stuck. Will come down as soon as we can. [3:07 p.m.]

PETERS: She gave [redacted] her card. [3:09 p.m.]

KIESEL: You waiting for me or going back with Paul [3:09 p.m.]

PETERS: Tried to file a bunch of docs. I'm with Paradis. [3:11 p.m.]

KIESEL: Going back to City Hall? I will meet you there if you go with Paul. [3:12 p.m.]

PETERS: Yes. My office please. I will get you parking. [3:14 p.m.]

KIESEL: Thanks. [3:14 p.m.]

PETERS: **Settle the case if you can! I need you to take care of this.** We are in my office. [3:40 p.m.]

KIESEL: On my way up now will be there in three minutes. [3:59 p.m.]

L: I am meeting Julissa tonight at 7:30 PM. With [redacted] Will get this done. [6:09 p.m.]

KIESEL: **Deal with J at 800.** 450 within 7 days. Have 150 in si[redacted]balance by May 1. She will work with attorney [redacted] as her counsel. Will return all documents when completed. Oyyy [9:15 p.m.]

PETERS: **Good job. Be sure there is a confidentiality agreement of a sort that would make Marty Singer envious.** [11:43 p.m.]

14. I believe that these texts corroborate the information proffered by KIESEL, described herein, that at 2:00 p.m. on December 4, 2017, Salgueiro attended a hearing in the LADWP billing litigation following her threat to do so if KIESEL did not pay her $900,000, which led to KIESEL renewing negotiations to pay Salgueiro $800,000 in exchange for her silence and her assent to a confidentiality agreement.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

15. Upon review of the above-described text messages, KIESEL recalled that PETERS attended that hearing with KIESEL and PARADIS and was in fact present in court when Salgueiro showed up, which is consistent with my interpretation of the text messages.

16. I believe that PETERS's statements, "She gave [redacted] her card," and "Tried to file a bunch of docs," are consistent with information proffered by PARADIS and KIESEL and proffered [redacted] to by Salgueiro -- namely, that Salgueiro approached Gibson, Dunn & Crutcher attorney [redacted] (who represented PwC in the *City v. PwC* litigation) at the hearing to provide her contact information, and that she tried to file with the court the documents taken from KIESEL's firm. KIESEL and PARADIS have both opined, and Salgueiro has confirmed, that Salgueiro did so in order to show KIESEL and PETERS that she was willing to share the information about the City's litigation practices with the City's adversary and with the court.

17. I believe that KIESEL's text message, "Deal with J at 800. 450 within 7 days. Have 150 in sixty days balance by May 1," reflects his description to PETERS of his agreement to pay Salgueiro $800,000. I believe that this is also consistent with information proffered by PARADIS, information [redacted] by Salgueiro, and the settlement documents provided by PARADIS and Salgueiro, as described further herein and in the omnibus affidavit.

18. I believe that PETERS's text message, "Good job. Be sure there is a confidentiality agreement of a sort that would

make Marty Singer envious," reflects PETERS's endorsement of KIESEL's decision to pay Salgueiro $800,000 to buy her silence as to the City Attorney's Office's litigation practices, and to obtain a strong and enforceable confidentiality agreement. I am aware from open-source media reports that Marty Singer is a prominent Hollywood-based attorney who is known for aggressive tactics including the use and enforcement of strong confidentiality agreements.

C. KIESEL's Diary Entry

19. In a recent proffer session with the government, KIESEL advised that since 1980, he has regularly kept a handwritten diary on noteworthy events in his life.

20. During that same proffer, KIESEL showed the government an entry in his diary that was dated December 1, 2017, that appears to recount KIESEL's recollection of the above-described October 2017 meeting in which PETERS called KIESEL up from Orange County to discuss Salgueiro's threat. According to the entry, which described PETERS as "spitting MAD" (emphasis in original), PETERS told KIESEL, "How could you not tell me about this threat, Paul??" The entry further reports, "Thom said you have 2 choices. Either settle with J [Salgueiro] or your FIRED!" (emphasis in original).

21. I believe that this contemporaneous information from KIESEL's handwritten diary is consistent with the other information described herein as to events surrounding Salgueiro's threat.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

D. [redacted]

22. The government has interviewed, [redacted] and obtained documents from Salgueiro. Salgueiro [redacted] advised[10], in pertinent part, as follows:

a. Before leaving KIESEL's employ, Salgueiro took certain documents from his firm that she believed would show that the firm and the City conspired to represent both sides of the litigation in the *Jones v. City of Los Angeles* matter and in other matters (the "Salgueiro documents").

b. After Salgueiro's firing by KIESEL in or around July 2017, she demanded a large sum of money, around $900,000, from KIESEL in order to return the Salgueiro documents, refrain from taking the Salgueiro documents public, and resolve certain employment discrimination and harassment complaints.

c. KIESEL countered Salgueiro's demand with a lower five-figure offer, using former Special Counsel PAUL PARADIS as a mediator.

d. Salgueiro attempted to resolve the issue by providing some or all of the Salgueiro documents to Deputy City Attorney JAMES CLARK, but she was not successful in her attempt to speak directly with CLARK.

---

9 [redacted]

10 I attended the government's interview of Salgueiro.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

e. Salgueiro thereafter went to a court hearing in the *City of Los Angeles v. PwC* case on approximately December 4, 2017, and attempted to give some or all of the Salgueiro documents to the court, but the court clerk would not take them.

f. At that court hearing, while KIESEL and perhaps others from the City were present, Salgueiro approached PwC's counsel and told him that she had information for him. PwC's counsel provided his contact information and asked her to call him.

g. Immediately thereafter, KIESEL resumed negotiations with Salgueiro, and the parties reached a final settlement figure of $800,000 and an agreement requiring Salgueiro to return the Salgueiro documents and remain quiet about them. Salgueiro returned the Salgueiro documents but retained a copy of them in violation of the confidentiality agreement.[11]

h. After entering into a formal settlement agreement, KIESEL paid Salgueiro $800,000.

E. Recorded Telephone Conversation with PETERS

23. [redacted] recently provided the government a recording of a portion of a telephone

[11] Salgueiro provided the Salgueiro documents to the government [redacted]. These documents were submitted directly to the government's privilege-review team. Portions have since been provided to the prosecution team in heavily redacted form; however, the documents related to the *Jones* litigation have not yet been released.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

conversation between PETERS, KIESEL, PARADIS, and TUFARO.[12] According to [redacted], [redacted] surreptitiously recorded the conversation on January 27, 2019, when the City was preparing for the impending Person Most Qualified deposition of Deputy City Attorney JAMES CLARK.[13] The recording contains the following relevant portions:

> PETERS:[14] Okay. **Here's what I would like to do though, at Mike's request. He said to me, "What are the very, very worst documents out there** that we've created that would most likely lead to embarrassment or serve as a basis for somebody's… or Jamie Court's allegations that there was, that there was some conflict… anything from the pinnacle or standpoint of ethics." . . .
>
> Now, I said to him "Ya know, Mike, I don't really know," and he kinda chided me for not knowing and that's a fair criticism from where I stand. **I said, "although it's not teed up yet, there's a probably greater than 50 percent likelihood that eventually it will be revealed that we drafted for Landskroner a draft complaint."** Now, at first, there was a great gnashing of teeth.
>
> . . .
>
> PETERS: But this is, Mike is aware that this could get ugly for a while. But he wants to let us get in there and tear off the band-aids because once you get

[redacted]

[13] The FBI is in the process of obtaining [redacted] phone in order to obtain a copy of the recording directly therefrom. The copy that I have reviewed was provided on a disc by [redacted] criminal defense attorneys along with a draft transcript prepared at their behest (which I have also reviewed).

[14] I am not familiar with PETERS's voice. The transcript identifies a specific speaker as PETERS, which is corroborated by the context of the conversation as well as by the other participants addressing that speaker as "Tom" and "Tommy." I am familiar with the voices of KIESEL and PARADIS, and recognize both on the recording as indicated in the transcript.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

beneath the smoke, you know, you'll see that there really is ultimately, no ethical fire.

. . .

PETERS: And all of the story is going to be told through these emails? Right, Paul?

PARADIS: Yes. Yes.

KIESEL: **Yes. And by the way, there are emails with the City of L.A., discussing -- knowing we were doing this and encouraging us to do this quickly.**

PETERS: **Okay.**

. . .

KIESEL: And then, Tommy, the only other piece, at least on the emails I saw, was Michael Libman, who was gonna to be filing the Jones versus DWP complaint reached out to me. He was in trial, and he said, "Paul, I need the money to file the Jones action." And I said, maybe something like, "We'll take care of it." And Paul Paradis was copied on it. And Paul wrote back and said, “no Landskroner is picking up all costs, all expenses. It’s on Landskroner.” And Landskroner obviously paid for the filing of the complaint.

PETERS: I will want to read that one because that one, because optically, someone is going to optically scratch their head on. So, I'll know about that one. Yeah, so if you could send those things to me so I can get through 'em before Wednesday morning, that would make me more comfortable. **It's just what’s the universe of shit that’s going to happen. I can give a heads up to Mike.**

24. Based on the context of the messages and my knowledge of the investigation, I believe PETERS’ references to “Mike” throughout the conversation refer to Michael Feuer, the City Attorney and PETERS’ boss at that time. I further believe that the reference to “Jamie Court” refers to the president of an organization called Consumer Watchdog, which has, according to open-source media reports and other information revealed during

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

the investigation, raised public allegations of corruption and ethical violations by the City Attorney's Office and LADWP regarding the billing system litigation.

25. Feuer has voluntarily proffered information to the government [redacted] Feuer has also provided sworn testimony in a deposition in the underlying civil litigation. If PETERS' statements in the above conversation are true as to his conversations with Feuer, then they appear to be materially inconsistent with [redacted] information that Feuer has provided, including that Feuer was not aware of any City employee's involvement in the filing of the *Jones v. City* complaint or any coordination between the City and Jones' attorneys prior to that suit being filed.

26. I believe that PETERS's statements in the above-referenced telephone conversation are also inconsistent with a sworn declaration that he signed under penalty of perjury on June 11, 2019, and filed via the City's counsel. In that declaration, which I have reviewed, PETERS averred that he never authorized anyone to sue LADWP and was never aware of a plan for the City to authorize a lawsuit to be filed against LADWP.The text messages described herein and provided by KIESEL include messages between KIESEL and PETERS on January 26, 2019, that appear to coordinate the above-referenced January 27, 2019 recorded telephone call with PETERS, PARADIS, and KIESEL.

27. I believe that this evidence, coupled with other evidence -- including that articulated in the omnibus affidavit

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

-- gives rise to probable cause to believe that the **TARGET PHONE** will contain evidence of violations of the TARGET OFFENSES.

IV. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[15]

28. As used herein, the term "digital device" includes the **TARGET PHONE**.

29. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

---

[15] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

30. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

31. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

V. AFFIDAVIT NOT ATTACHED TO SEARCH WARRANT

32. The affidavit has not been attached to the search warrants because allowing disclosure during the search would give subjects and targets of the investigation an opportunity

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to destroy evidence, change patterns of behavior, notify confederates, flee from prosecution, or otherwise seriously jeopardize the investigation. In addition, I am aware that "if the face sheet and attachments clearly state that the agents have lawful authority to conduct the search and specify the location to be searched and the items sought, the affidavit supporting the probable cause determination need not be served at the time of the search." United States v. Celestine, 324 F.3d 1095, 1100, 1101 (9th Cir. 2003).

VI. CONCLUSION

33. Based on the foregoing, I request that the Court issue the requested search warrants.

ANDREW CIVETTI, Special Agent
Federal Bureau of
Investigation

Subscribed to and sworn before
me on September 12, 2019.

HONORABLE PATRICK J. WALSH
UNITED STATES MAGISTRATE JUDGE

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AO 93 (Rev. 11/13) Search and Seizure Warrant (USAO CDCA Rev. 04/17)

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* THOMAS PETERS, date of birth [redacted] 1966	)	Case No. 2:19-MJ-03814

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-2

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by reference[and attached hereto].

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 9/12/19 11:30 a.m.

Patrick J. Walsh

Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh, U.S. Magistrate Judge

Printed name and title

AUSA: Melissa Mills (213) 894-0627

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:19-MJ-03814	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-2

PERSON TO BE SEARCHED

The person to be searched is **THOMAS PETERS**, date of birth [redacted] 1966, as pictured below:

ATTACHMENT B

I. CELL PHONE ITEMS TO BE SEIZED

1. Law enforcement personnel are authorized to seize the cellular telephone with telephone number [redacted] (the **"TARGET PHONE"** or the "digital device").

2. During the execution of this search warrant, law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of THOMAS PETERS onto the Touch ID sensor of the **TARGET PHONE**, or hold the **TARGET PHONE** in front of PETERS's face to activate the Face ID sensor, in order to gain access to the contents of any such device as authorized by this warrant. The government may not use more force than is reasonable to obtain this access.

3. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the Electronically Stored Information ("ESI") and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review and seize the ESI contained on the **TARGET PHONE** for evidence of the criminal schemes and evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False Official Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); and 1346 (Deprivation of Honest Services);

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1621 (Perjury); 1951 (Extortion); 1956 (Money Laundering); 16 U.S.C. §§ 824o, 825o (Electric Reliability Standards) (collectively, the "Target Offenses"), occurring after December 1, 2015, namely:

a. Evidence of who accessed or used the digital device, including records about their identities and whereabouts.

b. Communications with or referencing: PAUL KIESEL, PAUL PARADIS, GINA TUFARO, JACK LANDSKRONER, JAMES CLARK, Michael Feuer, or Julissa Salgueiro.

c. Records, documents, programs, applications, or materials referencing:

i. PETERS's bank accounts, credit card accounts, tax returns and records, other financial accounts, and wire transfer records;

ii. PETERS's calendar or date book, including calendars or date books stored on digital devices;

iii. Any lawsuit where the City was a party to the lawsuit and appears to have had a legal, representational, and/or financial interest in both sides of the lawsuit, including Jones v. City of Los Angeles;

iv. The litigation of City of Los Angeles v. PricewaterhouseCoopers, including the initial filing of the action, and any discovery, depositions, or filings therein;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

v. Any litigation or contemplated litigation relating to the LADWP Customer Care and Billing system, or the resolution of such litigation;

vi. Financial payments, gifts, services, or other benefits given or offered to officials at LADWP or the City Attorney's Office or their staff or family members, or solicited by officials at LADWP or the City Attorney's Office or their staff or family members;

vii. Efforts to conceal the City Attorney's Office's business practices or members thereof, including but not limited to knowledge or direction of payments made or benefits given to individuals or entities in an effort to discourage their revelation of those practices;

viii. Negotiations or agreements relating to hush money payments offered to or solicited by any individual or entity to conceal business practices by the City Attorney's Office or members thereof, and communications relating thereto;

ix. Obstruction of justice, perjury, or false official statements.

d. Any **TARGET PHONE** which is itself or which contains evidence, contraband, fruits, or instrumentalities of the criminal schemes and evidence of the Target Offenses, and forensic copies thereof.

e. With respect to any **TARGET PHONE** used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

i. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations;

ii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

iii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications or other text or written communications sent to or received from any digital device;

iv. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

v. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

vi. evidence of the attachment of other devices;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

vii. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

viii. evidence of the times the device was used;

ix. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

x. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

xi. records of or information about Internet Protocol addresses used by the device;

xii. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

5. The Privilege Review Team will review the identified digital device as set forth herein. The Search Team will review only digital device data which has been released by the Privilege Review Team.

6. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

7. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

8. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

9. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

10. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

11. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

12. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

13. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

14. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

15. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

16. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

17. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

18. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AO 93 (Rev. 11/13) Search and Seizure Warrant (USAO CDCA Rev. 04/17)

UNITED STATES DISTRICT COURT

for the

Central District of California

ORIGINAL

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

[redacted] Pacific Palisades, CA 90272

Case No. 2:19-MJ-03813

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-1

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by reference[and attached hereto].

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for____days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 9/12/19 11:30

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh, U.S. Magistrate Judge
Printed name and title

AUSA: Melissa Mills (213) 894-0627

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 2:19-MJ-03813	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-1

PROPERTY TO BE SEARCHED

The premises to be searched is a single-family residence located at [redacted] Pacific Palisades, CA 90272 which is a residence of THOMAS PETERS ("**PETERS's RESIDENCE**"). **PETERS's RESIDENCE** is pictured below:

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

ATTACHMENT B

I. CELL PHONE ITEMS TO BE SEIZED

1. Law enforcement personnel are authorized to seize the cellular telephone with telephone number [redacted] (the "**TARGET PHONE**" or the "digital device").

2. During the execution of this search warrant, law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of THOMAS PETERS onto the Touch ID sensor of the **TARGET PHONE**, or hold the **TARGET PHONE** in front of PETERS's face to activate the Face ID sensor, in order to gain access to the contents of any such device as authorized by this warrant. The government may not use more force than is reasonable to obtain this access.

3. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the Electronically Stored Information ("ESI") and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review and seize the ESI contained on the **TARGET PHONE** for evidence of the criminal schemes and evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False Official Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); and 1346 (Deprivation of Honest Services);

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1621 (Perjury); 1951 (Extortion); 1956 (Money Laundering); 16 U.S.C. §§ 824o, 825o (Electric Reliability Standards) (collectively, the "Target Offenses"), occurring after December 1, 2015, namely:

a. Evidence of who accessed or used the digital device, including records about their identities and whereabouts.

b. Communications with or referencing: PAUL KIESEL, PAUL PARADIS, GINA TUFARO, JACK LANDSKRONER, JAMES CLARK, Michael Feuer, or Julissa Salgueiro.

c. Records, documents, programs, applications, or materials referencing:

i. PETERS's bank accounts, credit card accounts, tax returns and records, other financial accounts, and wire transfer records;

ii. PETERS's calendar or date book, including calendars or date books stored on digital devices;

iii. Any lawsuit where the City was a party to the lawsuit and appears to have had a legal, representational, and/or financial interest in both sides of the lawsuit, including Jones v. City of Los Angeles;

iv. The litigation of City of Los Angeles v. PricewaterhouseCoopers, including the initial filing of the action, and any discovery, depositions, or filings therein;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

v. Any litigation or contemplated litigation relating to the LADWP Customer Care and Billing system, or the resolution of such litigation;

vi. Financial payments, gifts, services, or other benefits given or offered to officials at LADWP or the City Attorney's Office or their staff or family members, or solicited by officials at LADWP or the City Attorney's Office or their staff or family members;

vii. Efforts to conceal the City Attorney's Office's business practices or members thereof, including but not limited to knowledge or direction of payments made or benefits given to individuals or entities in an effort to discourage their revelation of those practices;

viii. Negotiations or agreements relating to hush money payments offered to or solicited by any individual or entity to conceal business practices by the City Attorney's Office or members thereof, and communications relating thereto;

ix. Obstruction of justice, perjury, or false official statements.

d. Any **TARGET PHONE** which is itself or which contains evidence, contraband, fruits, or instrumentalities of the criminal schemes and evidence of the Target Offenses, and forensic copies thereof.

e. With respect to any **TARGET PHONE** used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_000696
Page 696 of 1425

i. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations;

ii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

iii. records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications or other text or written communications sent to or received from any digital device;

iv. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

v. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

vi. evidence of the attachment of other devices;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_000697
Page 697 of 1425

vii. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

viii. evidence of the times the device was used;

ix. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

x. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

xi. records of or information about Internet Protocol addresses used by the device;

xii. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_000698
Page 698 of 1425

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

5. The Privilege Review Team will review the identified digital device as set forth herein. The Search Team will review only digital device data which has been released by the Privilege Review Team.

6. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

7. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

8. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

9. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

10. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

11. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

12. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

13. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_000701
Page 701 of 1425

14. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

15. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

16. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

17. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_000702
Page 702 of 1425

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

18. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

UNITED STATES DISTRICT COURT

for the

Central District of California

COPY

In the Matter of the Search of: Information associated with accounts identified as [redacted] joseph.brajevich@ladwp.com; and associated with the phone number [redacted] that is within the possession, custody, or control of Apple Inc.	Case No. 2:20-MJ-00396

FILED
CLERK, U.S. DISTRICT COURT
JAN 31 2020
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

APPLICATION FOR WARRANT PURSUANT TO 18 U.S.C. § 2703

I, a federal law enforcement officer, request a warrant pursuant to Title 18, United States Code, Section 2703, and state under penalty of perjury that I have reason to believe that within the following data:

See Attachment A-1

There are now concealed or contained the items described below:

See Attachment B

The basis for the search is:

- ☑ Evidence of a crime;
- ☑ Contraband, fruits of crime, or other items illegally possessed;
- ☐ Property designed for use, intended for use, or used in committing a crime.

The search is related to a violation of:

Code section(s)	*Offense Description*
18 U.S.C. §§ 371; 666; 1001; 1341; 1343; 1346; 1505; 1510; 1951; 1956; and 1621	Conspiracy; Bribery and Kickbacks Concerning Federal Funds; False Statements; Mail Fraud; Wire Fraud; Deprivation of Honest Services; Obstructing Federal Proceeding; Obstruction of Justice; Extortion; Money Laundering; and Perjury in a Federal Proceeding (collectively, the "Target Offenses").

The application is based on these facts:

See attached Affidavit, which is incorporated herein by reference.

/s/
Applicant's signature

Andrew Civetti, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 1/31/2020

Patrick J. Walsh
Judge's signature

City and State: L.A., CA

Patrick J. Walsh, U.S. Magistrate Judge
Printed name and title

AUSA: Melissa Mills- Ext. 0627

ATTACHMENT A-1

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the Apple accounts associated with the below, and specifically including associated iCloud and iTunes accounts, that is within the possession, custody, or control of Apple Inc., a company that accepts service of legal process at 1 Infinite Loop, M/S 36-SU, Cupertino, California, 95014, regardless of where such information is stored, held, or maintained.

a. The Apple iCloud account, [redacted], associated with the phone number [redacted] and the name MIKE FEUER ("**FEUER's ACCOUNT**");

b. The Apple iCloud account, [redacted], and Apple iCloud account, joseph.brajevich@ladwp.com, associated with the phone number [redacted] and the name JOSEPH BRAJEVICH ("**BRAJEVICH's ACCOUNT**");

c. The Apple iCloud account associated with the phone number [redacted] and the name JAMES CLARK ("**CLARK's ACCOUNT**").

ATTACHMENT B

I. SEARCH PROCEDURES INCLUDING PRIVILEGE REVIEW PROCEDURE

1. The warrant will be presented to personnel of Apple, Inc. (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below in Section IV.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.15.a. below), law enforcement agents and/or other individuals assisting law enforcement agents who are not participating in the investigation of the case and who are assigned as the "Privilege Review Team" will review the content records, according to the procedures set forth herein, to determine whether or not any of the content records appears to contain or refer to communications between an attorney, or to contain the work product of an attorney, or between a spouse and any person ("potentially privileged information"). The "Search Team" (law enforcement personnel conducting the investigation

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

and search and other individuals assisting law enforcement personnel in the search) will review only content records which have been released by the Privilege Review Team. With respect to the non-content information produced by the PROVIDER (see Section II.15.b. below), no privilege review need be performed and the Search Team may review immediately.

5. With respect to content records, the Search Team will provide the Privilege Review Team and/or appropriate litigation support personnel[1] with an initial list of "scope key words" to search for on the content records, to include words relating to the items to be seized as detailed below. The Privilege Review Team will conduct an initial review of the content records using the scope key words, and by using search protocols specifically chosen to identify content records that appear to be within the scope of the warrant. Content records that are identified by this initial review, after quality check, as not within the scope of the warrant will be maintained under seal and not further reviewed absent subsequent authorization or in response to the quality check as described below.

6. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for among the content records that are identified by the initial review and quality check described above as appearing to fall within the

[1] Litigation support personnel and computer forensics agents or personnel, including IRS Computer Investigative Specialists, are authorized to assist both the Privilege Review Team and the Investigation Team in processing, filtering, and transferring documents and data seized during the execution of the warrant.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

scope of the warrant, to include specific words like names of any identified attorneys or law firms and names of any identified spouses] or their email addresses, and generic words such as "privileged" and "work product". The Privilege Review Team will conduct an initial review of these content records by using the privilege key words, and by using search protocols specifically chosen to identify content records containing potentially privileged information. Content records that are not identified by this initial review as potentially privileged may be given to the Search Team.

7. Content records that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Content records determined by this review not to be potentially privileged may be given to the Search Team. Content records determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a Privilege Review Team Assistant United States Attorney ("PRTAUSA"). Content records identified by the PRTAUSA after review as not potentially privileged may be given to the Search Team. If, after review, the PRTAUSA determines it to be appropriate, the PRTAUSA may apply to the court for a finding with respect to particular content records that no privilege, or an exception to the privilege, applies. Content records that are the subject of such a finding may be given to the Search Team. Content records identified by the PRTAUSA after review as privileged will be maintained under seal by the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

investigating agency without further review absent subsequent authorization.

8. The Search Team will search only the content records that the Privilege Review Team provides to the Search Team at any step listed above in order to locate, extract and seize content records that are within the scope of the search warrant (see Section III below). The Search Team does not have to wait until the entire privilege review is concluded to begin its review for content records within the scope of the search warrant. The Search Team and the Privilege Review Team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

9. During its review, the Search Team may provide the Privilege Review Team and/or appropriate litigation support personnel with a list of additional "scope key words" or search parameters to capture the items to be seized as detailed below; any additional content records identified through this quality check must first be reviewed by the Privilege Review Team subject to the terms set forth herein before being released to the Search Team. This quality check is intended only to ensure that the initial scope key word review successfully eliminated only data outside the scope of the search warrant from seizure.

10. If, while reviewing content records or non-content information, either the Privilege Review Team or the Search Team encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

shall immediately discontinue its search pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

11. The Privilege Review Team and the Search Team will complete the search of non-content information and both stages of the search of the content records discussed herein as soon as is practicable but not to exceed 180 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the records beyond this 180-day period without first obtaining an extension of time order from the Court.

12. Once the Privilege Review Team and the Search Team have completed their review of the non-content information and the content records and the Search Team has created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the Search Team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, neither the Privilege Review Team nor the Search Team will access the data from the sealed original production which fell outside the scope of the items to be seized or was determined to be privileged absent further order of the Court.

13. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

14. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDER

15. To the extent that the information described in Attachment A is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each **TARGET ACCOUNT** listed in Attachment A:

a. All contents of all wire and electronic communications associated with the **TARGET ACCOUNT**, limited to that which occurred on or after December 1, 2014,[2] including:

i. All e-mails, communications, or messages of any kind associated with the **TARGET ACCOUNT**, including stored or preserved copies of messages sent to and from the account, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information

[2] To the extent it is not reasonably feasible for the PROVIDER to restrict any categories of records based on this date restriction (for example, because a date filter is not available for such data), the PROVIDER shall disclose those records in its possession at the time the warrant is served upon it.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

associated with each e-mail or message, and any related documents or attachments.

ii. All records or other information stored by subscriber(s) of the **TARGET ACCOUNT**, including address books, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files.

iii. All records pertaining to communications between the PROVIDER and any person regarding the **TARGET ACCOUNT**, including contacts with support services and records of actions taken.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), any alternate names, other account names or e-mail addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, **and including any changes made to any subscriber information** or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

services used, and including the dates on which such changes occurred, for the following accounts:

(I) the **TARGET ACCOUNT.**

ii. All user connection logs and transactional information of all activity relating to the **TARGET ACCOUNT** described above in Section II.15.a., including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations, and including specifically the specific product name or service to which the connection was made.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

16. For each **TARGET ACCOUNT** listed in Attachment A, the search team may seize all information between December 1, 2014, and the present described above in Section II.15.a. that constitutes evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding), namely:

a. Information relating to who created, accessed, or used the **TARGET ACCOUNT**, including records about their identities and whereabouts.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Retention of PAUL PARADIS and PAUL KIESEL, or entities related thereto, to represent the City of Los Angeles;

ii. Communications involving or relating to any party to, or to counsel for any party to, *Jones v. City of Los Angeles* (the "*Jones* matter") or *City of Los Angeles v. PricewaterhouseCoopers* (the "*PwC* matter"), including communications with or referencing MICHAEL FEUER, JAMES CLARK, THOMAS PETERS, PAUL PARADIS, PAUL KIESEL, GINA TUFARO, LEELA KAPUR, JOSEPH BRAJEVICH, Julissa Salgueiro, and other counsel and parties;

iii. Any lawsuit where the City was a party to the lawsuit and appears to have had a legal, representational, and/or financial interest in both sides of the lawsuit, including the *Jones* matter;

iv. The litigation of the *Jones* matter and the *PwC* matter, including discovery disputes, the deposition of the City's "person most qualified," and emails and other materials arguably or allegedly responsive to discovery demands or court orders;

v. Efforts to conceal the litigation practices of the City Attorney's Office's or members or representatives thereof in the litigation related to the LADWP billing system, including knowledge or direction of payments made or benefits

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

given to individuals or entities in an effort to discourage their revelation of those practices;

vi. Efforts to conceal actions by the City Attorney's Office or members or representatives thereof in the litigation related to the LADWP billing system, including shielding documents from production, filing false or misleading documents with the court, and offering false or misleading testimony;

vii. The City's actions, strategy, or tactics in responding to revelations or allegations of fraud, discovery violations, and unethical conduct in the litigation related to the LADWP billing system, including media outreach and contacts, litigation decisions, notification or lack of notification to the court of relevant developments, authorization of payment of hush money, and other actions;

viii. Negotiations or agreements relating to hush money payments offered to or solicited by any individual or entity to conceal business practices related to the LADWP billing litigation by the City Attorney's Office or members thereof, and communications relating thereto;

ix. Obstruction of justice, perjury, or false official statements related to the LADWP billing litigation;

x. Destruction or concealment of evidence related to the LADWP billing litigation.

c. Calendar or date book entries and notes, including calendars or date books stored on digital devices;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

d. All records and information described above in Section II.15.b.

IV. PROVIDER PROCEDURES

17. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. The PROVIDER shall send such information to:

18. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

19. IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 2705(b), that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A, of the existence of the warrant, until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date this warrant is signed by the magistrate judge or such later date as may be set by the Court upon application for an extension by the United States. Upon expiration of this order, at least ten business days prior to disclosing the existence of the warrant, the PROVIDER shall notify the filter attorney identified above of its intent to so notify.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AFFIDAVIT

I, Andrew Civetti, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since September 2015. I am currently assigned to a Public Corruption Squad, where I specialize in the investigation of corrupt public officials, including bribery, fraud against the government, extortion, money laundering, false statements, and obstruction of justice. In addition, I have received training in the investigation of public corruption and other white collar crimes.

2. I am currently one of the agents assigned to an investigation of alleged corrupt activities at the Los Angeles Department of Water and Power ("LADWP") and the Los Angeles City Attorney's Office ("City Attorney's Office"). As discussed in more detail herein, these activities include the following criminal schemes, among others:

a. Collusive litigation practices related to lawsuits involving the City Attorney's Office and LADWP, which were fueled in at least one instance by a $2.175 million kickback from plaintiff's attorney JACK LANDSKRONER to attorney PAUL PARADIS, a Special Counsel retained by the City Attorney's Office.

b. The concealment of an $800,000 hush-money payment to a prospective whistleblower by Special Counsels PARADIS and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

PAUL KIESEL in exchange for silence as to collusive and potentially fraudulent litigation practices involving PARADIS, KIESEL, and THOMAS PETERS, then the Chief of Civil Litigation at the City Attorney's Office, among others.

3. I am aware that the City receives in excess of $10,000 annually in federal funds through various programs.

II. PURPOSE OF AFFIDAVIT

4. I make this affidavit in support of applications for search warrants to Apple, Inc., Google, Inc., and Microsoft Corporation for the seizure of information associated with the following accounts (collectively, the "**TARGET ACCOUNTS**"):

Apple, Inc. Accounts

a. The Apple iCloud account,[1] [redacted], associated with the phone number [redacted] and the name MIKE FEUER ("**FEUER's ACCOUNT**");

b. The Apple iCloud account, [redacted], and Apple iCloud account, joseph.brajevich@ladwp.com, associated with the phone number [redacted] and the name JOSEPH BRAJEVICH ("**BRAJEVICH's ACCOUNT**");

[1] According to Apple's website, "iCloud stores your content securely and keeps your apps up to date across all your devices. That means all your stuff—photos, files, notes, and more—is safe and available wherever you are. iCloud comes with 5 GB of free storage and you can add more storage at any time." Based on my review of Apple's website and my review of Apple subscriber information, I understand that phone numbers are linked to iCloud Accounts to secure and retrieve data. Specifically, the use of iCloud with an Apple device and associated phone number may have content capturing an individual's utilization of that device.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

c. The Apple iCloud account associated with the phone number [redacted] and the name JAMES CLARK ("**CLARK's ACCOUNT**");

Google, Inc. Accounts

d. Mike.Feuer@lacity.org ("**FEUER's EMAIL**");

e. Leela.Kapur@lacity.org ("**KAPUR's EMAIL**");

Microsoft Corporation Account

f. Joseph.Brajevich@ladwp.com ("**BRAJEVICH's EMAIL**").

5. Apple Inc. ("PROVIDER #1") is a provider of electronic communication and remote computing services, headquartered at Cupertino, California. Google, Inc. ("PROVIDER #2") is a provider of electronic communication and remote computing services, headquartered at Mountain View, California. Microsoft Corporation ("PROVIDER #3") is a provider of electronic communication and remote computing services, headquartered at Redmond, Washington (collectively, the "PROVIDERS").[2]

---

[2] Because this Court has jurisdiction over the offenses being investigated, it may issue the warrant to compel the PROVIDERS pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). See 18 U.S.C. §§ 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction") and 2711 ("the term 'court of competent jurisdiction' includes -- (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that -- (i) has jurisdiction over the offense being investigated; (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title").

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

6. The information to be searched is described in Attachments A-1 through A-3. This affidavit is made in support of applications for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A) and 2703(d)[3] to require the PROVIDERS to disclose to the government copies of the information (including the content of communications) described in Section II of Attachment B. Upon receipt of the information described in Section II of Attachment B, law enforcement agents and/or individuals assisting law enforcement and acting at their direction will review that information to locate the items described in Section III of Attachment B subject to the search protocol and potential privilege review procedures outlined in Attachment B. Attachments A-1 through A-3 and Attachment B are incorporated herein by reference.

7. As described more fully below, I respectfully submit there is probable cause to believe that the information associated with the **TARGET ACCOUNTS** constitutes evidence, contraband, fruits, or instrumentalities of criminal violations

---

[3] The government is seeking non-content records pursuant to 18 U.S.C. § 2703(d). To obtain the basic subscriber information, which do not contain content, the government needs only a subpoena. See 18 U.S.C. § 2703(c)(1), (c)(2). To obtain additional records and other information--but not content--pertaining to subscribers of an electronic communications service or remote computing service, the government must comply with the dictates of section 2703(c)(1)(B), which requires the government to supply specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation in order to obtain an order pursuant to 18 U.S.C. § 2703(d). The requested warrant calls for both records containing content as well as subscriber records and other records and information that do not contain content (see Attachment B).

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding) (collectively, the "Target Offenses").

8. The facts set forth in this affidavit are based upon my personal observations, my training and experience, information obtained from other agents and witnesses [redacted], consensually recorded conversations, and information obtained from the prior related search warrants, as detailed further below. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

9. On September 12, 2019, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized two search warrants (19-MJ-3813 and 19-MJ-3814) for PETERS's residence and person to seize PETERS's cell phone (collectively, the "September 2019 search warrants"). On July 18, 2019, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized two search warrants (19-MJ-2915 and 19-MJ-2923) for the seizure of information associated with nineteen e-mail accounts from two Internet Service Providers, and six search warrants (19-MJ-2913,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

19-MJ-2914, 19-MJ-2917, 19-MJ-2919, 19-MJ-2920, and 19-MJ-2922) for the premises of sixteen locations (collectively, the "July 2019 search warrants"). All of the July 2019 search warrants were supported by a single omnibus affidavit (the "omnibus affidavit"). The September 2019 and July 2019 search warrants and their supporting omnibus affidavit are incorporated herein by reference, and copies can be made available for the Court.[4]

III. BACKGROUND ON SUBJECTS

10. MICHAEL FEUER is the City Attorney for the City of Los Angeles. On July 22, 2019, during the execution of a search warrant at the City Attorney's Office, FEUER provided a voluntary interview, portions of which are detailed herein.[5] Thereafter, FEUER provided certain additional information to the prosecution team via telephone or in person, either directly or

---

[4] In addition, on April 18, 2019, the Honorable Jacqueline Chooljian, United States Magistrate Judge, authorized search warrants relating to the Los Angeles Department of Water and Power's then General Manager, DAVID WRIGHT. Specifically, these warrants authorized search warrants for WRIGHT's phone, WRIGHT's laptop, two of WRIGHT's email addresses, and two of WRIGHT's Apple iCloud accounts (collectively, the "April 2019 search warrants"). On June 4, 2019, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized search warrants for two of WRIGHT's residences, WRIGHT's office, WRIGHT's cellular phone, and a burner cellular phone that the FBI had surreptitiously provided to WRIGHT, as well as for an e-mail account used by Deputy Los Angeles City Attorney JAMES CLARK; on June 18, 2019, Judge Walsh authorized a subsequent search warrant for WRIGHT's Riverside residence (collectively, the "June 2019 search warrants"). The April 2019 and June 2019 search warrants and their supporting affidavits are also incorporated herein by reference, and copies can be made available for the Court.

[5] For all interviews and proffer sessions detailed herein, I either attended the interview myself or received information from another FBI agent who attended.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

via his Chief of Staff, LEELA KAPUR. [redacted] FEUER has indicated to the government that he had plans to run for Mayor of Los Angeles in 2022 and he believed he would be among the favorites.

a. Based on my review of Apple iCloud subscriber information which registered **FEUER's ACCOUNT** to FEUER's phone number [redacted]), my review of PETERS's phone, including messages with FEUER at [redacted] my review of subscriber records for [redacted] and FEUER's use of [redacted] to contact the prosecution team relating to the investigation, I believe that FEUER uses **FEUER's ACCOUNT.**

b. Based on my review of e-mail records, I believe FEUER uses **FEUER's EMAIL.**

11. LEELA KAPUR is the Chief of Staff to FEUER.

a. Based on my review of PETERS's phone, I believe KAPUR uses the telephone number [redacted] Based on my review of e-mail records, I believe KAPUR uses **KAPUR's EMAIL.**

12. JOSEPH BRAJEVICH is an Assistant City Attorney and the General Counsel for LADWP.

a. Based on my review of Apple iCloud subscriber information which registered **BRAJEVICH's ACCOUNT** to BRAJEVICH's phone number ([redacted] my review of PETERS's phone, including messages with BRAJEVICH at [redacted] and

---

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

BRAJEVICH's use of [redacted] to contact the prosecution team about the investigation, I believe that BRAJEVICH uses **BRAJEVICH's ACCOUNT.**

b. Based on my review of e-mail records, I believe BRAJEVICH uses **BRAJEVICH's EMAIL.**

13. JAMES CLARK is the Deputy Chief for the Los Angeles City Attorney and a retired partner with Gibson, Dunn & Crutcher, LLP ("Gibson Dunn"). On November 7, 2019, CLARK submitted to a voluntary interview with the prosecution team in the presence of his attorneys and pursuant to a written proffer agreement.[7]

14. Based on my review of PETERS's phone, including messages with CLARK at [redacted] I believe that CLARK uses **CLARK's ACCOUNT.**

15. THOMAS PETERS was the Chief of Civil Litigation at the City Attorney's Office. On or about March 22, 2019, PETERS resigned from that position. PETERS has requested immunity from the government pursuant to 18 U.S.C. § 6001 et seq., as well as other protections and/or recommendations with respect to prospective investigations or actions by other authorities. The government continues to consider those requests and has neither acted on them nor made representations as to whether or not they will be granted. On January 28, 2019, the government

[7] Under the terms of the proffer sessions discussed herein, the government is allowed to make derivative use of the information provided to it. The government agrees only not to use the information against the provider of the information in the government's case-in-chief against that person, provided the person is entirely truthful in proffer sessions.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

interviewed PETERS in the presence of his attorneys and pursuant to a proffer agreement.

15. PAUL PARADIS is an attorney and partner at Paradis Law Group, PLLC, operating in New York and Los Angeles. At relevant times between 2015 and March 2019, PARADIS acted as Special Counsel for the City in a civil lawsuit against PricewaterhouseCoopers ("PwC") regarding an alleged faulty billing system, (Superior Court of California, captioned *City of Los Angeles v. PricewaterhouseCoopers*, Case No. BC574690 ("*PwC* case")).

a. I have interviewed PARADIS on numerous occasions regarding his involvement in the criminal schemes and Target Offenses detailed herein in the presence of his attorneys and pursuant to a proffer agreement. Much of the information provided by PARADIS has been substantially corroborated by other evidence, and other than the details provided in footnote 9 below, I do not have a reason to believe that PARADIS has provided untruthful information.

b. PARADIS has no criminal record and has agreed to assist the government in exchange for favorable consideration in a potential future prosecution of him related to his conduct in this matter.

c. PARADIS has provided the government access to his email account, cell phone, bank accounts, and many other documents relevant to the investigation. PARADIS has also made numerous consensual recordings at the request of the government, some of which are detailed in the omnibus affidavit.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_000725
Page 725 of 1425

16. GINA TUFARO was at relevant times a New York attorney and the law partner of PARADIS.

a. On June 19, 2019, I interviewed TUFARO in the presence of her attorney [redacted]

b. [redacted]

17. PAUL KIESEL, a Los Angeles-based attorney, was at relevant times a Special Counsel for the City Attorney's Office on litigation relating to the LADWP billing system.

a. The government has conducted voluntary interviews with KIESEL in the presence of his attorney, as detailed in pertinent part below. To date and to my knowledge, information proffered by KIESEL has largely been consistent with other evidence, with the possible exception of the information provided in footnote 9.[9]

[redacted]

[9] In the first part of January 2020, KIESEL informed me that he intended to contact PARADIS about litigation strategy for a federal civil lawsuit (related to the events detailed herein) in which KIESEL and PARADIS were named as defendants. PARADIS contacted me to inform me that KIESEL had contacted him before PARADIS returned the contact. At my direction, PARADIS did not record the contact. Both KIESEL and PARADIS also reported back to me on the contact. Their accounts varied slightly in the following respect:

PARADIS reported that during the course of the discussion about the federal civil lawsuit, KIESEL asked whether they had a

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. KIESEL has also voluntarily provided certain documentary information, including text messages, emails, and a handwritten entry from his diary.

18. JULISSA SALGUEIRO was previously employed as a paralegal by KIESEL until approximately July 2017. Salgueiro submitted to a voluntary interview with the prosecution team [redacted]

19. [redacted] is an attorney affiliated with KIESEL's law firm. On December 5, 2019, [redacted] submitted to a voluntary interview with the prosecution team.

20. [redacted] is a law partner of KIESEL's firm. On January 14, 2020, [redacted] submitted to a voluntary interview with the prosecution team.

21. DAVID WRIGHT was the General Manager of LADWP until his resignation or dismissal on or about July 23, 2019.

a. I have interviewed WRIGHT on several occasions, including one voluntary interview without counsel during the execution of a search warrant at his home in June 2019, and several additional voluntary interviews in the presence of his

---

conversation with PETERS in late January 2019 about documents requested by *PwC* (a situation described in further detail below). PARADIS told me that he did not provide a substantive answer to KIESEL, but that he attempted to jog KIESEL's memory by reminding him about a location significant to the conversation that PARADIS recalled. KIESEL reported that PARADIS answered his substantive question and told KIESEL that they did in fact have such a conversation with PETERS. I do not know whether this discrepancy is attributable to a misunderstanding between KIESEL or PARADIS, a lapse of memory by one of them, or an intentional misstatement by one of them. Based on my history of interactions with both and the lack of any apparent reason for either to lie about this issue, I suspect that it was either a misunderstanding or a memory lapse.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

counsel and pursuant to a proffer agreement. At various points, I believe that WRIGHT provided untruthful information in response to my questions.

22. ROBERT WILCOX is a press spokesman for the City Attorney's Office.

VI. PRESERVATION REQUESTS & SEARCH WARRANTS

23. On or about December 4, 2019, the government sent Google, Inc. a preservation letter for **FEUER** and **KAPUR EMAILS** and Microsoft Corporation a preservation letter for **BRAJEVICH's EMAIL.**

24. On or about December 6, 2019, the government obtained orders pursuant to 18 U.S.C. § 2703(d) for information associated with the **FEUER, BRAJEVICH,** and **KAPUR EMAILS.**

25. On or about January 8 and 9, 2020, the government sent Apple Inc. subpoenas, nondisclosure orders, and preservation letters for subscriber information associated with the **FEUER, BRAJEVICH,** and **CLARK ACCOUNTS.**

26. Other than what has been described herein to my knowledge, the United States has not attempted to obtain the contents of the **TARGET ACCOUNTS** by other means.

IV. SUMMARY OF PROBABLE CAUSE

A. FEUER's Knowledge of Hush Money, [redacted]

27. [redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

[redacted] the evidence provides probable cause to believe that at FEUER's implied direction, PETERS ordered KIESEL to confidentially settle Salgueiro's demands or face termination of his Special Counsel contract. Specifically, as detailed further below, PETERS informed the government that he advised FEUER of Salgueiro's threats and demands, ordered KIESEL to buy Salgueiro's silence in accordance with FEUER's perceived direction, and apprised FEUER after the hush-money settlement that the matter had been taken care of. This information is corroborated in part by information proffered by PARADIS and KIESEL, as well as by documentary evidence.

B. FEUER's Knowledge of Special Counsel's Collaboration with Opposing Counsel and Collusive Litigation by January 2019, [redacted]

28. Multiple sources of evidence provide probable cause to believe that FEUER obstructed justice, made materially misleading statements to the FBI, [redacted] relating to the timing of FEUER's knowledge that his Special Counsel (PARADIS and KIESEL) had collaborated with opposing counsel in a collusive lawsuit that allowed the City to settle multiple class actions on the City's preferred terms. Specifically, FEUER made official statements to the government [redacted] that I believe were intended to misleadingly indicate that

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

FEUER first learned about emails showing collaboration between Special Counsel and the City's opposing counsel on April 24, 2019, and that he immediately disclosed that information to the court, the City's litigation opponent, and the media. Based on my training, experience, and knowledge of the investigation, by misleadingly portraying FEUER's knowledge in this way, it appears FEUER was attempting to personally distance himself from this scandal likely for political gain (or to avoid political fallout).

29. However, the evidence indicates that PETERS apprised FEUER in as early as late January 2019 of the existence of those emails and the facts that they revealed. Specifically, as further detailed below, PETERS proffered that he told FEUER in late January 2019 about the emails and what they would show, that FEUER was very upset, that PETERS withheld them from discovery in the *PwC* matter at what he perceived to be FEUER's direction in order to conceal it from the court and the public, and that PETERS subsequently advised FEUER that FEUER no longer needed to worry about the documents being made public. This information is corroborated in part by a surreptitiously recorded phone call from January 27, 2019, wherein PETERS relayed to PARADIS, KIESEL, and TUFARO the substance of his initial contemporaneous conversation with FEUER. PETERS's proffer information is also partially corroborated by emails and calendar entries showing meetings between FEUER and PETERS related to the LADWP matters during the last week of January 2019, as well as with other evidence.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

V. STATEMENT OF PROBABLE CAUSE

25. The FBI is conducting an ongoing investigation into the City Attorney's Office and LADWP, including a suspected bribery-fueled collusive litigation settlement that allegedly defrauded LADWP ratepayers out of many millions of dollars, an $800,000 hush-money payment made in order to conceal those collusive litigation practices, and obstruction of justice [redacted] relating to this investigation. Background facts relating to these and other facets of the investigation are further detailed in the omnibus affidavit referenced above and incorporated herein. The case numbers associated with the search warrants supported by my omnibus affidavit are outlined above.

A. [redacted]

1. Salgueiro's Initial Threats to Reveal Information Related to the Collusive Litigation and Demands for Hush Money

26. As further detailed below, the evidence indicates that Salgueiro obtained certain documents from KIESEL's law firm, including but not limited to documents reflecting coordination between the City's Special Counsel and the plaintiff's counsel in the *Jones* lawsuit, and threatened to reveal the documents if KIESEL did not pay her a large amount of money.

27. KIESEL advised the government of the following information:[10]

[10] As noted below, some of this information is corroborated by a contemporaneous diary entry provided by KIESEL; which I have reviewed.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. Around August or September 2017, KIESEL was approached by Salgueiro, an employee that his law firm terminated in or around July 2017.

b. Salgueiro told KIESEL that she had taken certain documents from the firm, including some that showed the City's entanglement in the representation of an adverse party that had sued the City in the LADWP billing system litigation.

c. Salgueiro initially demanded $1,500,000 from KIESEL, or she would take the materials public.

d. KIESEL was not initially concerned about Salgueiro taking the materials public, because although they might be "embarrassing" to the City, he did not believe that they reflected any wrongdoing.

28. Salgueiro advised the government [redacted] as follows:

a. Before leaving KIESEL's employ, Salgueiro took certain documents from KIESEL's firm that she believed would show that the firm and the City conspired to represent both sides of the litigation in the *Jones v. City of Los Angeles* matter and in other matters, including unrelated cases and employment-related matters (collectively, the "Salgueiro documents").[11]

---

[11] Salgueiro provided to the government, [redacted], electronic files that she described as the documents that she took from KIESEL's firm and threatened to review. These documents were submitted directly to the government's privilege-review team, and I have since reviewed a redacted version. They comprise several folders in different case names, with the documents relevant to the *Jones* matter

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. After Salgueiro was fired by KIESEL in or around July 2017, she demanded a large sum of money, around $900,000, from KIESEL in order to return the Salgueiro documents, refrain from taking the Salgueiro documents public, and resolve certain employment discrimination and harassment complaints.

c. KIESEL countered Salgueiro's demand with a lower five-figure offer, using former Special Counsel PAUL PARADIS as a mediator.

29. PARADIS proffered to the government as follows:

a. Salgueiro took the Salgueiro documents when she left KIESEL's firm and threatened to reveal them if KIESEL did not pay her a large sum of money.

---

marked "Jones." The documents from the "Jones" folder include the following relevant representative items:

- An April 16, 2015 email from KIESEL directing Salgueiro to prepare a notice of related case in the *Jones* matter "as though it was coming from Michael Libman, counsel for Jones, and NOT coming from us."
- Screenshots of apparent metadata indicating Salgueiro's preparation of various pleadings for both LANDSKRONER and the City
- Documents showing that Salgueiro and the KIESEL law firm filed documents for LANDSKRONER and LIBMAN on behalf of plaintiff Jones (including the first amended complaint), paid associated filing fees, and otherwise coordinated plaintiff's counsel's work
- Timesheets showing that Salgueiro billed time for her work preparing, finalizing, and filing documents on behalf of plaintiff Jones

The remainder of the documents (the ones not in the "Jones" folder) as provided to the prosecution team after filtering are heavily redacted, and any relevance they may have to this investigation is not presently clear to me based on the current evidence.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. PARADIS believed that some of the documents related to the *Jones* matter, and others related to another matter wherein the City played both sides of litigation.

2. Awareness by FEUER, KAPUR, BRAJEVICH, CLARK, and PETERS of Salgueiro's Threats and Demands

30. Information from multiple sources, as detailed below, provides probable cause to believe that PETERS, acting at FEUER's implied direction, instructed KIESEL to pay the hush money that Salgueiro demanded to keep her from going public with her information, including information about secret collaboration between the City and plaintiff's counsel in the *Jones* case. The below information also constitutes probable cause to believe that BRAJEVICH and KAPUR were aware of the Salgueiro threats and demands and their context. The evidence further provides probable cause to believe that CLARK had some awareness of Salgueiro's threats to reveal sensitive documents relating to the *Jones* matter, although he may not have had a full understanding of the details.

a. KIESEL'S and PARADIS'S October 2017 negotiations with Salgueiro

31. On October 10, 2017, Salgueiro sent a text message, which I have reviewed, to PARADIS stating in pertinent part, "Hi Mr. P, I left a written message with Clark's asst. on Fri. re set up of mtg n didn't hear bk. 1. Okay 2 drop off set of docs w/note saying if w/like 2 discuss 2 call me?"

32. [redacted] in October 2017, she went to the City Attorney's Office to try to speak with CLARK, but he

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

was not there. According to Salgueiro, she left with CLARK's assistant a large envelope containing a copy of the Salgueiro documents, along with a message. [redacted].

33. As described below, the evidence indicates that KIESEL engaged in multiple initial attempts to negotiate with Salgueiro, which were unsuccessful due to KIESEL's unwillingness to pay an amount that Salgueiro was willing to accept.

34. KIESEL advised the government as follows:

a. KIESEL met with Salgueiro on October 30 or 31, 2017, in a meeting at LADWP headquarters coordinated by PARADIS, who was serving as a "mediator" between Salgueiro and KIESEL. An individual known as Rosa or "Mama Rosa" (later identified as Rosa Rivas) accompanied Salgueiro. At that time, Salgueiro demanded $900,000, in an offer that she said would remain open for 24 hours. KIESEL agreed to think about it and then countered with an offer of $60,000.

b. KIESEL then received a text message from Salgueiro that she would see him in CCW[12] on December 4, 2017, which KIESEL interpreted as a threat to publicize her information at the next-scheduled hearing in *City of Los Angeles v. PwC*, which was scheduled for that date in the Central Civil West courthouse.

35. PARADIS proffered the following relevant information:

[12] Central Civil West was at the time a Superior Court courthouse in Los Angeles, where the judge presiding over the *City of Los Angeles v. PwC* litigation was located.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. On October 30, 2017, PARADIS and KIESEL met with Salgueiro and "Mama Rosa" at the LADWP cafeteria in an attempt to "mediate" Salgueiro's demands. At the conclusion of the mediation session, KIESEL informed PARADIS that he was willing to pay Salgueiro $120,000 to prevent her from publicizing the Salgueiro documents. Through PARADIS, Salgueiro countered that offer with a demand for $900,000 that would be open for 24 hours. On October 31, 2017, KIESEL told PARADIS that he rejected Salgueiro's $900,000 demand and would now offer $60,000 instead. PARADIS texted this new offer to Salgueiro, who texted both PARADIS and KIESEL that she would "c u both Dec. 4 at 2pm at CCW."

36. I have reviewed text messages between KIESEL, PARADIS, and Salgueiro which are substantively consistent with the above-referenced information.

b. November meetings with PETERS about Salgueiro

37. PETERS proffered the following information:

a. PETERS learned about Salgueiro's threats and demands from PARADIS during an in-person meeting with PARADIS and likely TUFARO on approximately November 16, 2017, after the first failed mediation with Salgueiro at LADWP headquarters.

b. At that initial meeting, the following took place:

i. PARADIS informed PETERS about the details of Salgueiro's demands, including that Salgueiro had threatened to reveal 1) certain attorney work-product documents that she had

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

taken from KIESEL's office, which included the *Jones* v. *PwC* draft complaint that the City was actively seeking to shield from production; 2) emails showing the transmittal of documents showing cooperation and coordination between the City and Jones' counsel (LANDSKRONER); 3) information that Salgueiro herself had filed the *Jones* lawsuit against the City (on behalf of KIESEL); and 4) other unidentified documents implicating cases involving the City.

ii. PETERS learned that KIESEL had engaged in a failed attempt to mediate Salgueiro's demands, and that this "mediation" had taken place at LADWP headquarters. PETERS felt that it was improper for the mediation to take place on City property.

iii. PETERS was "livid" to learn about the situation. He was particularly upset that KIESEL had not told him about Salgueiro's threats and demands, which PETERS felt that he had a need and a right to know.

iv. PETERS, PARADIS, and TUFARO agreed that they needed to have a discussion with KIESEL to talk about Salgueiro's threats and demands.

v. PETERS wanted to "impress on KIESEL the gravity of the situation."

vi. PARADIS told PETERS that KIESEL was not taking the situation seriously. PARADIS urged PETERS to be blunt in discussing the situation with KIESEL.

vii. PARADIS told PETERS that he "felt like a narc" for "ratting KIESEL out" and sharing this information with

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

PETERS without KIESEL's knowledge. PARADIS asked PETERS to "cloak" the fact that PARADIS was the source of the information. PETERS agreed to do so.

c. On November 17, 2017, PETERS sent KIESEL a series of text messages demanding that KIESEL come to his office immediately. KIESEL and PARADIS came to PETERS's office that day. At that November 17, 2017 meeting, the following occurred:

i. PETERS "read the riot act" to both KIESEL and PARADIS about the Salgueiro situation. PETERS included PARADIS to "cloak" the fact that he had learned the information from PARADIS, pursuant to PARADIS's request.

ii. PETERS asked KIESEL how KIESEL could not have shared the information with PETERS earlier. PETERS said that both PETERS and FEUER had a need and a right to know about Salgueiro's threats and demands, because this was an issue that could result in negative press coverage for the City Attorney's Office.

iii. PETERS, KIESEL, and PARADIS discussed the merits of Salgueiro's threats and demands, including the fact that Salgueiro was threatening to reveal documents relating to the *Jones* matter and other City litigation if KIESEL did not pay her money. PETERS recalled learning that Salgueiro was seeking "millions of dollars" from KIESEL.

iv. KIESEL was resistant to the idea of paying Salgueiro what she was asking. KIESEL told PETERS that he planned to hire a crisis-management person, an action that

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

PETERS considered ancillary to the City's more pressing concerns.

v. PETERS strenuously imparted to KIESEL that it was in his best interest to pay Salgueiro what she was asking to ensure that she did not make her information public.

vi. PETERS told KIESEL that if he did not take care of the situation, KIESEL would not be able to continue representing the City.

d. PETERS understood that Salgueiro had certain employment-related claims that she would agree not to pursue if KIESEL paid her to get the documents back. From PETERS's experience and his knowledge of Salgueiro, specifically her age, gender, ethnicity, termination after a medical leave for an allegedly work-related injury, and length of employment, PETERS believed that Salgueiro's employment claims might present a litigation risk for KIESEL.[13]

---

[13] Based on information provided by PETERS, KIESEL, PARADIS, and Salgueiro, I understand that Salgueiro was prepared to allege employment claims that included: 1) her termination after a lengthy medical leave; 2) unfulfilled promises that she believed KIESEL had made, including to pay for her to attend law school; and 3) KIESEL's general harsh or demanding treatment of her throughout her employment.

Based on that information and other information described herein, it is my belief that Salgueiro's threat to bring an employment lawsuit against KIESEL might have conferred a credible litigation risk to KIESEL and his firm. However, I further believe that such a lawsuit would not have been substantially damaging to the City. I also believe that the City's primary or sole concern in seeking to convince KIESEL — who was reluctant to pay and willing to risk public revelation of all the information — to pay to resolve Salgueiro's claims, was a desire to conceal the documents concerning the City's collaboration with Jones.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

e. PETERS viewed Salgueiro's demands as creating a "crisis situation" for himself and for the City Attorney's Office. PETERS believed that if the Salgueiro information were revealed, it would not only be embarrassing for the City Attorney's Office, but it would also implicate the candor of the process by which the *Jones* settlement had been approved. PETERS believed that the revelation of previously undisclosed cooperation between PARADIS/KIESEL and LANDSKRONER in the preparation of a complaint to sue the City could imperil the *Jones* settlement, including by providing objectors to the settlement with a foundation to reopen the objections that they had already unsuccessfully raised.

38. During CLARK's proffer, he advised the government that he was not familiar with any threats to reveal documents or information relating to the collusive litigation or demands for hush money, and that he did not recall ever receiving any such documents, information, or contacts. CLARK further advised that such events would have been significant and memorable in his opinion, and that he believed he would have recalled them if he observed them.[14]

---

[14] Multiple witnesses, including FEUER and CLARK, have advised that CLARK suffered from [redacted] during a period that included 2017 and 2018, which affected CLARK's functionality at work and culminated with a medical leave during late 2018 and early 2019 while he received [redacted]. CLARK advised the government that his [redacted] problem was resolved by February 2019, when he recommenced work. However, during the July 22, 2019 court-authorized search of CLARK's office, the FBI found approximately [redacted] hidden throughout CLARK's small office space. The government immediately advised FEUER of

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

39. Based on the foregoing and my knowledge of the investigation, I believe that CLARK, at some point, had some awareness of Salgueiro's threats, but may not have had a full understanding of the scope of the information that Salgueiro was threatening to reveal. I further believe that CLARK delegated handling of this situation to PETERS with an express directive that it be taken care of.

40. KIESEL advised the government as follows:

a. On November 17, 2017, KIESEL received a series of text messages from PETERS demanding that KIESEL come to see him immediately.[15]

b. KIESEL left a court proceeding in Orange County to drive to PETERS's office at City Hall East in Los Angeles, where he and PARADIS met with PETERS.

c. During that meeting, PETERS was visibly angry and told KIESEL to make the problem go away or KIESEL and PARADIS would be fired. PETERS told KIESEL and PARADIS that Salgueiro

that discovery. [redacted]

[15] I have reviewed text messages between PETERS and KIESEL on that date that corroborate this information.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

had called the City Attorney's Office asking to speak with FEUER, that FEUER had not taken the call, and that the call was routed to CLARK, who re-routed the call to PETERS and directed him to handle it. KIESEL further advised that his sense was that CLARK did not have a full awareness of the situation, and that KIESEL did not recall any in depth conversations with CLARK about Salgueiro.

d. During the meeting, PETERS told KIESEL to do "whatever it takes" and "whatever it costs," which KIESEL understood as a directive to pay whatever Salgueiro was asking to buy her silence.

e. KIESEL believed that Salgueiro had a "legitimate severance demand" based on her employment with him. However, KIESEL did not see any issues with the prospect of the Salgueiro documents being publicly revealed, because the City was fully aware of what those documents contained, and KIESEL did not think they would make the City look bad.

f. KIESEL was reluctant to pay what Salgueiro was asking, but he did not want to be fired from the Special Counsel role, particularly after investing substantial time and resources into the case of *City of Los Angeles v. PwC* over approximately three years without any compensation (because the Special Counsel contract provided for compensation for KIESEL and PARADIS only on a contingency-fee basis). KIESEL had by that time spent approximately a quarter million dollars of his own money on costs associated with the case, which contributed to his desire to remain on the case to recoup that investment.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

g. KIESEL could not recall whether PETERS told him that FEUER was aware of Salgueiro's threats and demands, but he believed that PETERS and CLARK would have told FEUER. Based on the circumstances and relationships that KIESEL observed, he "could not imagine" that CLARK and PETERS would not have told FEUER about this situation, because they were "good soldiers" to FEUER.

41. KIESEL further advised the government that after the aforementioned meeting wherein PETERS threatened to fire him, he subsequently met with PETERS again, and that PETERS had calmed down. At that time, PETERS indicated that he would not terminate the contract, and that they would see what happened.

42. KIESEL advised the government that since approximately 1980, he has regularly kept a handwritten diary on noteworthy events in his life. KIESEL showed the government (and provided a copy of) an entry in his diary that was dated December 1, 2017, that appears to recount KIESEL's recollection of the above-described November 2017 meeting in which PETERS called KIESEL up from Orange County to discuss Salgueiro's threat. According to the entry, which described PETERS as "spitting MAD" (emphasis in original), PETERS told KIESEL, "How could you not tell me about this threat, Paul??" The entry further reports, "Thom [PETERS] said you have 2 choices. Either settle with J [Salgueiro] or your FIRED!" (emphasis in original).

43. The above-described diary entry provided by KIESEL dated December 1, 2017, further related KIESEL's efforts to address and resolve Salgueiro's demands following his meeting

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

with PETERS. It then stated as follows: "Last Wed [November 29, 2017], I met, again, with Thom [PETERS] + laid all of this out and thankfully he understood + indicated he would not terminate us + we'll see how things develop."

44. I believe that the contemporaneous information from KIESEL's handwritten diary related herein is consistent with the information provided herein and other evidence described herein as to events surrounding Salgueiro's threat.

45. PARADIS proffered the following relevant information:

a. After Salgueiro's warning that she would see them at the *PwC* hearing, PARADIS grew concerned that the situation with Salgueiro was "rapidly escalating out of control" and that PETERS needed to be apprised of the details.

b. On November 6, 2017, PARADIS left a voicemail for PETERS advising that there were a couple of matters they needed to discuss and asking to meet.[16]

c. On November 16, 2017, PARADIS and TUFARO met with PETERS in PETERS's office and informed PETERS of the status of the Salgueiro situation, including that she was threatening to reveal documents relating to her employment-related claims as well as documents showing potential conflicts in the *Jones* case and other cases. PARADIS related the following relevant information about that meeting:

i. PETERS described CLARK's involvement in the Salgueiro matter, as detailed above.

[16] PETERS's phone does not reflect such a voicemail on that date; rather, it reflects a text message from PARADIS asking for a meeting with PETERS.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

ii. PETERS discussed the merits of Salgueiro's employment claims and noted that he had witnessed first-hand KIESEL's treatment of Salgueiro when PETERS worked at KIESEL's firm.

iii. PETERS stated that KIESEL had been primarily responsible for PETERS's wife being appointed as a Superior Court judge, because KIESEL had exerted his influence in the selection process. PETERS further shared his goal to also be appointed as a judge after leaving the City Attorney's Office, and he stated that he was aware of KIESEL's influence over that process as a member of the Governor's Committee that recommended candidates for judgeships, which was a factor in PETERS wanting the matter resolved promptly without becoming public.

iv. PETERS and PARADIS discussed a variety of approaches and then agreed that PETERS should text KIESEL the following morning to tell KIESEL that PETERS urgently wanted to see him in his office. They further agreed that KIESEL should not be informed that PETERS and PARADIS had met on November 16, 2017. At PARADIS's urging, they also agreed that PETERS should "take a very stern approach" with KIESEL, demand that he resolve the situation with Salgueiro, and threaten KIESEL with termination as Special Counsel if he did not do so. They did not discuss invoking FEUER's name as part of such an approach.

d. After their meeting on November 16, 2017, PETERS called PARADIS that evening to further discuss the planned conversation with KIESEL.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

e. On the morning of November 17, 2017, PARADIS left a voicemail for PETERS and subsequently received a call back from PETERS. PETERS stated that he was going to text KIESEL and PARADIS as they had previously discussed.[17]

f. Later that day, PARADIS and KIESEL met with PETERS in PETERS's office. During that November 17, 2017 meeting, the following took place:

i. PETERS did not disclose to KIESEL that he had met with PARADIS and TUFARO the day before about the Salgueiro matter.

ii. According to PETERS, he had learned from CLARK that CLARK had received from Salgueiro a package and two phone calls requesting a meeting. PETERS relayed that CLARK had advised him as follows: [18]

(I) CLARK was "fucking pissed" about the fact that Salgueiro had brought this to CLARK's attention, and CLARK had not responded because he did not intend to meet with Salgueiro.

(II) CLARK told PETERS that he wanted KIESEL's situation with Salgueiro resolved so that it did not become public.

---

[17] According to the phone records, PETERS had already begun texting KIESEL by the time PARADIS said that he had this conversation with PETERS.

[18] PETERS proffered that he could not remember discussing the Salgueiro matter with CLARK before the settlement was paid, but did specifically remember a conversation with CLARK about it after the matter was resolved.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

(III) CLARK asked PETERS what Salgueiro was complaining about specifically, and PETERS explained to CLARK that Salgueiro was complaining about KIESEL "having been on both sides of several cases" related to the approximately six cases reflected in the documents that Salgueiro had provided in her package to CLARK.

(IV) PETERS stated his understanding that at least two of the cases on which Salgueiro was threatening to reveal information were litigation with the City, and that one was the *Jones v. City* case.

iii. PETERS advised that he had already informed FEUER about this situation. PETERS stated that FEUER was extremely unhappy about it, and that if it was not immediately cleaned up, KIESEL's firm, and probably PARADIS's firm too, would be terminated as Special Counsel to the City in the *PwC* case.

iv. KIESEL was resistant and stated that Salgueiro was unreasonable, that he was not prepared to pay her $900,000, and that he viewed her threats as extortion.

v. PETERS stated that while he understood Salgueiro was demanding a large amount of money, PETERS, FEUER, and CLARK had no choice but to demand that KIESEL work out a deal with Salgueiro to pay her because the City Attorney's Office could not tolerate this situation becoming public.

vi. PETERS ended the meeting by firmly directing KIESEL to work out a deal with Salgueiro to buy her silence and ensure that her information did not become public. PETERS also

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

again made clear that if KIESEL did not comply quickly, he, and likely PARADIS also, would be terminated.

46. PARADIS proffered that after the November 17, 2017 meeting, KIESEL left, and PETERS stopped PARADIS on the way out to instruct PARADIS to reiterate to KIESEL what was going to happen if KIESEL did not agree to pay Salgueiro off. PARADIS indicated that he would do so.

47. PARADIS proffered that at the time of the November 17, 2017 meeting, PARADIS was unsure as to whether PETERS had truly informed FEUER about Salgueiro's threats, or whether that was simply a tactic that PETERS was using to try to convince KIESEL to comply. However, PARADIS did not think that PETERS would take the actions he did without apprising FEUER, because PETERS was afraid of FEUER and would have wanted to "cover his ass."[19]

c. PETERS's November discussions with FEUER and BRAJEVICH about Salgueiro's threats and demands

48. PETERS proffered that at some point after the aforementioned November 17, 2017 meeting and before December 1, 2017, PETERS spoke with FEUER as another meeting was breaking up. PETERS provided the following relevant information as to that conversation:

a. PETERS did not specifically recall whether anyone else was present during this conversation, but he believed that

[19] As noted below, PARADIS proffered that PETERS later confirmed to him that he in had in fact informed FEUER about Salgueiro's threats and demands.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

KAPUR was probably present, and that Robert Wilcox (FEUER's media spokesman) might have been there as well.

b. During this conversation, PETERS told FEUER that a disgruntled former employee of KIESEL's was threatening to reveal documents including the draft *Jones v. PwC* complaint, which FEUER was then aware was the subject of a contested motion to compel in the *PwC* case, as well as other documents showing cooperation and coordination between PARADIS and Jones' counsel (JACK LANDSKRONER) before the *Jones* complaint was filed that had not previously been disclosed to PwC or the court. According to PETERS, FEUER was already aware that there had been some cooperation between PARADIS and the plaintiff's counsel.

c. PETERS advised FEUER that the former employee seemed irrational, was being guided by a "guru," and was "holding the City hostage" by threatening to reveal these documents, which PETERS characterized as the City's attorney work product.

d. PETERS provided this information as a "heads up" to FEUER, as PETERS knew that FEUER always wanted to be made aware of matters that might be reported in the press.

e. FEUER was upset by this information and questioned how KIESEL could have let this happen.

f. It was apparent to PETERS that FEUER, whom PETERS characterized as "a very smart man," immediately saw the risk to the City inherent this situation.

g. PETERS assured FEUER that PETERS was monitoring the situation.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

49. PETERS proffered that on November 30, 2017, PETERS received a call from BRAJEVICH, and they spoke on the phone.[20] PETERS had not told BRAJEVICH about the Salgueiro situation, but BRAJEVICH already had some awareness of it, including the fact that KIESEL and PARADIS had attempted to mediate the dispute with Salgueiro at LADWP headquarters. PETERS proffered the following with respect to that conversation:

a. BRAJEVICH asked PETERS how much PETERS knew about the Salgueiro situation, and PETERS gave BRAJEVICH some details about her threats and demands.

b. PETERS told BRAJEVICH that he was scheduled to discuss the issue with FEUER the following day (Friday, December 1, 2017), and he invited BRAJEVICH to join that discussion.

c. PETERS believed that BRAJEVICH needed to be involved in the discussions about Salgueiro's threats and demands, for two reasons. First, BRAJEVICH was effectively supervising KIESEL's and PARADIS's work on the matter to which Salgueiro's threats related. Second, LADWP headquarters, where the failed "mediation" had taken place, was BRAJEVICH's "domain" (as LADWP General Counsel).

d. The December 1, 2017 meeting with FEUER, KAPUR, BRAJEVICH, and PETERS about Salgueiro

---

[20] I have reviewed an email from this date to PETERS from his secretary requesting that PETERS call BRAJEVICH. As described below, a subsequent meeting invitation indicates that BRAJEVICH was scheduled to telephonically join a previously scheduled December 1, 2017 meeting with FEUER, KAPUR, and PETERS on the *PwC* case.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

50. PETERS proffered that on Friday, December 1, 2017, PETERS participated in a scheduled meeting with FEUER, KAPUR, and BRAJEVICH (called in) to provide an update on the Salgueiro situation.[21] PETERS proffered the following information about this December 1 meeting:

a. The Salgueiro situation — which PETERS described as "the issue du jour" at that time, in light of Salgueiro's looming threat to appear at the Monday, December 4 hearing — was the primary or sole focus of that planned meeting.

b. The meeting took place at the end of the day in FEUER's office.

c. BRAJEVICH was not present in person but instead called in to the meeting to participate by telephone.

d. PETERS provided an "update on the state of play" of the Salgueiro situation, including that Salgueiro still had the documents showing cooperation between the City and Jones, and that Salgueiro had threatened to appear at the hearing set for Monday, December 4, 2017.

e. The participants discussed the likelihood that if Salgueiro appeared at the hearing, she would try to file or give the documents.

---

[21] As noted herein and detailed below, I have reviewed a calendar entry for FEUER and a meeting invitation reflecting this meeting from 4:45 p.m. to 5:00 p.m. PETERS proffered that he could not recall whether anyone else attended this meeting. He opined that FEUER's press spokesman, Rob Wilcox, "would have been there" if available. PETERS also stated that [redacted], FEUER's Chief of Intergovernmental Relations, might also have attended. As noted herein, documents reflecting the scheduling of this meeting do not indicate that either Wilcox or [redacted] was invited.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

f. The participants discussed the possibility that Salgueiro would invite the press to attend the hearing in order to publicize the information to the media.

g. FEUER and BRAJEVICH expressed frustration that KIESEL had not been able to take care of the problem and reach an "accommodation" with Salgueiro.

h. FEUER stated that KIESEL needed to do whatever needed to be done to take care of the situation.

i. Accordingly to PETERS, it was "absolutely clear" and understood by all participants at this meeting that Salgueiro was demanding money from KIESEL in exchange for the return of the documents.

j. PETERS told FEUER that he would personally attend the Monday hearing, in light of Salgueiro's threat to show up. FEUER did not ask PETERS to attend the hearing, but PETERS preemptively offered because he knew from his prior experience with FEUER that this was what FEUER would want.

k. FEUER conveyed that he was confident that PETERS could handle the situation.

l. Both FEUER and BRAJEVICH expressed the view that it was outrageous that the "mediation" had happened on City property.

51. According to an electronic calendar entry, there was a scheduled meeting regarding the *PwC* case between FEUER, KAPUR, PETERS, and BRAJEVICH on December 1, 2017, from 4:45 p.m. to 5:00 p.m. The meeting notice specified that BRAJEVICH would be participating by phone.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

52. In a text message on December 1, 2017, at 5:07 p.m., using **BRAJEVICH's ACCOUNT**, BRAJEVICH said to PETERS, "Thom- when you have a chance **I want to follow on the fact that the mediation took place at DWP.** Not urgent and can wait until Monday. Thanks and have a great weekend." Metadata from PETERS' phone indicates that PETERS opened this message at 9:19:10 p.m on that same date.

a. PETERS proffered that he understood this to refer to KIESEL's attempted "mediation" with Salgueiro on LADWP property, which he and BRAJEVICH and others had discussed in the aforementioned meeting that afternoon.

53. In a text message on December 1, 2017, at 9:18:57 p.m., PETERS told PARADIS, "**Mike is not firing anyone at this point. But he is far from happy about the prospect of a sideshow. Also, mediating Paul's matter at DWP, not a popular move.** We can speak over the weekend. Thanks."[22]

a. PETERS has informed the government that this message meant to convey that FEUER had considered and then rejected the idea of firing PARADIS and KIESEL, but that FEUER considered the threatened release of documents by SALGUEIRO to be a prospective "sideshow" that would impair both the litigation and the reputation of FEUER's office. The "sideshow" was a reference to media attention.

[22] Based on my general knowledge of text messaging services, I am aware that a user receiving a text message can often see a banner containing part or all of a message without opening the message. Based on the sequence of events and timing of these messages, I believe PETERS may have viewed BRAJEVICH's message via such a banner, sent the related message to PARADIS, and then opened BRAJEVICH's message in order to reply to it.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

54. Based on my knowledge of the investigation and the above-described information and timeline, I believe that the "mediation at DWP" discussed in the BRAJEVICH-PETERS and PETERS-PARADIS texts, both from December 1, 2017, referenced KIESEL's unsuccessful attempts to negotiate Salgueiro's demands for hush money, as directed by PETERS at FEUER's implied direction.

55. I further believe that BRAJEVICH's message to PETERS -- which BRAJEVICH sent seven minutes after his meeting with FEUER, KAPUR, and PETERS about the *PwC* matter was scheduled to end, and which asked to "follow on the fact that the mediation took place at DWP" -- suggests that this topic of KIESEL's dispute with Salgueiro and its bearing on the City's interest in the *PwC* case was likely discussed at that meeting. This belief is supported by the language selected by BRAJEVICH. In particular, I believe that BRAJEVICH's request indicated his intent to "follow on" an existing discussion. Moreover, BRAJEVICH's lack of any explanation or background as to what "mediation" he meant suggests to me that BRAJEVICH and PETERS had recently discussed this topic. Finally, I note the fact that his text message identifies two separate but related issues, likely from the meeting: (1) the "sideshow" and (2) "also" the location of the "mediation."

56. PETERS proffered that in one of his multiple conversations with FEUER about the Salgueiro situation, FEUER questioned whether KIESEL should be fired for allowing this to happen, but FEUER ultimately did not decide to terminate KIESEL or PARADIS.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

57. PETERS proffered that in one of his multiple conversations with FEUER about the Salgueiro situation before the settlement, PETERS believed that he conveyed to FEUER that Salgueiro was "looking for seven figures," meaning that Salgueiro was demanding a million dollars or more.

e. *Settlement of Salgueiro's demands on December 4, 2017*

58. Information from multiple witnesses and documents indicate that on December 4, 2017, Salgueiro made good on her above-described threat to appear at a court hearing in the PwC matter and attempted to provide copies of the Salgueiro documents both to the court and to the counsel for PwC. The evidence provides probable cause to believe that after Salgueiro showed up in court and attempted to provide her documents to the court and PwC's counsel in the presence of PETERS, PETERS directed KIESEL to settle with Salgueiro and was later informed that KIESEL had done so by paying $800,000 in hush money.

59. [redacted]

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

62. PETERS, KIESEL, and PARADIS each (separately) advised the government substantively as follows:

a. PETERS, KIESEL, and PARADIS all attended the aforementioned *PwC* hearing in the LADWP billing litigation.[24]

b. At or after the hearing, Salgueiro approached [redacted] which PETERS, KIESEL, and PARADIS interpreted as a signal that Salgueiro was prepared to carry out her threat to reveal her information.

---

[23] [redacted] confirmed to the government that the described incident took place (he was not certain of the hearing date but believed it to be in that general time frame).

[24] PARADIS proffered that PETERS told him that he was attending the hearing at the express direction of FEUER. PETERS proffered that he told FEUER that he would attend the hearing, because he knew that FEUER would have wanted him to do so, and would have asked him to do so had he not preemptively volunteered.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

c. PETERS, KIESEL, and PARADIS reconvened in PETERS's office after the hearing, and they agreed that KIESEL would met with Salgueiro for the purpose of doing whatever he needed to do to resolve the situation and ensure that she did not reveal her information.

d. KIESEL met with Salgueiro later that day and agreed to pay her $800,000 in exchange for the return of her information and her assent to a confidentiality agreement.

63. Text messages between PETERS and KIESEL reflect the following exchange from December 4, 2017, with times indicated in brackets:

> KIESEL: I am parked on the north west corner of 1st and Los Angeles Street. [12:13 p.m.]
>
> PETERS: I'm with Paradis. Can u come to my office now to meet? [3:06 p.m.]
>
> KIESEL. Yes. [redacted] is at the elevator engaging J [Salgueiro] so [redacted] and I are stuck. Will come down as soon as we can. [3:07 p.m.]
>
> PETERS: She gave [redacted] her card. [3:09 p.m.]
>
> KIESEL: You waiting for me or going back with Paul [3:09 p.m.]
>
> PETERS: Tried to file a bunch of docs. I'm with Paradis. [3:11 p.m.]
>
> KIESEL: Going back to City Hall? I will meet you there if you go with Paul. [3:12 p.m.]
>
> PETERS: Yes. My office please. I will get you parking. [3:14 p.m.]
>
> KIESEL: Thanks. [3:14 p.m.]
>
> PETERS: **Settle the case if you can! I need you to take care of this.** We are in my office. [3:40 p.m.]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

KIESEL: On my way up now will be there in three minutes. [3:59 p.m.]

KIESEL: I am meeting Julissa tonight at 7:30 PM. With [redacted] **Will get this done.** [6:09 p.m.]

KIESEL: **Deal with J at 800. 450 within 7 days. Have 150 in sixty days balance by May 1.** She will work with attorney [redacted] as her counsel. **Will return all documents when completed. Oyyy** [9:15 p.m.]

PETERS: **Good job. Be sure there is a confidentiality agreement of a sort that would make Marty Singer envious.** [11:43 p.m.]

64. PETERS and KIESEL both (separately) advised the government that these texts corroborate the above-described information that PETERS attended this hearing in the LADWP billing litigation; that Salgueiro showed up at the hearing following her threat to do so if KIESEL did not pay her; that Salgueiro's actions led to KIESEL renewing negotiations to pay Salgueiro $800,000 — a dramatic increase from KIESEL's previous counteroffer of $60,000 — in exchange in exchange for her silence and her assent to a confidentiality agreement; that KIESEL advised PETERS of the terms of the settlement; and that PETERS directed KIESEL to obtain a strong confidentiality agreement.

65. I believe that KIESEL's text message, "**Deal with J at 800. 450 within 7 days. Have 150 in sixty days balance by May 1,**" reflects his description to PETERS of his agreement to pay Salgueiro $800,000. This understanding is consistent with information separately provided by both PETERS and KIESEL as to their respective intents and understanding of this message.

66. I believe that PETERS's text message, "**Good job. Be sure there is a confidentiality agreement of a sort that would**

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

make Marty Singer envious," reflects PETERS's endorsement of KIESEL's decision to pay Salgueiro $800,000 to buy her silence as to the City Attorney's Office's litigation practices, and to obtain a strong and enforceable confidentiality agreement. I am aware from open-source media reports that Marty Singer is a prominent Hollywood-based attorney who is known for aggressive tactics including the use and enforcement of strong confidentiality agreements. This understanding is consistent with information separately provided by both PETERS and KIESEL as to their respective intents and understanding of this message. Moreover, based on my experience and knowledge of the investigation, the fact that the City (as conveyed by PETERS) was more concerned with the confidentiality portion of the agreement than its financial terms strongly suggests that the City's primary interest in the hush money payment was to buy Salgueiro's silence because of its potential damage to the City.

67. KIESEL and PARADIS both advised the government that after the confidential settlement agreement between KIESEL and Salgueiro was formalized, KIESEL paid Salgueiro $800,000, and PARADIS paid KIESEL $400,000.[25]

68. [redacted] participated in a voluntary interview with the prosecution team and advised as follows:

---

[25] According to PARADIS, the money that he contributed came from his own funds, and he did not inform PETERS that he had contributed to the settlement. According to PETERS, he believed, based on information later provided to him by PARADIS, that some portion of the settlement was paid by LANDSKRONER. Information from PARADIS and LANDSKRONER and review of their financial records does not indicate any such direct contribution by LANDSKRONER.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. [redacted] had no prior involvement in or knowledge of the issue before KIESEL asked him to attend the December 4, 2017 hearing and intervene with Salgueiro on KIESEL's behalf. [redacted] was aware that the hearing must have some significance to KIESEL but didn't know what it was. [redacted] understood that Salgueiro had taken some papers from KIESEL's office regarding a case, and that KIESEL wanted [redacted]s help in getting them back. [redacted] volunteered his services and did not get anything in return.

b. At the hearing, [redacted] observed Salgueiro unsuccessfully attempt to give some papers to the court clerk.

c. Following the hearing, [redacted] saw Salgueiro approach [redacted], counsel for PwC, speak with him briefly, and take his business card.

d. [redacted] asked Salgueiro to meet with him and KIESEL over dinner, and she agreed. Salgueiro brought along her friend, Rosa (last name unknown to [redacted]). [redacted] could not recall the details of the negotiation session, but it was relatively short. KIESEL balked at paying the full amount that Salgueiro was demanding because he didn't have access to those funds at that time, and he asked if she would agree to a payment plan. [redacted] believed that they ultimately settled on approximately $800,000.

e. [redacted] knew PETERS from PETERS's tenure at KIESEL's firm, but they were not close. From the time that PETERS accepted a job with FEUER at the City Attorney's Office, it was [redacted]s belief that PETERS intended to follow FEUER when FEUER proceeded to higher political offices after his tenure as City

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Attorney. [redacted] did not have further evidentiary support for his opinion and stated that it was just [redacted]'s belief.

f. PETERS's post-settlement report to FEUER that KIESEL had paid Salgueiro to resolve her threats and demands, and PETERS's post-settlement discussions of the situation with BRAJEVICH and CLARK

69. PETERS proffered that he did not recall reporting these events to FEUER on the day of the December 4, 2017 hearing, which PETERS described as "very unusual" given how concerned and focused FEUER was with respect to Salgueiro's threat to appear at the hearing that day if she did not receive the money she was demanding.

70. PETERS proffered that shortly after the December 4, 2017 hearing (likely on December 5, 2017, but PETERS was unsure of the exact date), PETERS met with FEUER in person, and the following took place:

a. PETERS reported to FEUER that KIESEL had "stepped up" and "reached an accommodation" with Salgueiro.

b. PETERS advised FEUER that settling the matter had "cost KIESEL a ton of money."

c. PETERS confirmed to FEUER that the City would get its documents back as the result of the settlement with Salgueiro, and that they would not be made public.

d. FEUER responded favorably, telling PETERS that this was "great" and that PETERS had done "good work" in facilitating the settlement.

e. FEUER did not ask PETERS for further details of the settlement, and PETERS did not provide them.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

71. PETERS proffered that he was "quite sure" that he would not have advised FEUER after the settlement as to the specific amount that KIESEL had paid, because FEUER would not have been interested in the dollar figure. Rather, FEUER's concern was that the threat of the documents being exposed had been mitigated.

72. PARADIS proffered that around the time of the December 4, 2017 *PwC* hearing where Salgueiro appeared in court (as described in more detail elsewhere), PETERS confirmed to PARADIS that he had in fact —— as PETERS had previously maintained —— told FEUER about Salgueiro's threats, including the nature of the material that she was threatening to reveal.[26] After PETERS confirmed that he had told FEUER about the Salgueiro threats and demands, PETERS also stated that FEUER knew about the "mediation" of her demands taking place on LADWP property, and that FEUER was "pissed" about it.

73. I believe that FEUER's reported displeasure about the use of LADWP headquarters as the venue for the mediation, as described herein, related to the fact that it linked the City to the mediation of Salgueiro's demands, which would, if discovered, cast the City in a negative light.

74. PETERS proffered that at some point after KIESEL settled the matter with Salgueiro, PETERS discussed it with CLARK. PETERS advised that he did not recall the specifics of

[26] PARADIS further advised that he believed that, based on what he knew of PETERS, PETERS indeed told FEUER about the looming threat, because PETERS would not have wanted to risk FEUER being blindsided if "all hell broke loose" and Salgueiro in fact went public with her information.

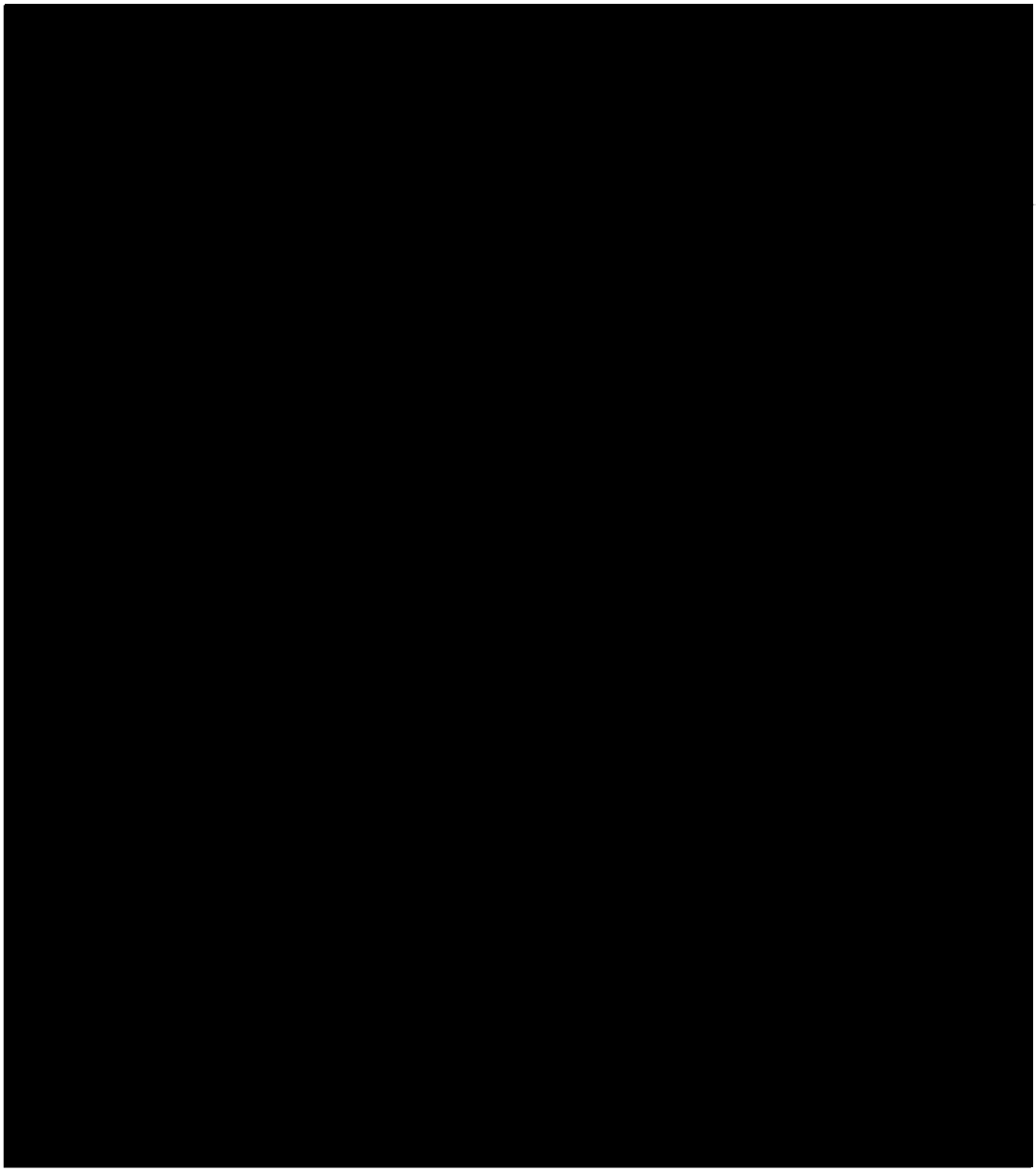
Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

that conversation, and he did not know whether CLARK had details about the Salgueiro matter. PETERS also advised that he could not recall whether he had other conversations with CLARK about the Salgueiro matter.

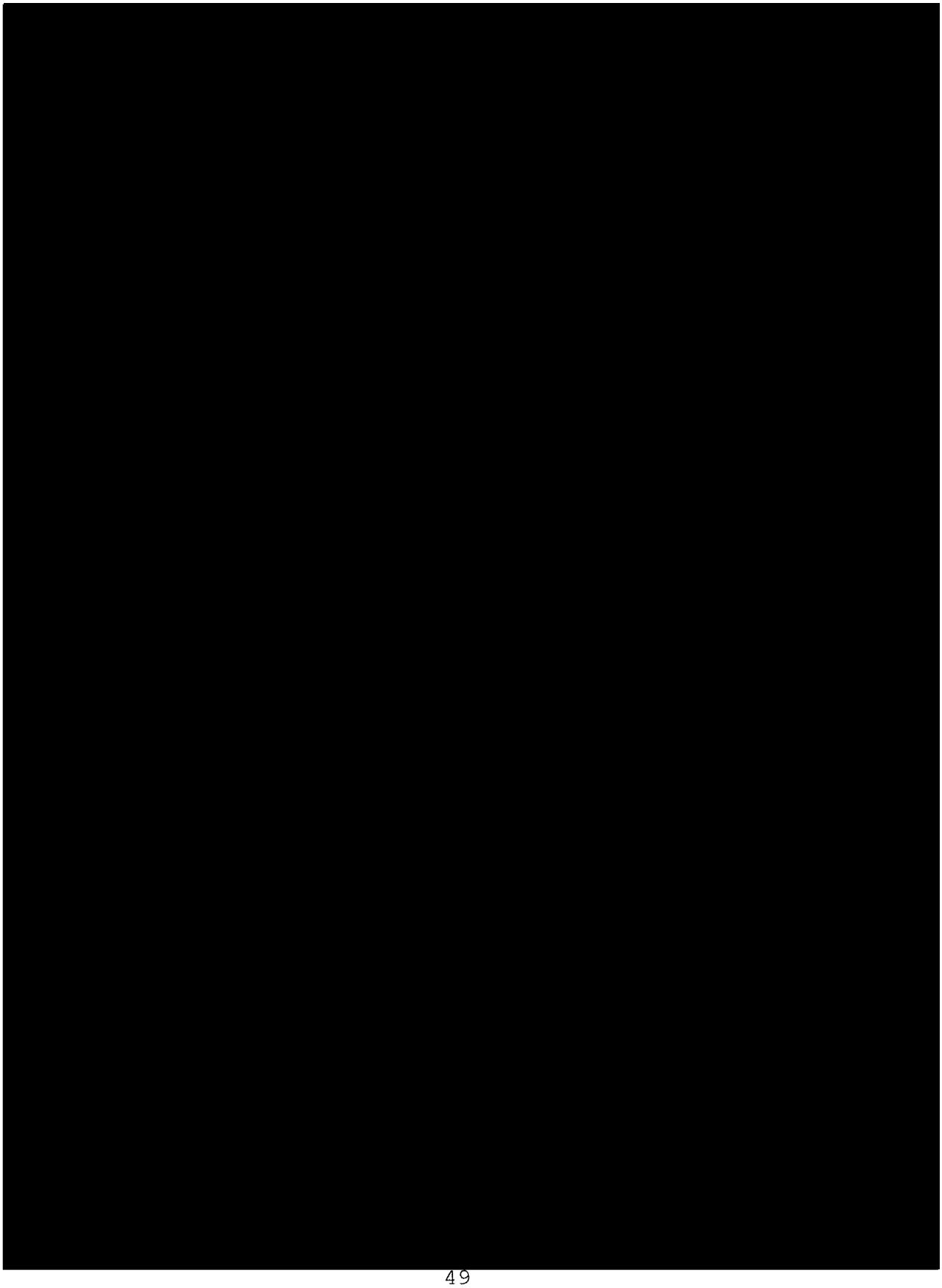
75. PETERS proffered that at some point after KIESEL settled with Salgueiro, PETERS and BRAJEVICH spoke again about the matter.

3. [redacted]

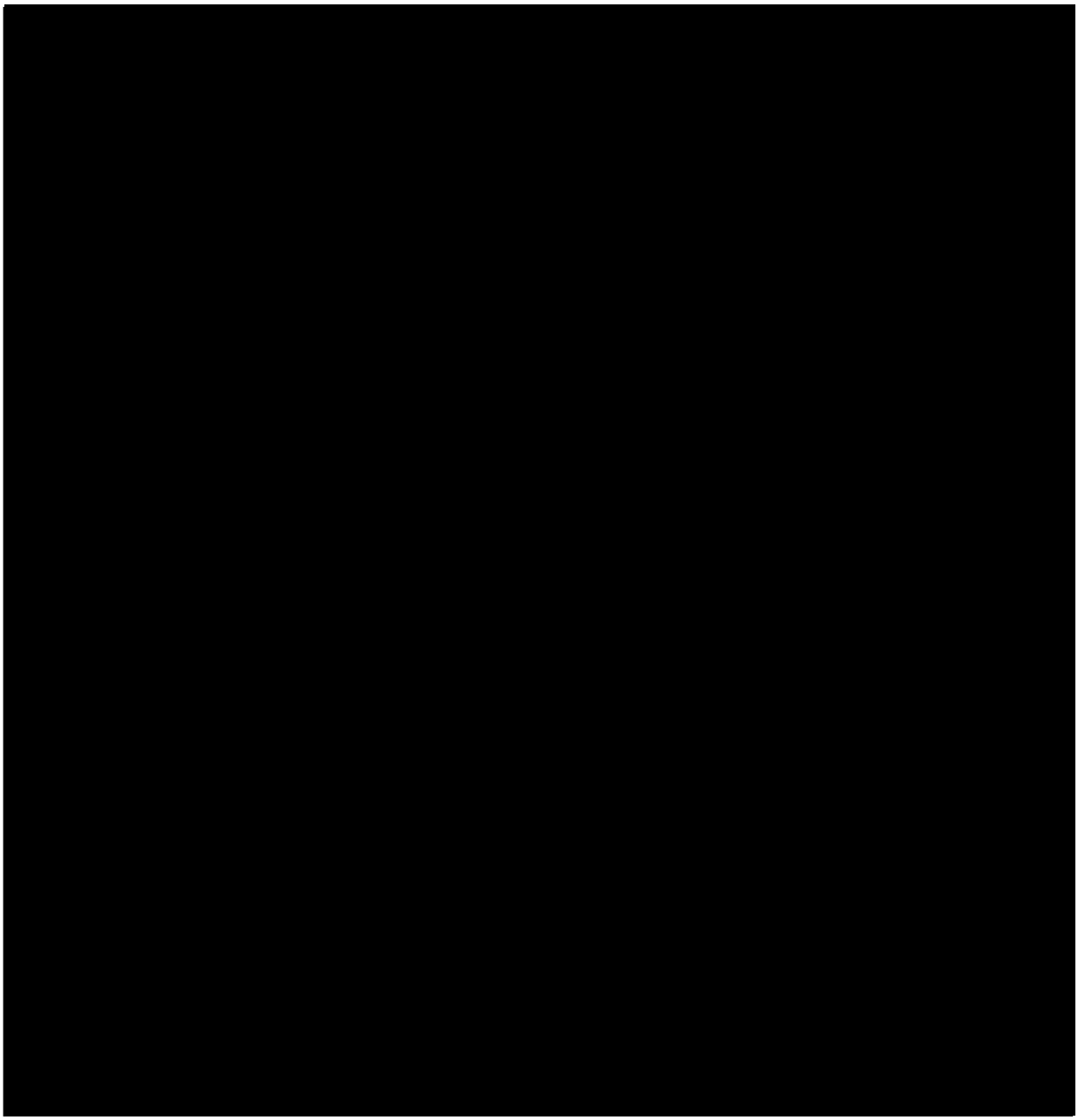
Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB



Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB



Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB



Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

[redacted]

79. Based on the foregoing, I believe there is probable cause to believe that FEUER was in fact aware of Salgueiro's threats to reveal information about the City Attorney's Office's litigation practices unless she were paid for her silence, [redacted] Specifically, my belief is based on:

a. PETERS's proffered information that he advised FEUER about the details and context of Salgueiro's threats and demands, that FEUER was very upset and contemplated firing Special Counsel, and that FEUER expressed to PETERS that KIESEL needed to take care of the matter, which PETERS understood to mean that FEUER wanted him to make sure that KIESEL paid Salgueiro to ensure that the information was not revealed.

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. PARADIS's information that at their meeting on November 17, 2017, PETERS told him that he had notified FEUER of Salgueiro's threats, and that FEUER was very upset about the situation.

c. KIESEL's information that PETERS would fire him if he did not settle with Salgueiro, and that he believed PETERS would likely have discussed the matter with FEUER before making such a threat.

d. KIESEL's contemporaneous diary entry corroborating the information provided by both KIESEL and PARADIS that PETERS had threatened to fire KIESEL if he did not settle with Salgueiro.

e. The December 1, 2017 text message from PETERS to PARADIS stating, "Mike is not firing anyone at this point. But he is far from happy about the prospect of a sideshow. Also, mediating Paul [KIESEL]'s matter at DWP, not a popular move." In addition to PETERS's explanation that this message meant that FEUER had considered but rejected the idea of firing Special Counsel, and that he was displeased about the matter, I believe that this message corroborates the substantively consistent information from PETERS, PARADIS, and KIESEL, and from KIESEL's diary entry, as described above.

f. The December 1, 2017 text message from BRAJEVICH to PETERS asking to discuss "the fact that the mediation took place at DWP," the timing of that message contemporaneous to the above-described message from PETERS to PARADIS relating FEUER's displeasure with the situation and the fact that using LADWP as

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a venue for the mediation was "not a popular move," and BRAJEVICH's relationship with FEUER.

g. PETERS's proffered information that FEUER was aware that the "mediation" had taken place at LADWP, and that FEUER was displeased with that fact.

h. PARADIS's proffered information that PETERS had informed him that FEUER knew that the "mediation" of Salgueiro's demands had taken place on LADWP property, and that FEUER was "pissed" about it.

i. PETERS's proffered information that he discussed the matter with FEUER again after the settlement and advised that KIESEL had "stepped up" and settled the matter with Salgueiro, and that the resolution had "cost KIESEL a ton of money."

j. PARADIS's proffered information that shortly after KIESEL reached a settlement with Salgueiro on December 4, 2017, by agreeing to pay her $800,000, PETERS confirmed to PARADIS that PETERS had in fact told FEUER about Salgueiro's threats, including the nature of the material that she was threatening to reveal.

80. I believe that the above information, taken together, constitutes probable cause to believe that [redacted] FEUER not only was aware of Salgueiro's threats and demands, but he impliedly directed PETERS to ensure that KIESEL settled those demands by paying a large sum of hush money.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

B. There Is Probable Cause To Believe That FEUER Obstructed Justice By Giving Misleading [redacted] Statements Indicating That He First Learned In April 2019 About Documents Indicating the Special Counsel's Work On Behalf Of The Jones Plaintiff

81. As further described below, the evidence provides probable cause to believe that in January 2019, PETERS apprised FEUER that KIESEL and PARADIS had documents responsive to PwC's court-authorized discovery demand that would be damaging to the City. Specifically, according to multiple sources of evidence — — including a contemporaneous recorded conversation wherein PETERS recounted his recent conversations with FEUER — PETERS told FEUER that the documents would reflect previously undisclosed coordination between Special Counsel and Jones's counsel, JACK LANDSKRONER, in filing the *Jones v. City* complaint, including potentially the fact that Special Counsel acting on behalf of the City had drafted the *Jones v. City* complaint.

82. According to PETERS, FEUER was very upset, reacted with extreme shock and dismay, and stated that the revelation of those facts would be a "catastrophe." Based on that interaction and his experience with FEUER, PETERS understood from their discussions that FEUER wanted PETERS to ensure that the documents were not produced or otherwise revealed. KIESEL and PARADIS both sent the documents to PETERS as discussed, but PETERS, at the perceived direction of FEUER, did not produce the documents to PwC or alert the state court or anyone else of their existence. Instead, PETERS, at FEUER's direction, appeared at a hearing in the *PwC* case and represented to the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

state court that "there were documents that were requested of the City through that PMQ deposition notice.[28] We will be producing those documents."

83. As further detailed below, the evidence indicates that the documents that KIESEL sent to PETERS — which were responsive to the PMQ document demand and which FEUER and PETERS knew would be damaging to the City's litigation position and the City Attorney's Office's, specifically including FEUER's, reputation — eventually surfaced during a review of PETERS's hard drive that was directed by Browne George, the City's outside counsel. FEUER made official statements to the prosecution team [redacted] on this topic, along with various public statements and filings and sworn civil deposition testimony. The evidence provides probable cause to believe that FEUER's [redacted] official statements to the government were knowingly misleading, in that he did not first learn of the information revealed in the KIESEL Emails in late April 2019, which is when the KIESEL Emails were independently discovered and a need arose for FEUER to publicly address it. In fact, FEUER learned of this information months earlier, namely, not later than January 2019, after which he impliedly directed their concealment. Based on my training, experience, and knowledge of this investigation, I believe FEUER had a strong incentive to personally distance

---

[28] In California civil litigation, a PMQ deposition requires the "person most qualified" at an entity to testify on behalf of the entity as to certain relevant facts either known to the deponent or gathered through the deponent's investigation.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

himself from any knowledge of the collusive litigation for his own political gain (or to avoid political fallout).

1. The evidence indicates that FEUER, along with KAPUR and BRAJEVICH, learned about the KIESEL Emails in January 2019

84. On the afternoon of January 23, 2019, a hearing took place in the *PwC* case. According to the transcript of the hearing, the judge overruled the City's privilege objections to documents demanded by PwC and ordered the City to submit a "person most qualified" ("PMQ") to represent the City at a deposition. The judge further expressed concerns about the City's privilege assertions and related conduct, and asked KIESEL, who was representing the City at the hearing, to "bring these matters not only to the attention of the internal affairs department, if there is such a department, but also to bring it to the attention of the City Attorney, Mike Feuer, directly."

85. On January 23, 2019, at 4:59 p.m., BRAJEVICH (using **BRAJEVICH's ACCOUNT**) sent PETERS a text message stating, "Lets talk before you speak with mike [FEUER]." BRAJEVICH and PETERS exchanged additional text messages and agreed to speak the next day.

86. At 6:52 p.m. on January 23, 2019, PETERS sent an email to FEUER at **FEUER's EMAIL**. In the email, PETERS summarized the hearing, including the judge's invocation of FEUER's name. PETERS stated that "**[Judge] Berle is now aware of communications between Paradis and Landskroner about the latter taking over Mr. Jones' contemplated case against PwC, and the fact that such representation soon evolved into *Jones v. DWP*.**" PETERS further

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

noted that the court "was wondering aloud today whether the *Jones* settlement is somehow vulnerable to being reevaluated due to possible conflicts by Paradis." PETERS opined that there were no ethical lapses by the City, but that they should discuss the matter soon. PETERS suggested a meeting with just PETERS, FEUER, and KAPUR, but he offered to involve PARADIS, KIESEL, or BRAJEVICH if FEUER so desired.

87. At 7:02 p.m. on January 23, 2019, FEUER replied from **FEUER's EMAIL** with a brief email directing PETERS to set up a meeting for January 25, 2019, with PETERS, FEUER, and KAPUR. Later that evening, PETERS replied that he had done so.

88. At 7:06 p.m. on January 23, 2019, FEUER (using **FEUER's EMAIL**) again replied to PETERS's original email, stating, "Although it may be too late to fix all this, it may be a good idea to have someone from our office at the next hearing before Judge Berle." Later that evening, PETERS replied, "I'll be there."

89. On January 24, 2019, KIESEL forwarded to PETERS, TUFARO, and BRAJEVICH (at **BRAJEVICH's EMAIL**) an email from counsel for PwC regarding the City's PMQ document and production of outstanding documents. PETERS replied to all asking whether the City owed documents to PwC, and indicating that if so, it should produce them. KIESEL forwarded the email to PARADIS, who replied to all stating, "Yesterday when we met with Thom [PETERS] (with Joe B. [BRAJEVICH] on the phone), Thom directed us to research and draft a writ to be filed in the very near future." PARADIS opined that the City should await resolution

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

of the writ before proceeding with either the PMQ deposition or the document production. PETERS replied to all asking when the writ could be ready, TUFARO replied with a projected date, and PETERS replied with an acknowledgement.

90. PETERS proffered that on January 24, 2019, he met with PARADIS, and the following took place:

a. PARADIS appeared very upset about the events that were unfolding in the *PwC* case, and he told PETERS, "I'm not going to go down for this bullshit."

b. PARADIS told PETERS that not only had PARADIS aided LANDSKRONER in the drafting of the *Jones v. City* complaint, but PARADIS had in fact personally drafted both the complaint and the settlement demand letter. PARADIS further advised that "everyone" at the City knew about this, including CLARK, DAVID WRIGHT, LADWP Board President MELTON EDISES LEVINE, Assistant City Attorney Eskel Solomon, and others.

c. PETERS told PARADIS that he wanted to review the documents that would reflect these facts.

91. On January 25, 2019, at 8:03 a.m., BRAJEVICH (using the **BRAJEVICH's ACCOUNT**) left a voicemail for PETERS indicating that BRAJEVICH had sent PETERS a couple of emails relating to two declarations filed by LANDSKRONER. BRAJEVICH stated that he had concerns about the declarations, specifically; 1) in a section denying any relationships with counsel in the case, LANDSKRONER omitted reference to PARADIS; and 2) LANDSKRONER stated that he had started working on the case in November 2014, which was inconsistent with the City's timelines in connection

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

with the City's attempt to assert a "common-interest defense" privilege.[29]

92. On January 25, 2019, at 8:42 a.m., BRAJEVICH (using the **BRAJEVICH's ACCOUNT**) left another voicemail message for PETERS, which expressed BRAJEVICH's desire to have TUFARO send legal authority for their position on the common-interest privilege. BRAJEVICH opined that the City needed to identify a common-interest agreement reached between Jones and the City, and that he wasn't sure how they would do that under existing legal authority. BRAJEVICH noted that "when you're making declarations it looks like you're hiding something when you're not disclosing it." BRAJEVICH opined that he thought they would be okay because the ratepayers got 100 cents on the dollar in the *Jones* settlement, but he was concerned about "how we get through all the appearances and the sloppy ass shit."

93. On January 25, 2019, at 8:44 a.m., BRAJEVICH, using **BRAJEVICH's ACCOUNT**, sent PETERS a text message stating that BRAJEVICH had "Left you 2 voicemails on your cell when you have a chance to listen."

94. KIESEL's law partner, [redacted], advised the government that on January 25, 2019, she participated in a conference call with PETERS, KIESEL, PARADIS, and TUFARO, during which the parties discussed whether a privilege would apply to the documents sought by PwC and whether the City would take a writ. [redacted] was generally unfamiliar with the case at that

[29] I have reviewed two emails that BRAJEVICH (using **BRAJEVICH's EMAIL**) sent to PETERS on January 25, 2019, which I believe are the emails referenced here.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

time. She recalled that during this discussion, PETERS appeared inclined to take a writ, but that PETERS said that he was going to discuss the matter with FEUER. [redacted] further recalled PETERS stating that he had a scheduled meeting with FEUER that evening (Friday, January 25), and that PETERS was not looking forward to giving FEUER bad news on a Friday evening.

a. An electronic calendar entry showed that on January 25, 2019, at 12:30 p.m., KIESEL invited PETERS, BRAJEVICH (on **BRAJEVICH's EMAIL**), PARADIS, TUFARO, and [redacted] to a "Follow Up Conference Call" on January 28, 2019, at 9:30 a.m.

b. I believe that this entry scheduling a "follow up" corroborates [redacted]'s recollection that she joined a call with PETERS, KIESEL, PARADIS, and TUFARO on January 25, 2019. I further believe that the inclusion of BRAJEVICH on the invitation, paired with BRAJEVICH's inclusion on the aforementioned January 24 email chain, suggests that BRAJEVICH may also have participated in the January 25 call that [redacted] recalled.[30]

c. I further believe that a voicemail from BRAJEVICH using **BRAJEVICH's ACCOUNT** to PETERS on the morning of January 28, 2019 (described in more detail below), to touch base about their planned 9:30 a.m. conference call set for that morning, additionally supports the other evidence that BRAJEVICH was

[30] A further calendar entry indicates that KIESEL canceled the January 28 call.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

aware of the issues being discussed and planned to take place in this "follow up" call.

95. On January 25, 2019, PETERS took part in a phone call with KIESEL, PARADIS, and TUFARO. [redacted] surreptitiously recorded a portion of the call and later provided the recording to the government.[31] I have reviewed the transcript, which reflects PETERS, PARADIS, and TUFARO discussing matters including: 1) the fact that the City had not disclosed the City's coordination with LANDSKRONER in drafting and filing the complaint, 2) their view that the City had not had an obligation to disclose it in the past, 3) whether or not to disclose it now, and 4) the possible reactions of the court to such a disclosure. PETERS opined that this was an "optical" problem, but stated that as a legal matter, he did not believe the City had done anything wrong.

96. FEUER's daily schedule, which was emailed to PETERS, indicates a scheduled meeting on Friday, January 25, 2019, from 4:30 p.m. to 5:00 p.m., between FEUER, KAPUR, and PETERS.

97. PETERS proffered that on either January 25, 2019, or January 28, 2019, PETERS attended a meeting with FEUER and KAPUR to discuss PwC's court-authorized demand for documents related

---

[redacted]

The metadata from the recording [redacted] suggests that this recording was saved at 11:24 a.m. PST on January 25, 2019. It is unclear to me whether this is part of the same call that [redacted] participated in. [redacted] indicated that she did not speak during that call.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to the City's upcoming PMQ deposition. According to PETERS, the following occurred at that meeting:

a. PETERS advised that there were documents in KIESEL's and PARADIS' possession that would be damaging to the City.

b. PETERS told FEUER that he did not at that time know precisely what the documents contained, but that he believed they would show coordination between KIESEL/PARADIS and LANDSKRONER before the *Jones v. City* complaint was filed.

c. PETERS told FEUER that he anticipated that the documents would show the City providing existing complaints to KIESEL/PARADIS to aid their drafting of the *Jones v. City* complaint.

d. PETERS further stated that the documents would likely show that PARADIS drafted the *Jones v. City* complaint and the settlement demand letter.

e. FEUER's reaction was like nothing PETERS had seen before. FEUER was highly emotional and visibly upset, covering his face with his hands for a long period. FEUER repeated multiple times that this "can't be so." FEUER stated that this would be "catastrophic," which PETERS understood to reference the anticipated effect that disclosure of these facts would have on the *Jones* settlement and the reputation of FEUER's office.

f. PETERS told FEUER not to "panic," and told FEUER that he (PETERS) would look into the situation.

g. FEUER did not at any time ask to see the documents that PETERS had described, nor did he ever ask PETERS

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to obtain them, review them, or show them to FEUER or anyone else.

h. FEUER and PETERS discussed the next hearing before Judge Berle, which was set to occur the following Wednesday, January 30, 2019, in the *Jones* case. FEUER and PETERS agreed that they (officials from the City, not Special Counsel) needed to convey to Judge Berle the message that he had the attention of the City Attorney's Office, and that the City Attorney's Office would not tolerate any unethical conduct.

i. FEUER directed PETERS to draft, over the weekend, a script bearing this message, which PETERS would deliver in person at the *Jones* hearing the following Wednesday.

98. On Saturday, January 26, 2019, in a series of text messages that I have reviewed, PETERS asked KIESEL to set up a call for the next day. KIESEL agreed and asked, "Will Mike [FEUER] give us clearance for disclosure of documents and full disclosure on questions?" PETERS did not reply to that inquiry, and they set a call for 2:00 p.m. the following day with them and PARADIS.

99. On Saturday, January 26, 2019, in a series of text messages that I have reviewed, KIESEL asked PARADIS to participate in a call with PETERS the next day at 2:00 p.m. PARADIS agreed and asked whether KIESEL had "anything to report now." KIESEL replied that PETERS had left a message that FEUER had reached a decision on another issue, but KIESEL stated that PETERS "said nothing about the documents or objections."

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. Based on the context of the above two text exchanges and my knowledge of the investigation, I understand that KIESEL indicated that PETERS had not yet advised whether FEUER would authorize them to disclose the potentially damaging documents that PwC was demanding.

100. On January 27, 2019, at approximately 2:20 p.m. PST, PETERS, KIESEL, PARADIS, and TUFARO participated in a telephone call. [redacted] surreptitiously recorded a part of the conversation and later provided the recording and a draft transcript to the government.[32] The recording contains the following relevant portions:

> PETERS: Okay. **Here's what I would like to do though, at Mike's request. He said to me, "What are the very, very worst documents out there that we've created that would most likely lead to embarrassment** or serve as a basis for somebody's… or Jamie Court's allegations that there was, that there was some conflict… anything from the pinnacle or standpoint of ethics." . . .
>
> Now, I said to him "Ya know, Mike, I don't really know," and he kinda chided me for not knowing and that's a fair criticism from where I stand. **I said, "although it's not teed up yet, there's a probably greater than 50 percent likelihood that eventually it will be revealed that we drafted for Landskroner a draft complaint." Now, at first, there was a great gnashing of teeth.**
>
> . . .
>
> PETERS: But this is, **Mike is aware that this could get ugly for a while.** But he wants to let us get in there and tear off the band-aids because once you get beneath the smoke, you know, you'll see that there really is ultimately, no ethical fire.
>
> . . .

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

PETERS: And all of the story is going to be told through these emails? Right, Paul?

PARADIS: Yes. Yes.

KIESEL: Yes. And by the way, **there are emails with the City of L.A., discussing -- knowing we were doing this and encouraging us to do this quickly.**

PETERS: **Okay.**

. . .

KIESEL: And then, Tommy, the only other piece, at least on the emails I saw, was Michael Libman, who was gonna to be filing the Jones versus DWP complaint reached out to me. He was in trial, and he said, "Paul, I need the money to file the Jones action." And I said, maybe something like, "We'll take care of it." And Paul Paradis was copied on it. And Paul wrote back and said, "no Landskroner is picking up all costs, all expenses. It's on Landskroner." And Landskroner obviously paid for the filing of the complaint.

PETERS: **I will want to read that one** because that one, **because optically, someone is going to optically scratch their head on.** So, I'll know about that one. Yeah, so if you could **send those things to me so I can get through 'em before Wednesday morning,** that would make me more comfortable. **It's just what's the universe of shit that's going to happen. I can give a heads up to Mike.**

. . .

KIESEL: Well, let me just add that I am feeling a whole lot better after this conversation than I had been for the last 48 hours. This has been a difficult situation.

PETERS: What were you expecting? What were you figuring that Mike was gonna ask us to do?

KIESEL: **I was figuring that Mike was not gonna release the documents at all** but Mike wanted to take a writ on the objections and we were just gonna make this thing so much worse than it is, in the end. So, I'm thrilled that we're getting transparency. Light is what will disinfect the situation, nothing more.

PETERS: Yep.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

101. Based on the context of the messages and my knowledge of the investigation, I believe the parties' references to "Mike" throughout the January 27 conversation refer to FEUER. I further believe that the reference to "Jamie Court" refers to the president of an organization called Consumer Watchdog, which has, according to open-source media reports and other information revealed during the investigation, raised public allegations of corruption and ethical violations by City Attorney's Office and LADWP regarding the billing system litigation.

102. PETERS proffered that he participated in a phone call with KIESEL and PARADIS on January 27, 2019, and provided the following information relevant to that call:

a. PETERS told KIESEL and PARADIS that he wanted to see the documents.

b. KIESEL asked whether FEUER would allow them to produce the documents, and PETERS stated that "I will take a look."

c. KIESEL "seemed resigned" to the fact that the documents would be produced. By contract, PARADIS was more reluctant and concerned about the possibility of production.

103. PETERS proffered that, at some point during this time period, he conveyed to KIESEL and PARADIS that FEUER was "not interested in producing these documents."[33]

---

[33] I recognize that this information is inconsistent with other evidence described herein and, if true, would appear to represent a change in direction from the discussion reflected in the aforementioned partially recorded call on January 27, 2019.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

104. On the morning of Monday, January 28, 2019, at 9:08 a.m., BRAJEVICH (using **BRAJEVICH's ACCOUNT**) left a voicemail for PETERS. BRAJEVICH stated that he was calling to touch base with PETERS before "the 9:30 call," which BRAJEVICH planned to take from the road.[34]

105. PETERS proffered that over the weekend of January 26-27, 2019, as directed by FEUER, PETERS drafted a written script to read in court at the January 30 *Jones* hearing

106. PETERS further proffered that the following took place at and between a series of meetings with FEUER and KAPUR early in the week of January 28, 2019:

a. In preparation for the January 30, 2019 hearing in the *Jones* case, PETERS and FEUER worked together to hone the written script that PETERS was instructed to read aloud in court.

b. To the best of PETERS' recollection, PETERS drafted his statement by hand on a yellow pad and delivered it orally to FEUER at FEUER's direction. FEUER then critiqued PETERS's performance and directed him to make various changes. According to PETERS, FEUER's changes were of the "micromanagerial" variety and included instructing PETERS to refrain from using a definitive article.

---

[34] As noted above, I believe that this referenced 9:30 a.m. conference call was a scheduled call that KIESEL had invited PETERS, BRAJEVICH, PARADIS, TUFARO, and [redacted] (via an electronic calendar invitation that I have seen) to join at that time. A further email from KIESEL at 9:24 a.m. on January 28, 2019, indicates that this call was cancelled a few minutes before it was to take place.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

c. FEUER had never required PETERS to do anything like this before. PETERS was embarrassed about being required, as a division chief, to deliver a mock presentation to the City Attorney.

d. In addition to FEUER and KAPUR, PETERS recalled that Wilcox was present for at least one of the mock presentations. PETERS further believed (but was uncertain) that BRAJEVICH may have been present.

107. An electronic calendar entry sent by Google calendar on behalf of FEUER at **FEUER's EMAIL** to PETERS and KAPUR at **KAPUR's EMAIL** indicates a scheduled meeting between FEUER, KAPUR, and PETERS on Monday, January 28, 2019, from 2:30 p.m. to 3:30 p.m (two days before the scheduled hearing on the documents).

108. On the evening of Monday, January 28, 2019, BRAJEVICH left a voicemail for PETERS. BRAJEVICH reported that he had a good meeting with Maribeth [Annaguey], and noted that he and PETERS were "on for 11:00 tomorrow." BRAJEVICH said that he told "them" that if there were "any particular buzz words" that PETERS should say when PETERS was "down there on Wednesday" [January 30, 2019], to give them to PETERS tomorrow.

a. I believe that BRAJEVICH's reference to buzz words that PETERS was supposed to say on January 30, 2019, indicates BRAJEVICH's awareness that PETERS was receiving direction from others about what to say at the January 30 hearing.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

109. FEUER's daily schedule, which was emailed to PETERS, indicates a scheduled meeting on Tuesday, January 29, 2019 (one day before the hearing), from 10:30 a.m. to 11:00 a.m., between FEUER, KAPUR, and PETERS.

110. I have reviewed a January 29, 2019 email from PARADIS to PETERS and TUFARO attaching a .pdf file. The attached .pdf files contained email correspondence reflecting PARADIS's and KIESEL's coordination with LANDSKRONER in drafting and filing the *Jones v. City* complaint.[35] In an email on January 30, 2019, PETERS replied to confirm receipt.

111. Both KIESEL and [redacted] advised the government that early in the week of January 28, 2019, KIESEL asked [redacted] to gather emails responsive to PwC's document request related to the City's PMQ deposition, that [redacted] worked with KIESEL's technical staff to do so, and that on January 30, 2019, [redacted] sent an email to PETERS and PARADIS with a Dropbox link to a .pst[36] file containing the emails from KIESEL's system that [redacted] found to be responsive.

---

[35] To my knowledge, these files from PARADIS, which I have reviewed, have not been revealed or produced by the City. I do not know whether they were recovered in the City's forensic examination of PETERS's computer (described below) or why they were not included in the City's below-described April 2019 filing revealing the KIESEL Emails.

[36] In computing, a Personal Storage Table (".pst") is an open proprietary file format used to store copies of messages, calendar events, and other items within Microsoft software such as Microsoft Exchange Client, Windows Messaging, and Microsoft Outlook.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. I have reviewed this email from [redacted] to PETERS and PARADIS dated January 30, 2019, with a Dropbox link to a .pst file labeled "Emails Responsive to PMQ."

112. PETERS proffered as follows:

a. PETERS received the documents from both PARADIS and KIESEL on approximately January 29, 2019.

b. Believing that FEUER did not want the documents to come to light, PETERS did not tell FEUER that he had received these documents from PARADIS and KIESEL.

c. FEUER did not ask about the documents after the late-January meeting wherein PETERS told FEUER what he expected the documents to show, and PETERS understood that FEUER did not want him to produce the emails.

d. During this time period, on a date that he did not recall, PETERS informed KIESEL and PARADIS that "Mike has decided not to produce the documents," which PETERS believed to be FEUER's implicit directive to PETERS.

113. On the morning of January 30, 2019, PETERS appeared in court at the *Jones* hearing, as directed by FEUER. At the hearing, PETERS made the following statement (related in pertinent part), which was in substance the statement that FEUER had "flyspecked" and instructed him to make:

> My name is Tom Peters, and I'm appearing personally in this matter for the first time based on the court's request in the related case that the City Attorney be asked to review the status of these matters. That is being done, but I do want to make sure that you understand our commitment to assuring the court that . . . . This court needs to feel completely comfortable and at ease that its confidence in this settlement in justified. There are a few things I think we can do

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to advance that goal. Look, from the summer of 2014, if not earlier, the Department of Water and Power knew there was a huge problem with the Customer Care and Billing System. We still have a dispute, as to this day, as to whether it was PwC's fault or DWP's. That's the related litigation.

Look, fundamentally, with respect to this lawsuit, the Jones, et al., ratepayer class actions, there was a shared objective between the Department and the ratepayers from the get-go to give them 100 percent on the dollar refund of every dollar that had been overbilled, not 99 percent or 98 percent, but, Your Honor, also we couldn't pay 101 or 102 percent. That's a gift of public funds. **So through arm's length negotiations, that goal was ultimately achieved** as was the interrelated goal of getting a meaningful, durable, thorough process underway to make sure that the Customer Care and Billing System was repaired such that there was not a repeat, and we're obviously still grappling with that problem to this day. **But to the extent that anybody continues to be concerned at a lack of arm's length negotiation, I have some proposals**, and I think hopefully everybody will think are good ideas. One is the City suggested that we have a deposition of retired federal judge Dikran Tevrizian who presided over the multiple mediation sessions we had because he's the one person who, better than anyone else, would know the nature of the negotiations. The City certainly doesn't object to that.

To the extent that people are concerned about how the remediation or the refund is going, the City would certainly not object to deposition of Mr. Bender or Ms. Barbara Berkovich I think is her name, who is the special master who knows about the appellate process. The court has asked that she give her report at the end of this. If anybody's curious on how things stand today, then they should do it. I should also report to the court that in the related case, the City is not going to take any sort of a writ related to the recent litigation related to the PMQ depo notices.[37]

---

[37] From review of the transcripts and related materials, I understand this as a reference to the court's order that the City submit a PMQ witness for a deposition and produce related documents, which was issued over the City's objection. I also understand that the documents discussed between PETERS and FEUER, sent to PETERS by KIESEL and PARADIS, and withheld by PETERS at FEUER's implied direction were arguably responsive to this PMQ notice.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

> **As the court will recall, there were documents that were requested of the City through that PMQ deposition notice. We will be producing those documents.** We will be producing, also, the Chief Deputy of the office, Jim Clark, coincidentally a partner until about six years ago of the Gibson firm which is defending PwC. He will respond, I think, to all of the categories of inquiry set forth in that notice.

a. Following this statement by PETERS, the court commented as follows:

> I think that matter [of the discovery issues raised in the *PwC* case], it seems to be viewed seriously, which I think is important, and **I hear your words about cooperation with the discovery that will be coming along.**

b. PETERS replied as follows:

> Yeah. **We should all be assured that the City Attorney's commitment to always practicing with the highest ethical standards in mind has indeed been advanced, and I think that once the totality is understood, everyone will conclude that that is precisely what has happened here.**

c. Based on my knowledge of the investigation, I believe that by directing PETERS to make this prepared statement, FEUER intended for the court, the parties, and PwC to believe that the City would no longer fight production of all materials responsive to PwC's PMQ notice, and that it would comply with the order to produce that discovery.

114. On January 30, 2019, at 11:28 a.m., PETERS sent an email to FEUER at **FEUER's EMAIL** and KAPUR at **KAPUR's EMAIL** with the subject line "Things went well in court this morning." In the three-paragraph email, PETERS summarized that morning's hearing in the *Jones* case, including the following:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. PETERS opined that he had expressed his thoughts well with a "non-apologetic" tone, and that the judge had responded well.

b. PETERS stated that the court indicated that the propriety of the settlement was not being questioned, and that the only issue was whether there was a conflict.

c. PETERS stated, "Because we believe that our team's ethics will be vindicated once all of the facts concerning the interaction with Jones/Landskroner are revealed and understood, I am anxious to get those facts out as soon as possible and have yet again expressed such to the Pauls [KIESEL and PARADIS], who agree."

d. "[O]ur purpose for the day appears to have been fulfilled. Now on to the implementation of our plan, where I will be working carefully to see that things go as smoothly as possible."

e. PETERS asked FEUER to advise whether PETERS should come to FEUER's office to discuss further.

115. Seventeen minutes later, using **FEUER's EMAIL**, FEUER replied to all, "Thank you so much, Thom. Deeply appreciated. I would be grateful for a few more minutes with you today on this point, but no emergency. Mike."

116. At 12:56 p.m. on January 30, KAPUR (using **KAPUR's ACCOUNT**) replied to just PETERS as follows: "Thom - glad to hear it went well - I know a big relief to you (and Mike) as it sounds that you were successful of starting to turn the course of the ship -- not an easy thing to do!"

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

117. PETERS proffered that soon after the January 30 hearing, and after PETERS sent the aforementioned email to FEUER and KAPUR reporting that the hearing had gone well, FEUER came down to PETERS's office, which was on a different floor, and the following events took place:

a. FEUER and PETERS did not have a meeting scheduled; rather, FEUER was dropping by unannounced.

b. FEUER left his security detail outside PETERS's office and shut the door.

c. FEUER expressed that he was very thankful that things had gone well at the hearing, and that PETERS had stuck to the script and delivered their message to FEUER's satisfaction.

d. FEUER stated that he was pleased that Maribeth Annaguey, the City's outside counsel, had given PETERS's performance a positive review.

e. FEUER was very effusive in his praise of PETERS and in expressing his gratitude.

f. FEUER apologized if he had offended PETERS for "treating him like a first-year associate" and requiring him to deliver mock performances in FEUER's office.

g. FEUER came around to PETERS's side of the desk and stood behind PETERS. FEUER "laid hands on" PETERS by placing both hands on PETERS's shoulders in a friendly and intimate gesture.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

h. During the conversation, FEUER stated words to the effect that, "I've got your back," and "I've always taken care of you."

i. During this interaction, PETERS told FEUER words to the effect that, "By the way, you don't need to worry about those documents." FEUER replied with words to the effect that this was "great, wonderful. I appreciate it."

j. FEUER did not ask what documents PETERS was talking about, nor did he ask what PETERS meant. At no time did FEUER ever ask to see the documents, or ask whether PETERS had seen them or what they had revealed.

k. FEUER's unannounced visit to PETERS's office lasted approximately 10-15 minutes.

l. The interaction was unusual, and it was very significant to PETERS. PETERS interpreted it as confirmation that he had done the right thing in withholding the documents, because he had correctly intuited that FEUER did not want him to do so.

103. PETERS proffered that during this time period, BRAJEVICH was involved in discussions relating to the City's strategy for shielding from production the documents sought by PWC in its PMQ discovery demand.

104. I believe the evidence, including the above-described proffer information, voicemails, emails, and meeting invitations to or from BRAJEVICH, combined with BRAJEVICH's engaged role in this high-profile lawsuit involving LADWP, provides probable cause to believe that BRAJEVICH was involved in substantive

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

discussions as to the City's strategy to shield the damaging KIESEL and PARADIS PMQ documents, about which FEUER later gave the potentially false [redacted] statements described herein.[38]

2. The events between late January 2019 and April 2019

105. As further described in the omnibus affidavit, evidence indicates that the following relevant events took place between late January 2019 and April 2019:

a. In February 2019, FEUER and PETERS decided that CLARK would serve as the City's "person most qualified" witness in the City's PMQ deposition, notwithstanding the facts that 1) CLARK was set to return from a lengthy medical leave [redacted] just days before the deposition, and 2) CLARK was officially recused from the *PwC* case because he received retirement income from Gibson Dunn, PwC's counsel.

b. On February 26, 2019, CLARK testified as the City's PMQ witness. CLARK's testimony included the following:

[38] In a text message from BRAJEVICH to PETERS on March 2, 2019, BRAJEVICH stated that he "did not realize Paradis had prepared a complaint vs DWP and sent it to Jones." PETERS replied by text that he did not know that either. I do not know whether BRAJEVICH included this in a text message to falsely cover himself and/or PETERS as these issues were starting to become public, or whether BRAJEVICH was truly unaware that PARADIS had drafted the *Jones v. City* complaint. As discussed herein, the evidence indicates that by that date, PETERS was aware of that fact, notwithstanding his statement to the contrary in this text exchange.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

i. CLARK first learned that Jones would be suing LADWP in March 2015, after it became clear that the *Jones v. PwC* lawsuit was not going to go forward.

ii. The City expected the *Jones v. City* complaint before it was filed on April 1, 2015.

iii. After PARADIS concluded that he had a conflict in representing Jones against the City, which was PARADIS's client, CLARK was aware that PARADIS recommended that LANDSKRONER be brought in as Jones's new counsel, and that CLARK assumed that someone at the City authorized that action.

iv. CLARK understood that the City had recommended LANDSKRONER to represent Jones because the lawyers in the class actions that had already been filed against the City were intransigent and difficult to deal with, and CLARK didn't know if they were "willing to do what DWP wanted."

c. On March 14, 2019, the City submitted on CLARK's behalf a lengthy "errata" containing 54 changes to CLARK's testimony, many of them substantive, including the following:[39]

i. CLARK was asked, "How much earlier than April 1 did you know that the settlement demand would be forthcoming at some point and that you would be settling with Mr. Jones?" CLARK replied, "Sometime during the latter half of — the end of March." In his errata, the City retracted this answer and changed it to, "I didn't."

[39] The errata was signed by CLARK. Information from multiple sources, including CLARK, indicates that the errata document was the result of one or more lengthy discussions among lawyers from the City Attorney's Office and outside counsel, who determined that CLARK's answers needed to be amended.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

ii. In a reply to a question as to why one of the existing class counsel was not recommended to Jones, CLARK testified as follows: "My understanding, and this is mostly from outside counsel, the Liner [law firm] people, who have been trying to deal with [the plaintiffs' lawyers for the existing class actions], that they were just intransigent, couldn't — they wouldn't — didn't want to negotiate or propose things that were not — were not acceptable. And I don't know if they were willing to do what DWP wanted, which was basically — there would have been overcharge repaid and have the — and have oversight of the system to correct it." The City's errata changed CLARK's answer to, "I don't know what Mr. Paradis recommended to Mr. Jones."

iii. At his deposition, CLARK was asked the following question: "No one brought Mr. Landskroner into the case because he was viewed as someone who would be the most zealous advocate available for Mr. Jones to pursue claims; correct?" CLARK replied, "That's — that's right." In his errata, the City changed CLARK's reply to, "I don't know why Mr. Paradis recommended him to Mr. Jones."

d. On or about March 6, 2019, shortly after LANDSKRONER invoked the Fifth Amendment in court in response to questions by the judge about whether any of his attorney's fees had been paid to PARADIS and the Special Counsels' representation of Jones was revealed in court, the City Attorney's Office announced that both PARADIS and KIESEL had stepped down or been terminated.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

e. On or about March 22, 2019, the City Attorney's Office announced that PETERS had resigned in the wake of media requests for information about PETERS' receipt of outside counsel referral fees unrelated to the LADWP billing litigation.

3. The City's April 26, 2019 filing and press release claiming that the KIESEL Emails had just been discovered

106. On April 26, 2019, under FEUER's name and at his direction, the City filed a "Notice Re: Documents" in the *City v. PwC* case. The Notice stated that "[o]n April 24, 2019, at approximately 5:30 p.m., counsel for the City learned that a .pst file labeled "Emails Responsive to PMQ(1).pst existed on a forensically imaged hard drive."[40] The Notice went on to describe certain emails between and among PARADIS, KIESEL, LANDSKRONER, and LIBMAN indicating that PARADIS and KIESEL had prepared and filed the *Jones v. City* complaint on behalf of LANDSKRONER and LIBMAN, along with other coordination. The Notice specifically noted that "No City employee or officer sent or received any of these emails." The Notice attached some of the emails and indicated that the emails had been produced to PwC after they were discovered.[41]

[40] According to multiple sources, including FEUER, the hard drive in question had been used by PETERS and, after PETERS's resignation, was forensically imaged by an outside vendor at the direction of the Browne George law firm representing the City after PETERS resigned in late March 2019.

[41] The omnibus affidavit articulated my understanding at that time that the .pst file — which the City's April 26, 2019 filing described as containing 131 records but attached only a fraction (approximately 29) of that number — contained at least some of the emails among City personnel that later emerged during the *PwC* litigation notwithstanding the City's stringent efforts to shield those emails from production. This

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

107. Contemporaneous with the City's Notice, the City issued a press release that included the following statement by Rob Wilcox, spokesperson for the City Attorney's Office:

> **The emails we've just discovered reveal a reprehensible breach of ethics** by outside lawyers in whom our office placed trust. **The conduct of outside counsel now coming to light** was outrageous and inexcusable.

108. I believe that the City's filing and public statement were intended to convey that no City official or employee, to include FEUER, knew about Special Counsel's coordination with LANDSKRONER and LIBMAN in advance of the *Jones v. City* complaint until the KIESEL Emails were discovered in a forensic review of PETERS' hard drive on April 24, 2019.

---

understanding was informed in part by information provided by KIESEL, and in part by my review of the complex and dynamic factual landscape of the *Jones* and *PwC* litigation.

The prosecution team's review of the contents of the .pst file was hindered by privilege protections and technical difficulties. Only after those issues were successfully mitigated was I finally able to review the contents of the file. This was after the omnibus affidavit was filed and when I learned that it contained 145 items. Several of these, in a folder marked "Deleted Items," were email chains and attachments that reflected communications between and among City employees and officials related to the LADWP billing litigation. The file did not contain other emails to and from City personnel that the City sought to shield and that later emerged.

I do not know how the City arrived at the count of 131 records itemized in its April 2019 notice, or whether the hard drive that the FBI obtained (from the City's vendor with assistance from the City) after execution of the search warrant was in the same condition as when it was earlier reviewed by the City's outside counsel. Nor is it clear whether the City's counsel, upon reviewing the .pst file and making the representation that none of the emails were sent to or from City employees or officials, viewed the items in the folder marked "Deleted Items." The FBI continues to investigate these and other questions related to the .pst file and the hard drive, both through forensic examination and through witness interviews and other investigative means.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

4. FEUER's initial interview with the prosecution team

109. On July 22, 2019, while agents were executing the July 2019 search warrants, including at the City Attorney's Office, FEUER met with the prosecution team and requested to be interviewed immediately. The interview was recorded, and I have reviewed the transcript.

110. During that interview, FEUER advised the government as follows:

Q: Are you aware of whether anybody in your office, including special counsel or anybody else, forwarded or provided internal privy information to the Jones litigators in order to help it achieve that hierarchy?

A: I would have been horrified, and had I been cognizant of that activity, whoever provided it would not have been engaged with the City, on the staff, or outside counsel then or ever again.

Q: Why is that?

A: Because I would not have considered that ethical behavior.

Q: Have you since learned that any of that occurred?

A: What I have since learned is that, because **I've seen email traffic that emerged fairly recently, in April** that —— especially Mr. Kiesel, and it appeared, from the email traffic, Mr. Paradis, had been assisting in the filing of the Jones and DWP litigation with Plaintiff's counsel.

And to anticipate a question, **around mid to late April, something in that time frame, three months ago or so, I received a phone call** from our counsel indicating that they had found, I think, a thumb drive or something on the computer that had not been opened. There had been attempts made to open it a couple times, and they had found a way to open it. And that that drive contained emails that I just referred to. And they described the content of those emails to me at that point. Maybe early April something like that. And we agreed on that conversation —— I remember the conversation. I was

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

> on my way to an event that night. **And we agreed that information had to be immediately disclosed to the Court and to opposing counsel.**

111. In the interview, FEUER further advised the government as follows as part of a lengthy statement about KIESEL's deposition testimony that the City directed his actions on behalf of the *Jones* plaintiff who sued the City:[42]

> A: "When the — **in April when I learned about the email exchange** and subsequent to that when there was testimony by Mr. Kiesel in deposition that our office was cognizant of that activity, it really made little sense to me."

112. During the interview, FEUER further stated as follows:

> A: **When the emails in mid to late April emerged**, I actually asked Mr. George to inquire as to whether [CLARK] knew anything about that.
>
> Q: To inquire of Mr. Clark?
>
> A: Yes. I don't remember for sure, but I believe that during that period his deposition was still forthcoming, and I wanted really to just create enough distance that Mr. Clark felt he could say whatever he thought the truth was about any of these issues.
>
> But Mr. George reported to me that he did ask Mr. Clark. He said Mr. Clark was infuriated by the **revelation of those emails.** And Mr. Clark . . . referred in passing to Mr. Kiesel has having perjured himself in his testimony with regard to whether our office was cognizant of any of these.
>
> **I asked Mr. George to ask Mr. Clark on or about April 20-something if he had any possible awareness of anything close to what was being memorialized in those emails.** To which Mr. George said Mr. Clark responded by becoming infuriated, said absolutely not, that's completely unethical, no one should ever do that. But was very - I was told was very exercised that someone he'd been working with had engaged in that behavior.
>
> . . .

---

[42] As FEUER's statement was not directly relevant to a pending question, no question is indicated here.

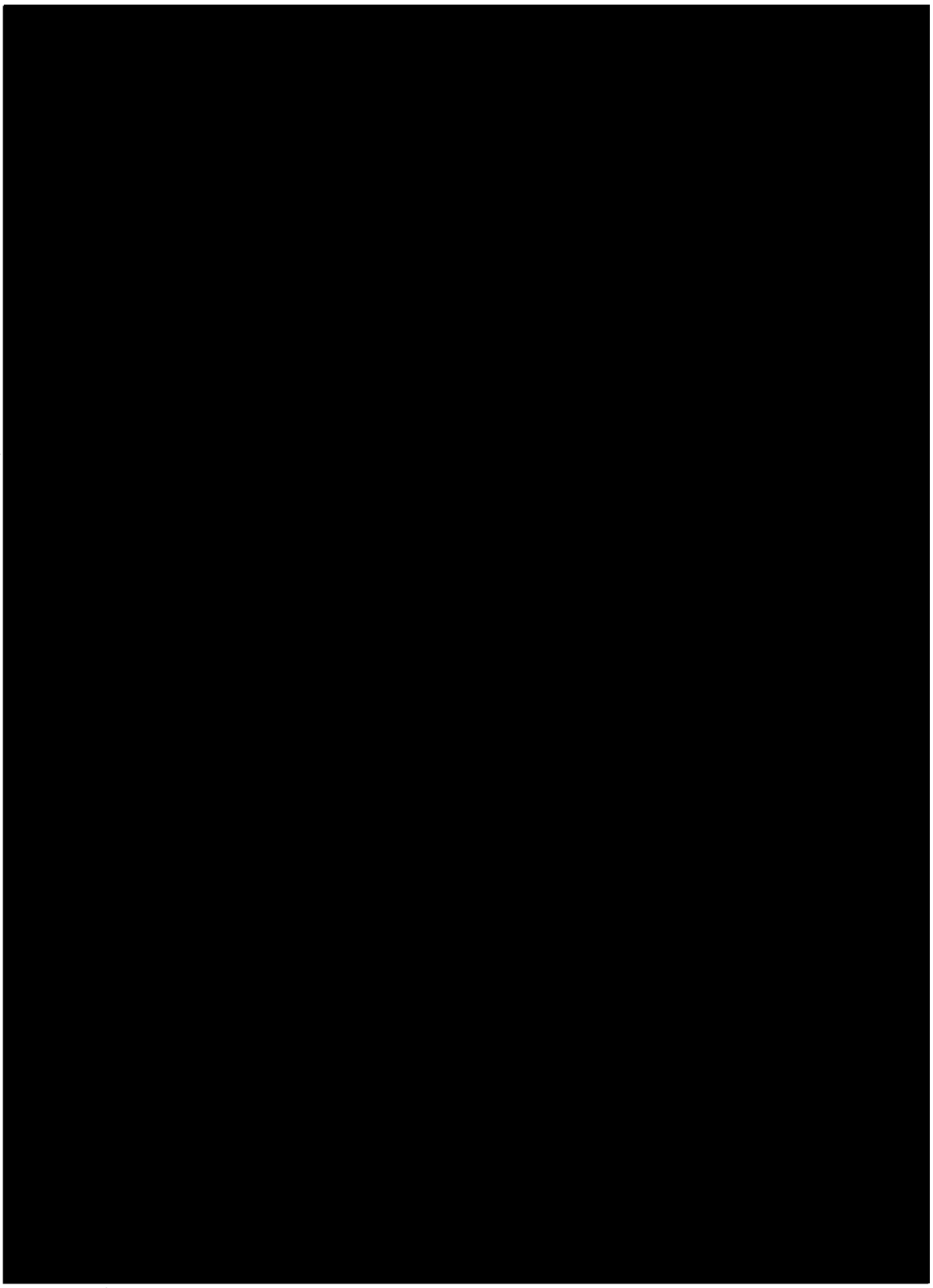
Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

> And I needed – **facts kept emerging of which I was unaware. The fact of the email, for example,** you know, what I thought we were at a stage where I thought I had a handle on what transpired, which – at that stage, with the exception of Mr. Landskroner invoking the Fifth Amendment [and] Mr. Paradis doing the same – **I thought I had a handle on exactly what had taken place here.**
>
> **And now this email exchange comes to light.**

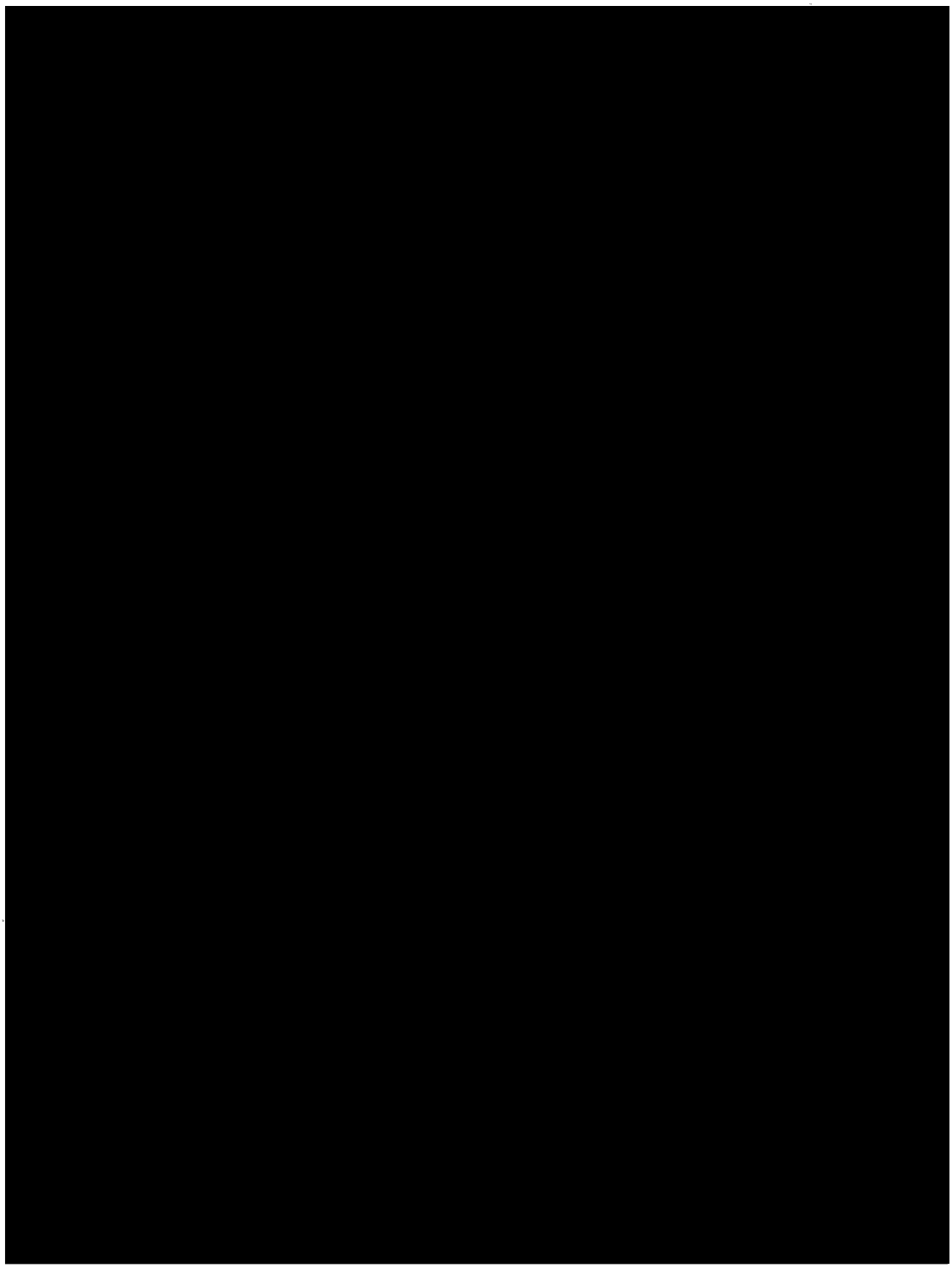
113. I believe that in these statements, FEUER intended to convey to the government that – consistent with the City's April 26, 2019 Notice and accompanying press release – FEUER had no awareness of Special Counsel's coordination with LANDSKRONER and LIBMAN in advance of the *Jones v. City* complaint until the KIESEL Emails were discovered in a forensic review of PETERS' hard drive on April 24, 2019. I further believe that these official statements by FEUER were material and misleading, based on the below-described evidence indicating that PETERS apprised FEUER in late January 2019 of both the existence of the KIESEL Emails and the damaging information that they likely contained, after which FEUER directed PETERS to take care of the KIESEL Emails, FEUER did not follow up to find out what was in the KIESEL Emails, and FEUER did not disclose the KIESEL emails to the Court or PwC. I believe that FEUER was motivated to provide such misleading statements in order to distance himself as far as possible from the, at minimum, unethical conduct engaged in by attorneys in his office and working on behalf of his office because of the resulting political damage to his reputation and that of the City Attorney's Office.

5. [redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB



Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB



Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

[redacted]

[redacted]

116. On August 13, 2019, FEUER testified in a deposition in the *PwC* case.[44] The deposition transcript reflects that FEUER testified as follows:

> **Q: On April 26, when this filing was made, did you authorize this filing?**
>
> **A. I directed it.**
>
> Q. Mr. Wilcox also made a statement on that day to The Los Angeles Times; is that correct?
>
> A. Correct.

[44] The information in this paragraph is derived from the deposition transcript, which I have reviewed.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Q. It accused Mr. Kiesel and Mr. Paradis of a egregious breach of ethics or a reprehensible breach of ethics, if I remember correctly; is that right?

A. Yes.

Q. Nothing was said about Mr. Peters; is that correct?

A. Correct.

. . .

Q: Did you have any understanding as to why Mr. Peters did not produce "Emails Responsive to PMQ" that had been provided to him by Mr. Kiesel's office?

A: At what time?

Q: On April 26, 2019.

A: My understanding was that the — that analysis had been done that revealed that there had not been — that the document had not successfully been opened.

Q: Did you understand that Mr. Kiesel's office had provided an email to Mr. Peters which provided him with instructions on how to open it and indicated that the name of the file was "Emails Responsive to PMQ"?

A: No.

Q: Do you have any understanding as to how — as to why it is that Mr. Peters says he didn't open a file called "Emails Responsive to PMQ" in preparation for a PMQ deposition that he was defending after a court order requiring the production of responsive documents?

A: No.

. . .

Q: **At the time that you learned about the documents, April 26,** did you have any concern about the fact that those documents had been identified as being responsive to the PMQ notice, that the second PMQ deposition had taken place after these documents were provided to Mr. Peters, and that Mr. Peters never produced them to PwC?

A: I wanted to know whether Mr. Peters was cognizant of the content of those documents at the time that they were transmitted to him.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

117. I believe that by this sworn testimony, FEUER intended to convey that he had no awareness of the facts that were ultimately revealed in the KIESEL Emails prior to learning about those emails shortly after his counsel discovered them on approximately April 24, 2019. I further believe that this sworn testimony was intended to convey that upon learning of the KIESEL Emails in late April 2019, FEUER immediately directed that the emails be filed with the court and produced to the defendant, and simultaneously authorized a statement condemning the conduct revealed by the emails as a "reprehensible breach of ethics." I believe that this testimony was misleading, given the evidence described herein. While false or misleading sworn testimony at a civil deposition in a state case would not, standing alone, violate federal law, it is consistent with what I perceive as FEUER's misleading or false narrative in an interview with the federal government [redacted] intended to convey that he was unaware of the KIESEL Emails until April 2019, when he immediately directed their disclosure.

6. Contacts regarding CLARK's and PETERS's depositions

118. On April 9 and April 29, 2019, CLARK provided additional testimony at his court-ordered PMQ deposition in the *PwC* case. CLARK prefaced his testimony with a prepared statement blaming poor preparation by his attorneys for what he described as his inaccurate testimony during his February 26, 2019 deposition. As noted above, I believe that his February 26

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

testimony was largely accurate, and that his subsequent errata purporting to correct critical parts of that testimony was largely inaccurate. CLARK's testimony on April 9 and April 29, 2019, was generally inconsistent with his February 26 testimony and consistent with his errata, and for the aforementioned reasons, I believe that CLARK's April 9 and April 26 testimony contained material false statements related to the collusive litigation described herein.

119. On May 1 and May 2, 2019, following his aforementioned March 2019 resignation from the City Attorney's Office, PETERS provided testimony at a court-ordered deposition in the *PwC* case. A review of PETERS' phone indicates no text messages between **CLARK's ACCOUNT** and PETERS after PETERS's March resignation until Monday, May 6, 2019. On May 6, 2019, one business day after PETERS' deposition testimony, CLARK texted PETERS from **CLARK's ACCOUNT** and asked PETERS to call him. After a series of text exchanges, the two men made an appointment for CLARK to call PETERS the following Friday afternoon using either **CLARK's ACCOUNT** or CLARK's home phone.

7. Contacts regarding KIESEL's deposition

120. On April 29, 2019, counsel for PwC contacted KIESEL and offered him an opportunity to sit for a deposition in which KIESEL could address what PwC viewed as the City's "Ro[gue] Special Counsel theory of the case, which is inconsistent with [PwC's] view of the evidence." KIESEL agreed. Before the end of May, KIESEL had agreed to be deposed in the *PwC* case.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

121. On April 30, 2019, PwC's counsel advised outside counsel for the City that PwC intended to take KIESEL's deposition in early May 2019. The City objected to that timing and invoked mediation, work-product, and attorney-client privilege objections to KIESEL's documents and testimony. After some scheduling discussions, a late May 2019 date was selected for KIESEL's deposition.

122. The City was by that time on notice that KIESEL would provide a narrative that was contrary to the City's, because by April 30, 2019 — responding to the City's press release accusing KIESEL of a "reprehensible breach of ethics" based on what was revealed by the KIESEL Emails — KIESEL provided the following media statement for an article published on the morning of April 30, 2019:

> I have always conducted myself with the highest level of ethics. Neither I nor my firm played any role in drafting the complaint. **This was done at the request of the city of Los Angeles.** The only thing reprehensible is the disingenuous spin coming out of the city attorney's office. **To be clear, I was completely open, direct and candid with everyone at all levels of the city attorney's office.**

123. On Friday, May 24, 2019, the business day before KIESEL was set to testify at his Tuesday, May 28, 2019 deposition,[45] CLARK called PETERS from **CLARK's ACCOUNT** and left a voicemail wherein CLARK stated that although they hadn't spoken in a few weeks, he was calling to discuss two issues, including the following: "I understand we're going to see each other on Tuesday [May 28], which I'd like to talk about."

[45] Monday, May 27, 2019, was the Memorial Day holiday.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. Based on the context and my knowledge of the investigation, and specifically the below-described information about CLARK and PETERS appearing collaboratively with the City at KIESEL's deposition the following Tuesday, I believe that CLARK was calling to discuss KIESEL's deposition and their plans for how it would be handled.

124. Later on May 24, 2019, CLARK left a subsequent voicemail for PETERS using **CLARK's ACCOUNT**. CLARK stated as follows:

> Hey Thom, it's Jim. We got cut off at a crucial point. Um. "The big question is, because" — and then I stopped hearing you. . . . We can talk about it on Tuesday.

a. I believe this message to mean that CLARK and PETERS had been speaking on the phone, and that after PETERS said, "The big question is, because," the call was cut off.

b. Based on the timing of these two messages and my knowledge of the investigation, I believe that the conversation that got cut off at a "crucial" point, but which could be continued on Tuesday, involved KIESEL's upcoming deposition the following Tuesday.

125. In a pair of subsequent text messages between **CLARK's ACCOUNT** and PETERS's phone on May 24, 2019, CLARK and PETERS agreed to continue their discussion "on Tuesday" due to PETERS's poor cell reception.

126. On May 28, 29, and 30, 2019, KIESEL testified at a deposition in the *PwC* case. KIESEL testified to facts that were contrary to the City's narrative about the *Jones* litigation,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

including that by February 2015, members of the City Attorney's Office authorized the plan to have Jones sue the City in order to obtain a favorable settlement of all of the existing class actions. KIESEL further testified that by early March 2015, both CLARK and PETERS were aware of the plan to file the *Jones v. City* complaint, and that both CLARK and PETERS were present when the decision was made for LIBMAN to serve as local counsel to LANDSKRONER, who had already been "recruited" to take over the representation of Jones.

127. KIESEL advised the government as follows with respect to his May 2019 deposition:

a. CLARK and PETERS attended KIESEL's deposition.

b. Despite the fact that PETERS had already abruptly resigned from the City Attorney's Office by that time, PETERS did not appear adverse to the City.

c. During breaks, CLARK and PETERS would huddle together with the City's outside counsel and look at KIESEL. CLARK's face was red, and "it looked like [CLARK] was going to have a stroke." KIESEL perceived these actions as an "intimidation tactic."

128. Based on the above information and my knowledge of the investigation, I believe that CLARK used **CLARK's ACCOUNT** to contact PETERS on May 24, 2019, to discuss KIESEL's upcoming deposition testimony, which the City had reason to know would be adverse to the City and contrary to the City's false or misleading narrative regarding the collusive litigation described herein.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

129. Again, I believe all of the foregoing narrative of apparent obfuscation, false and misleading statements, and omissions are part of FEUER's campaign to distance himself as far as possible from the, at minimum, unethical conduct engaged in by attorneys in his office and working on behalf of his office because of the resulting political damage to his reputation and that of the City Attorney's Office.

C. General Proffer Information about FEUER, KAPUR, BRAJEVICH, and CLARK

60. PETERS proffered that FEUER and KAPUR were very close, and that KAPUR usually attended PETERS' meetings with FEUER. PETERS opined that KAPUR had "extraordinary loyalty" toward FEUER, and that she was "very effective in enacting FEUER's directives." PETERS recalled that FEUER's schedule required him to be out of the office a lot, and that KAPUR did not generally travel with FEUER. However, PETERS believed that FEUER and KAPUR kept in close touch throughout the day and after hours on matters important to FEUER.

61. PETERS proffered that FEUER had hired BRAJEVICH for his current position as LADWP General Counsel, and that BRAJEVICH was "very well connected" in the City Attorney's Office and in political circles in the City more generally. PETERS believed that BRAJEVICH was somewhat close to FEUER. PETERS noted that on the *PwC* case, BRAJEVICH reported directly to FEUER, in light of CLARK's recusal from that matter.

62. PARADIS proffered to the government the following relevant information regarding BRAJEVICH:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

m. At one point, PETERS told PARADIS that he had told BRAJEVICH about Salgueiro's threats, and that BRAJEVICH was upset that the mediation of her demands had taken place at LADWP. PARADIS was unsure when this conversation with BRAJEVICH took place, other than it was during November or December 2017.

n. PARADIS did not recall specifically what PETERS said he had told BRAJEVICH. PARADIS had the sense that BRAJEVICH knew everything that FEUER knew about cases involving LADWP, but he could not provide a factual basis for that understanding.

o. PARADIS observed that BRAJEVICH was obsequious toward FEUER. PARADIS further proffered that although he did not witness many interactions between BRAJEVICH and FEUER and thus could not speak to the closeness of their relationship, he observed on multiple occasions BRAJEVICH "kissing up" to KAPUR, whom PARADIS understood to be FEUER's "gatekeeper."

118. PARADIS advised that he and BRAJEVICH "tolerated each other" but did not really like each other. PARADIS further informed the government that PARADIS and FEUER "hated" each other.

a. BRAJEVICH did not like to use email and frequently asked PARADIS not to discuss sensitive things with him by email but to instead contact him by phone or text.[46]

---

[46] WRIGHT proffered that BRAJEVICH was very careful about using both email and text messages, because of general concerns about discoverability. WRIGHT further noted that he was not aware of any nefarious reason for BRAJEVICH's caution about written communications.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

119. DAVID WRIGHT (former LADWP General Manager) proffered that BRAJEVICH — as an Assistant City Attorney assigned as General Counsel for LADWP — reported to FEUER. According to WRIGHT, the role of an LADWP General Counsel was to protect the City, and as such, BRAJEVICH's loyalties lay with the City Attorney's Office rather than with LADWP in instances where their respective interests diverged.

120. CLARK proffered that he and FEUER used to be very close, with a relationship of mutual trust and respect. However, after the FBI executed a search warrant at the City Attorney's Office, and specifically in CLARK's office, CLARK perceived that FEUER kept him at a distance.

D. Summary of Probable Cause for the TARGET ACCOUNTS

130. Based on my knowledge of the investigation and the information herein, I believe there is probable cause to believe that evidence of the Target Offenses and criminal schemes may be located in the **TARGET ACCOUNTS**. In particular, BRAJEVICH's use of **BRAJEVICH'S ACCOUNT** and **BRAJEVICH's EMAIL** to contact PETERS to discuss the KIESEL Emails and issues relating to disclosure in late January 2019, as well as other matters relating to the City's strategy in responding to allegations about the collusive litigation, indicates that **BRAJEVICH's ACCOUNT** and **BRAJEVICH's EMAIL** may contain evidence of the Target Offenses and criminal schemes.[47] Moreover, BRAJEVICH's reported caution in using email

[47] On or about December 6, 2019, I served on Microsoft an order pursuant to 18 U.S.C. § 2703(d) for **BRAJEVICH's EMAIL**. Microsoft advised that the only responsive information they had

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

and preference for telephonic communications further supports the probable cause to believe that **BRAJEVICH's ACCOUNT** will contain evidence of the Target Offenses and criminal schemes.

131. I believe that FEUER's use of **FEUER's EMAIL** and KAPUR's use of **KAPUR's EMAIL** to communicate with PETERS and each other about the City's strategy for responding to allegations of unethical conduct and a court order to reveal documents that were perceived as damaging to the City constitute probable cause to believe that evidence of the Target Offenses and criminal schemes will be found on **FEUER's EMAIL** and **KAPUR's EMAIL**.

132. I believe that CLARK's above-detailed use of **CLARK's ACCOUNT** to contact PETERS about matters related to the LADWP billing litigation, including KIESEL's anticipated deposition testimony that contradicted the City's false and misleading narrative about the collusive litigation, constitutes probable cause to believe that evidence of the Target Offenses and criminal schemes will be found in **CLARK's ACCOUNT**.

133. FEUER used **FEUER's ACCOUNT** to text PETERS, including in messages related to the collusive litigation. Specifically:

---

for **BRAJEVICH's EMAIL** was profile data confirming that the account was assigned to BRAJEVICH. In follow-up conversations, Microsoft informed me that the lack of other responsive information indicated to Microsoft that other responsive data (access logs and header information) indicated that it had been deleted. Microsoft was unable to determine when or by whom the data had been deleted, nor could they advise whether there was additional content available that would be potentially responsive to a search warrant. I believe that even if Microsoft has no content for **BRAJEVICH's EMAIL**, that fact may also constitute evidence of the Target Offenses and criminal schemes, including obstruction of justice.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. On July 18, 2015, during the period in which City was mediating the allegedly preordained settlement in the *Jones* case to resolve all of the class actions on terms favorable to the City, PETERS sent FEUER a text message on **FEUER's ACCOUNT** advising FEUER of KIESEL's cell phone number (which I assume, based on context and my knowledge of the investigation, FEUER had requested from PETERS). Later that day, FEUER acknowledged the information with a text from **FEUER's ACCOUNT** reading, "Thank you."

b. On March 12, 2019, within days of KIESEL's and PARADIS's withdrawal as Special Counsel, PETERS texted FEUER on **FEUER's ACCOUNT** to advise as follows relevant to the collusive litigation and the City's correlated public-relations problems:

> "Hello. Eric George [of the Browne George law firm] has agreed to take the case and has what is, in my view, a very solid approach to [Judge] Berle's and the press's concerns. I think you will benefit from learning the particulars. Eric also has a couple of tactical thoughts which you should hear and decide whether to approve. When able, please call him. [redacted]. Thank you."

i. As detailed above and in the omnibus affidavit, the Browne George law firm was involved in the City's media and public-relations strategy following the public revelation in March 2019 that PARADIS and KIESEL had represented Jones, and also in crafting FEUER's and the City's response to the discovery of the KIESEL Emails on PETERS's hard drive in April 2019. I believe that the use of **FEUER's ACCOUNT** to discuss the ongoing public-relations crisis — which FEUER was very concerned about and which I believe, as stated above,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

caused FEUER to make the false and/or misleading statements described herein — constitutes probable cause to believe that evidence of the Target Offenses and criminal schemes will be found on **FEUER's ACCOUNT**.

134. Moreover, the evidence shows that FEUER relied on members of his trusted inner circle — including CLARK, KAPUR, and possibly BRAJEVICH — and therefore, it is more likely that FEUER would have communicated with others, including **BRAJEVICH's ACCOUNT** and **CLARK's ACCOUNT**, about the facts underlying the Target Offenses and criminal schemes.

135. I believe that this evidence, coupled with other evidence -- including that articulated in the omnibus affidavit -- gives rise to probable cause to believe that the **TARGET ACCOUNTS** will contain evidence of violations of the Target Offenses and criminal schemes.

IX. BACKGROUND ON E-MAIL AND THE PROVIDERS

136. In my training and experience, I have learned that providers of e-mail and/or social media services offer a variety of online services to the public. Providers, like the PROVIDER, allow subscribers to obtain accounts like the **TARGET ACCOUNTS**. Subscribers obtain an account by registering with the provider. During the registration process, providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail or social media account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

payment (including any credit or bank account number). Some providers also maintain a record of changes that are made to the information provided in subscriber records, such as to any other e-mail addresses or phone numbers supplied in subscriber records. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of an account.

137. Therefore, the computers of a PROVIDER are likely to contain stored electronic communications and information concerning subscribers and their use of the PROVIDER's services, such as account access information, e-mail or message transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of a SUBJECT ACCOUNT.

138. A subscriber of a PROVIDER can also store with the PROVIDER files in addition to e-mails or other messages, such as address books, contact or buddy lists, calendar data, pictures or videos (other than ones attached to e-mails), notes, and other files, on servers maintained and/or owned by the PROVIDER. In my training and experience, evidence of who was using an account may be found in such information.

139. In my training and experience, e-mail and social media providers typically retain certain transactional information about the creation and use of each account on their systems.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail and social media providers often have records of the Internet Protocol ("IP") address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a **TARGET ACCOUNT.**

140. In my training and experience, e-mail and social media account users will sometimes communicate directly with the service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers of e-mails and social media services typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of a **TARGET ACCOUNT.**

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

141. I know from my training and experience that the complete contents of an account may be important to establishing the actual user who has dominion and control of that account at a given time. Accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. Given the ease with which accounts may be created under aliases, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of an account, investigators often have to rely on circumstantial evidence to show that an individual was the actual user of a particular account. Only by piecing together information contained in the contents of an account may an investigator establish who the actual user of an account was. Often those pieces will come from a time period before the account was used in the criminal activity. Limiting the scope of the search would, in some instances, prevent the government from identifying the true user of the account and, in other instances, may not provide a defendant with sufficient information to identify other users of the account. Therefore, the contents of a given account, including the e-mail addresses or account identifiers and messages sent to that account, often provides important evidence regarding the actual user's dominion and control of that account. For the purpose of searching for content demonstrating the actual user(s) of a **TARGET ACCOUNT**, I am requesting a warrant requiring the PROVIDER to turn over all information

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

associated with a **TARGET ACCOUNT** with the date restriction included in Attachment B for review by the search team.

142. Relatedly, the government must be allowed to determine whether other individuals had access to a **TARGET ACCOUNT**. If the government were constrained to review only a small subsection of an account, that small subsection might give the misleading impression that only a single user had access to the account.

143. I also know based on my training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as "lol" to express "laugh out loud"), or codewords (which require entire strings or series of conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of a message or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and parenthesis :) to convey a smile or agreement) to discuss matters. "Keyword searches" would not account for any of these possibilities, so actual review of the contents of an account by law enforcement personnel with information regarding the identified criminal activity, subject to the search procedures set forth in Attachment B, is necessary to find all relevant evidence within the account.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

144. This application seeks a warrant to search all responsive records and information under the control of the PROVIDER, which is subject to the jurisdiction of this court, regardless of where the PROVIDER has chosen to store such information.

145. As set forth in Attachment B, I am requesting a warrant that permits the search team to keep the original production from the PROVIDER, under seal, until the investigation is completed and, if a case is brought, that case is completed through disposition, trial, appeal, or collateral proceeding.

a. I make that request because I believe it might be impossible for a provider to authenticate information taken from a **TARGET ACCOUNT** as its business record without the original production to examine. Even if the provider kept an original copy at the time of production (against which it could compare against the results of the search at the time of trial), the government cannot compel the provider to keep a copy for the entire pendency of the investigation and/or case. If the original production is destroyed, it may be impossible for the provider to examine a particular document found by the search team and confirm that it was a business record of the provider taken from a **TARGET ACCOUNT**.

b. I also know from my training and experience that many accounts are purged as part of the ordinary course of business by providers. For example, if an account is not accessed within a specified time period, it -- and its contents

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

-- may be deleted. As a consequence, there is a risk that the only record of the contents of an account might be the production that a provider makes to the government, for example, if a defendant is incarcerated and does not (perhaps cannot) access his or her account. Preserving evidence, therefore, would ensure that the government can satisfy its Brady obligations and give the defendant access to evidence that might be used in his or her defense.

X. REQUEST FOR NON-DISCLOSURE

134. Pursuant to 18 U.S.C. § 2705(b), I request that the Court enter an order commanding the PROVIDER not to notify any person, including the subscribers of the **TARGET ACCOUNTS**, of the existence of the warrant until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date the requested warrant is signed by the magistrate judge, or such later date as may be set by the Court upon application for an extension by the United States. There is reason to believe that such notification will result in: (1) flight from prosecution; (2) destruction of or tampering with evidence; (3) intimidation of potential witnesses; (4) otherwise seriously jeopardizing the investigation; or (5) exposing the identities of confidential sources who have cooperated with the government and in some cases may continue to actively and covertly cooperate.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

XI. CONCLUSION

135. Based on the foregoing, I request that the Court issue the requested search warrants.

ANDREW CIVETTI, Special Agent
Federal Bureau of
Investigation

Subscribed to and sworn before
me on January 31, 2020.

Patrick J. Walsh

HONORABLE PATRICK J. WALSH
UNITED STATES MAGISTRATE JUDGE

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

UNITED STATES DISTRICT COURT

for the

Central District of California

ORIGINAL

In the Matter of the Search of: Information associated with accounts identified as [redacted]att.net; joseph.brajevich@ladwp.com; and associated with the phone number [redacted] that is within the possession, custody, or control of Apple Inc.	Case No. 2:20-MJ-00396

WARRANT PURSUANT TO 18 U.S.C. § 2703

To: Any Authorized Law Enforcement Officer

An application by a federal law enforcement officer requests the production and search of the following data:

See Attachment A-1

The data to be produced and searched, described above, are believed to contain the following:

See Attachment B

I find that the affidavit, or any recorded testimony, establishes probable cause to produce and search the data described in Attachment A-1, and to seize the data described in Attachment B. Such affidavit is incorporated herein by reference.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE HEREBY COMMANDED to serve this warrant on Apple Inc. at any time within 14 days from the date of its issuance.

Apple Inc. IS HEREBY COMMANDED to produce the information described in Attachment A within 10 calendar days of the date of service of this order. Apple Inc. **IS FURTHER COMMANDED** to comply with the further orders set forth in Attachment B, and, pursuant to 18 U.S.C. § 2705(b), shall not notify any person, including the subscriber(s) of the account/s identified in Attachment A-1, of the existence of this warrant.

The officer executing this warrant, or an officer present during the execution, shall prepare an inventory as required by law, and shall promptly return this warrant and the inventory to the United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE FURTHER COMMANDED to perform the search of the data provided by Apple Inc. pursuant to the procedures set forth in Attachment B.

Date and time issued: 1/31/2020 3:15 p.m. Patrick J. Walsh

Judge's signature

City and State: L.A., CA

Patrick J. Walsh, U.S. Magistrate Judge

Printed name and title

AUSA: Melissa Mills - Ext. 0627

Return	
Case No:	*Date and time warrant served on provider:*
Inventory made in the presence of:	
Inventory of data seized: [Please provide a description of the information produced.]	

Certification
I declare under penalty of perjury that I am an officer involved in the execution of this warrant, and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office. Date: _____ _____ *Executing officer's signature* _____ *Printed name and title*

ATTACHMENT A-1

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the Apple accounts associated with the below, and specifically including associated iCloud and iTunes accounts, that is within the possession, custody, or control of Apple Inc., a company that accepts service of legal process at 1 Infinite Loop, M/S 36-SU, Cupertino, California, 95014, regardless of where such information is stored, held, or maintained.

a. The Apple iCloud account, [redacted], associated with the phone number [redacted] and the name MIKE FEUER (**"FEUER's ACCOUNT"**);

b. The Apple iCloud account, [redacted], and Apple iCloud account, joseph.brajevich@ladwp.com, associated with the phone number [redacted] and the name JOSEPH BRAJEVICH (**"BRAJEVICH's ACCOUNT"**);

c. The Apple iCloud account associated with the phone number [redacted] and the name JAMES CLARK (**"CLARK's ACCOUNT"**).

ATTACHMENT B

I. SEARCH PROCEDURES INCLUDING PRIVILEGE REVIEW PROCEDURE

1. The warrant will be presented to personnel of Apple, Inc. (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below in Section IV.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.15.a. below), law enforcement agents and/or other individuals assisting law enforcement agents who are not participating in the investigation of the case and who are assigned as the "Privilege Review Team" will review the content records, according to the procedures set forth herein, to determine whether or not any of the content records appears to contain or refer to communications between an attorney, or to contain the work product of an attorney, or between a spouse and any person ("potentially privileged information"). The "Search Team" (law enforcement personnel conducting the investigation

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

and search and other individuals assisting law enforcement personnel in the search) will review only content records which have been released by the Privilege Review Team. With respect to the non-content information produced by the PROVIDER (see Section II.15.b. below), no privilege review need be performed and the Search Team may review immediately.

5. With respect to content records, the Search Team will provide the Privilege Review Team and/or appropriate litigation support personnel[1] with an initial list of "scope key words" to search for on the content records, to include words relating to the items to be seized as detailed below. The Privilege Review Team will conduct an initial review of the content records using the scope key words, and by using search protocols specifically chosen to identify content records that appear to be within the scope of the warrant. Content records that are identified by this initial review, after quality check, as not within the scope of the warrant will be maintained under seal and not further reviewed absent subsequent authorization or in response to the quality check as described below.

6. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for among the content records that are identified by the initial review and quality check described above as appearing to fall within the

[1] Litigation support personnel and computer forensics agents or personnel, including IRS Computer Investigative Specialists, are authorized to assist both the Privilege Review Team and the Investigation Team in processing, filtering, and transferring documents and data seized during the execution of the warrant.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

scope of the warrant, to include specific words like names of any identified attorneys or law firms and names of any identified spouses] or their email addresses, and generic words such as "privileged" and "work product". The Privilege Review Team will conduct an initial review of these content records by using the privilege key words, and by using search protocols specifically chosen to identify content records containing potentially privileged information. Content records that are not identified by this initial review as potentially privileged may be given to the Search Team.

7. Content records that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Content records determined by this review not to be potentially privileged may be given to the Search Team. Content records determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a Privilege Review Team Assistant United States Attorney ("PRTAUSA"). Content records identified by the PRTAUSA after review as not potentially privileged may be given to the Search Team. If, after review, the PRTAUSA determines it to be appropriate, the PRTAUSA may apply to the court for a finding with respect to particular content records that no privilege, or an exception to the privilege, applies. Content records that are the subject of such a finding may be given to the Search Team. Content records identified by the PRTAUSA after review as privileged will be maintained under seal by the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

investigating agency without further review absent subsequent authorization.

8. The Search Team will search only the content records that the Privilege Review Team provides to the Search Team at any step listed above in order to locate, extract and seize content records that are within the scope of the search warrant (see Section III below). The Search Team does not have to wait until the entire privilege review is concluded to begin its review for content records within the scope of the search warrant. The Search Team and the Privilege Review Team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

9. During its review, the Search Team may provide the Privilege Review Team and/or appropriate litigation support personnel with a list of additional "scope key words" or search parameters to capture the items to be seized as detailed below; any additional content records identified through this quality check must first be reviewed by the Privilege Review Team subject to the terms set forth herein before being released to the Search Team. This quality check is intended only to ensure that the initial scope key word review successfully eliminated only data outside the scope of the search warrant from seizure.

10. If, while reviewing content records or non-content information, either the Privilege Review Team or the Search Team encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

shall immediately discontinue its search pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

11. The Privilege Review Team and the Search Team will complete the search of non-content information and both stages of the search of the content records discussed herein as soon as is practicable but not to exceed 180 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the records beyond this 180-day period without first obtaining an extension of time order from the Court.

12. Once the Privilege Review Team and the Search Team have completed their review of the non-content information and the content records and the Search Team has created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the Search Team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, neither the Privilege Review Team nor the Search Team will access the data from the sealed original production which fell outside the scope of the items to be seized or was determined to be privileged absent further order of the Court.

13. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_000829
Page 829 of 1425

to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

14. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDER

15. To the extent that the information described in Attachment A is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each **TARGET ACCOUNT** listed in Attachment A:

a. All contents of all wire and electronic communications associated with the **TARGET ACCOUNT**, limited to that which occurred on or after December 1, 2014,[2] including:

i. All e-mails, communications, or messages of any kind associated with the **TARGET ACCOUNT**, including stored or preserved copies of messages sent to and from the account, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information

[2] To the extent it is not reasonably feasible for the PROVIDER to restrict any categories of records based on this date restriction (for example, because a date filter is not available for such data), the PROVIDER shall disclose those records in its possession at the time the warrant is served upon it.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

associated with each e-mail or message, and any related documents or attachments.

ii. All records or other information stored by subscriber(s) of the **TARGET ACCOUNT**, including address books, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files.

iii. All records pertaining to communications between the PROVIDER and any person regarding the **TARGET ACCOUNT**, including contacts with support services and records of actions taken.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), any alternate names, other account names or e-mail addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, **and including any changes made to any subscriber information** or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

services used, and including the dates on which such changes occurred, for the following accounts:

(I) the **TARGET ACCOUNT.**

ii. All user connection logs and transactional information of all activity relating to the **TARGET ACCOUNT** described above in Section II.15.a., including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations, and including specifically the specific product name or service to which the connection was made.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

16. For each **TARGET ACCOUNT** listed in Attachment A, the search team may seize all information between December 1, 2014, and the present described above in Section II.15.a. that constitutes evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding), namely:

a. Information relating to who created, accessed, or used the **TARGET ACCOUNT**, including records about their identities and whereabouts.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Retention of PAUL PARADIS and PAUL KIESEL, or entities related thereto, to represent the City of Los Angeles;

ii. Communications involving or relating to any party to, or to counsel for any party to, *Jones v. City of Los Angeles* (the "*Jones* matter") or *City of Los Angeles v. PricewaterhouseCoopers* (the "*PwC* matter"), including communications with or referencing MICHAEL FEUER, JAMES CLARK, THOMAS PETERS, PAUL PARADIS, PAUL KIESEL, GINA TUFARO, LEELA KAPUR, JOSEPH BRAJEVICH, Julissa Salgueiro, and other counsel and parties;

iii. Any lawsuit where the City was a party to the lawsuit and appears to have had a legal, representational, and/or financial interest in both sides of the lawsuit, including the *Jones* matter;

iv. The litigation of the *Jones* matter and the *PwC* matter, including discovery disputes, the deposition of the City's "person most qualified," and emails and other materials arguably or allegedly responsive to discovery demands or court orders;

v. Efforts to conceal the litigation practices of the City Attorney's Office's or members or representatives thereof in the litigation related to the LADWP billing system, including knowledge or direction of payments made or benefits

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

given to individuals or entities in an effort to discourage their revelation of those practices;

vi. Efforts to conceal actions by the City Attorney's Office or members or representatives thereof in the litigation related to the LADWP billing system, including shielding documents from production, filing false or misleading documents with the court, and offering false or misleading testimony;

vii. The City's actions, strategy, or tactics in responding to revelations or allegations of fraud, discovery violations, and unethical conduct in the litigation related to the LADWP billing system, including media outreach and contacts, litigation decisions, notification or lack of notification to the court of relevant developments, authorization of payment of hush money, and other actions;

viii. Negotiations or agreements relating to hush money payments offered to or solicited by any individual or entity to conceal business practices related to the LADWP billing litigation by the City Attorney's Office or members thereof, and communications relating thereto;

ix. Obstruction of justice, perjury, or false official statements related to the LADWP billing litigation;

x. Destruction or concealment of evidence related to the LADWP billing litigation.

c. Calendar or date book entries and notes, including calendars or date books stored on digital devices;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

d. All records and information described above in Section II.15.b.

IV. PROVIDER PROCEDURES

17. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. The PROVIDER shall send such information to:

18. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

19. IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 2705(b), that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A, of the existence of the warrant, until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date this warrant is signed by the magistrate judge or such later date as may be set by the Court upon application for an extension by the United States. Upon expiration of this order, at least ten business days prior to disclosing the existence of the warrant, the PROVIDER shall notify the filter attorney identified above of its intent to so notify.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

UNITED STATES DISTRICT COURT

for the

Central District of California

ORIGINAL

In the Matter of the Search of:
Information associated with account identified as Mike.Feuer@lacity.org ("**FEUER's EMAIL**") and Leela.Kapur@lacity.org ("**KAPUR's EMAIL**") that is within the possession, custody, or control of Google Inc.

Case No. 2:20-MJ-00397

WARRANT PURSUANT TO 18 U.S.C. § 2703

To: Any Authorized Law Enforcement Officer

An application by a federal law enforcement officer requests the production and search of the following data:

See Attachment A-2

The data to be produced and searched, described above, are believed to contain the following:

See Attachment B

I find that the affidavit, or any recorded testimony, establishes probable cause to produce and search the data described in Attachment A-2, and to seize the data described in Attachment B. Such affidavit is incorporated herein by reference.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE HEREBY COMMANDED to serve this warrant on Google Inc. at any time within 14 days from the date of its issuance.

Google Inc. IS HEREBY COMMANDED to produce the information described in Attachment A-2 within 10 calendar days of the date of service of this order. Google Inc. **IS FURTHER COMMANDED** to comply with the further orders set forth in Attachment B, and, pursuant to 18 U.S.C. § 2705(b), shall not notify any person, including the subscriber(s) of the account/s identified in Attachment A-2, of the existence of this warrant.

The officer executing this warrant, or an officer present during the execution, shall prepare an inventory as required by law, and shall promptly return this warrant and the inventory to the United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE FURTHER COMMANDED to perform the search of the data provided by Apple Inc. pursuant to the procedures set forth in Attachment B.

Date and time issued: 1/31/2020 3:15 p.m.

Patrick J. Walsh
Judge's signature

City and State: L.A., CA

Patrick J. Walsh, U.S. Magistrate Judge
Printed name and title

AUSA: Melissa Mills - Ext. 0627

Return	
Case No:	*Date and time warrant served on provider:*
Inventory made in the presence of:	
Inventory of data seized: [Please provide a description of the information produced.]	

Certification
I declare under penalty of perjury that I am an officer involved in the execution of this warrant, and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office. Date: _____ _____ *Executing officer's signature* _____ *Printed name and title*

ATTACHMENT A-2

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the accounts identified below, that is within the possession, custody, or control of Google, Inc., a company that accepts service of legal process at its headquarters located at Mountain View, California, regardless of where such information is stored, held, or maintained.

1. Mike.Feuer@lacity.org (**"FEUER's EMAIL"**)
2. Leela.Kapur@lacity.org (**"KAPUR's EMAIL"**)

ATTACHMENT B

I. SEARCH PROCEDURES INCLUDING PRIVILEGE REVIEW PROCEDURE

1. The warrant will be presented to personnel of Apple, Inc. (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below in Section IV.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.15.a. below), law enforcement agents and/or other individuals assisting law enforcement agents who are not participating in the investigation of the case and who are assigned as the "Privilege Review Team" will review the content records, according to the procedures set forth herein, to determine whether or not any of the content records appears to contain or refer to communications between an attorney, or to contain the work product of an attorney, or between a spouse and any person ("potentially privileged information"). The "Search Team" (law enforcement personnel conducting the investigation

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

and search and other individuals assisting law enforcement personnel in the search) will review only content records which have been released by the Privilege Review Team. With respect to the non-content information produced by the PROVIDER (see Section II.15.b. below), no privilege review need be performed and the Search Team may review immediately.

5. With respect to content records, the Search Team will provide the Privilege Review Team and/or appropriate litigation support personnel[1] with an initial list of "scope key words" to search for on the content records, to include words relating to the items to be seized as detailed below. The Privilege Review Team will conduct an initial review of the content records using the scope key words, and by using search protocols specifically chosen to identify content records that appear to be within the scope of the warrant. Content records that are identified by this initial review, after quality check, as not within the scope of the warrant will be maintained under seal and not further reviewed absent subsequent authorization or in response to the quality check as described below.

6. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for among the content records that are identified by the initial review and quality check described above as appearing to fall within the

[1] Litigation support personnel and computer forensics agents or personnel, including IRS Computer Investigative Specialists, are authorized to assist both the Privilege Review Team and the Investigation Team in processing, filtering, and transferring documents and data seized during the execution of the warrant.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

scope of the warrant, to include specific words like names of any identified attorneys or law firms and names of any identified spouses] or their email addresses, and generic words such as "privileged" and "work product". The Privilege Review Team will conduct an initial review of these content records by using the privilege key words, and by using search protocols specifically chosen to identify content records containing potentially privileged information. Content records that are not identified by this initial review as potentially privileged may be given to the Search Team.

7. Content records that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Content records determined by this review not to be potentially privileged may be given to the Search Team. Content records determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a Privilege Review Team Assistant United States Attorney ("PRTAUSA"). Content records identified by the PRTAUSA after review as not potentially privileged may be given to the Search Team. If, after review, the PRTAUSA determines it to be appropriate, the PRTAUSA may apply to the court for a finding with respect to particular content records that no privilege, or an exception to the privilege, applies. Content records that are the subject of such a finding may be given to the Search Team. Content records identified by the PRTAUSA after review as privileged will be maintained under seal by the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

investigating agency without further review absent subsequent authorization.

8. The Search Team will search only the content records that the Privilege Review Team provides to the Search Team at any step listed above in order to locate, extract and seize content records that are within the scope of the search warrant (see Section III below). The Search Team does not have to wait until the entire privilege review is concluded to begin its review for content records within the scope of the search warrant. The Search Team and the Privilege Review Team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

9. During its review, the Search Team may provide the Privilege Review Team and/or appropriate litigation support personnel with a list of additional "scope key words" or search parameters to capture the items to be seized as detailed below; any additional content records identified through this quality check must first be reviewed by the Privilege Review Team subject to the terms set forth herein before being released to the Search Team. This quality check is intended only to ensure that the initial scope key word review successfully eliminated only data outside the scope of the search warrant from seizure.

10. If, while reviewing content records or non-content information, either the Privilege Review Team or the Search Team encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_000842
Page 842 of 1425

shall immediately discontinue its search pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

11. The Privilege Review Team and the Search Team will complete the search of non-content information and both stages of the search of the content records discussed herein as soon as is practicable but not to exceed 180 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the records beyond this 180-day period without first obtaining an extension of time order from the Court.

12. Once the Privilege Review Team and the Search Team have completed their review of the non-content information and the content records and the Search Team has created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the Search Team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, neither the Privilege Review Team nor the Search Team will access the data from the sealed original production which fell outside the scope of the items to be seized or was determined to be privileged absent further order of the Court.

13. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_000843
Page 843 of 1425

to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

14. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDER

15. To the extent that the information described in Attachment A is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each **TARGET ACCOUNT** listed in Attachment A:

a. All contents of all wire and electronic communications associated with the **TARGET ACCOUNT**, limited to that which occurred on or after December 1, 2014,[2] including:

i. All e-mails, communications, or messages of any kind associated with the **TARGET ACCOUNT**, including stored or preserved copies of messages sent to and from the account, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information

[2] To the extent it is not reasonably feasible for the PROVIDER to restrict any categories of records based on this date restriction (for example, because a date filter is not available for such data), the PROVIDER shall disclose those records in its possession at the time the warrant is served upon it.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

associated with each e-mail or message, and any related documents or attachments.

ii. All records or other information stored by subscriber(s) of the **TARGET ACCOUNT**, including address books, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files.

iii. All records pertaining to communications between the PROVIDER and any person regarding the **TARGET ACCOUNT**, including contacts with support services and records of actions taken.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), any alternate names, other account names or e-mail addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, **and including any changes made to any subscriber information** or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

services used, and including the dates on which such changes occurred, for the following accounts:

(I) the **TARGET ACCOUNT**.

ii. All user connection logs and transactional information of all activity relating to the **TARGET ACCOUNT** described above in Section II.15.a., including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations, and including specifically the specific product name or service to which the connection was made.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

16. For each **TARGET ACCOUNT** listed in Attachment A, the search team may seize all information between December 1, 2014, and the present described above in Section II.15.a. that constitutes evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding), namely:

a. Information relating to who created, accessed, or used the **TARGET ACCOUNT**, including records about their identities and whereabouts.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_000846
Page 846 of 1425

b. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Retention of PAUL PARADIS and PAUL KIESEL, or entities related thereto, to represent the City of Los Angeles;

ii. Communications involving or relating to any party to, or to counsel for any party to, *Jones v. City of Los Angeles* (the "*Jones* matter") or *City of Los Angeles v. PricewaterhouseCoopers* (the "*PwC* matter"), including communications with or referencing MICHAEL FEUER, JAMES CLARK, THOMAS PETERS, PAUL PARADIS, PAUL KIESEL, GINA TUFARO, LEELA KAPUR, JOSEPH BRAJEVICH, Julissa Salgueiro, and other counsel and parties;

iii. Any lawsuit where the City was a party to the lawsuit and appears to have had a legal, representational, and/or financial interest in both sides of the lawsuit, including the *Jones* matter;

iv. The litigation of the *Jones* matter and the *PwC* matter, including discovery disputes, the deposition of the City's "person most qualified," and emails and other materials arguably or allegedly responsive to discovery demands or court orders;

v. Efforts to conceal the litigation practices of the City Attorney's Office's or members or representatives thereof in the litigation related to the LADWP billing system, including knowledge or direction of payments made or benefits

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

given to individuals or entities in an effort to discourage their revelation of those practices;

vi. Efforts to conceal actions by the City Attorney's Office or members or representatives thereof in the litigation related to the LADWP billing system, including shielding documents from production, filing false or misleading documents with the court, and offering false or misleading testimony;

vii. The City's actions, strategy, or tactics in responding to revelations or allegations of fraud, discovery violations, and unethical conduct in the litigation related to the LADWP billing system, including media outreach and contacts, litigation decisions, notification or lack of notification to the court of relevant developments, authorization of payment of hush money, and other actions;

viii. Negotiations or agreements relating to hush money payments offered to or solicited by any individual or entity to conceal business practices related to the LADWP billing litigation by the City Attorney's Office or members thereof, and communications relating thereto;

ix. Obstruction of justice, perjury, or false official statements related to the LADWP billing litigation;

x. Destruction or concealment of evidence related to the LADWP billing litigation.

c. Calendar or date book entries and notes, including calendars or date books stored on digital devices;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

d. All records and information described above in Section II.15.b.

IV. PROVIDER PROCEDURES

17. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. The PROVIDER shall send such information to:

18. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

19. IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 2705(b), that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A, of the existence of the warrant, until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date this warrant is signed by the magistrate judge or such later date as may be set by the Court upon application for an extension by the United States. Upon expiration of this order, at least ten business days prior to disclosing the existence of the warrant, the PROVIDER shall notify the filter attorney identified above of its intent to so notify.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
[redacted] Tarzana, California, 91356

Case No. 2:20-MJ-2994

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A-1

located in the Central District of California, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 371; 922(o) ; 922(a)(3) ; 1030; 1341; 1343; 1512; 1951; and 1956	Conspiracy; Possession of a machine gun; Illegal transportation of firearms; Unauthorized access of a computer; Mail Fraud; Wire Fraud; Witness Tampering; Extortion; and Money Laundering

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of_____days (*give exact ending date if more than 30 days*:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/

Applicant's signature

SA Julianne Mayfield – FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 6/26/2020

City and state: Los Angeles, CA

Patrick J. Walsh

U.S. Magistrate Judge Patrick J. Walsh

Printed name and title

AUSA: Melissa Mills

ATTACHMENT A-1

PROPERTY TO BE SEARCHED

The premises to be searched is located at [redacted], Tarzana, California, 91356, believed to be the residence of MICHAEL LIBMAN ("**LIBMAN HOME**") and pictured below. The residence is a detached two-story single-family home with a light beige exterior and a gated front yard. On the front curb of the residence is the number "[redacted]" painted in black. The number "[redacted] is also painted on the residence next to the garage door.

[redacted]

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 922(o) (Possession of a machine gun); 922(a)(3) (Illegal transportation of firearms); 1030 (Unauthorized access of a computer); 1341 (Mail Fraud); 1343 (Wire Fraud); 1512 (Witness Tampering); 1951 (Extortion); and 1956 (Money Laundering) (together, the "SUBJECT OFFENSES"), namely:

a. Records, documents, communications, or other materials from January 1, 2020, to the present discussing methods or tools for gaining unauthorized access to computers or computer networks, including the usage of encrypted software or surveillance tools to conceal access or the identity of those using them;

b. Records, documents, communications, or other materials from January 1, 2020, to the present involving foreign cybersecurity experts or any individual or entity in communication with **MICHAEL LIBMAN** about computer access, surveillance, intelligence, or other cyber-related operations;

c. Records, documents, communications, or other materials from January 1, 2020, to the present reflecting payments for hacking, computer fraud, electronic surveillance, or gaining unauthorized access to a computer;

d. Records, documents, communications, or other materials from January 1, 2020, to the present reflecting bank accounts or other financial instruments used to send or receive

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

funds derived from hacking, computer fraud, or gaining unauthorized access to a computer;

e. Records, documents, communications, or other materials from January 1, 2020, to the present reflecting plans to collect information about [redacted] or any existing collections of information about the same;

f. Audio recordings, pictures, video recordings, or still captured images involving hacking, computer fraud, electronic surveillance, or gaining unauthorized access to a computer, or the location of **MICHAEL LIBMAN** during the commission of such actions, from January 1, 2020, to the present;

g. Audio recordings, pictures, video recordings, or still captured images reflecting the purchase, sale, transportation, or distribution of firearms or ammunition, or the location of **MICHAEL LIBMAN** during the commission of such actions, from January 1, 2020, to the present;

h. Firearms, including handguns, shotguns, rifles, assault weapons, and machine guns, and records, documents, and tools used for or reflecting the ownership, manufacture, or maintenance of firearms or ammunition;

i. Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with sources of firearms;

j. Data, records, documents, or information (including electronic mail, messages over applications and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

social media, and photographs) from January 1, 2020, to the present reflecting efforts by **MICHAEL LIBMAN** to obtain, possess, use, apply for, or transfer money over $1,000, such as bank account records, cryptocurrency records, and accounts;

k. Address book information, including all stored, saved, or deleted telephone numbers, from January 1, 2020, to the present;

l. Call log information, including all telephone numbers dialed from the any digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls, from January 1, 2020, to the present;

m. SMS text, email communications, instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp) or other text or written communications, including evidence of deleted communications, from January 1, 2020, to the present, sent to or received from any of the digital devices mentioning [redacted] firearms, including machine guns, or the plans to access someone else's computer;

n. Contents of any calendar or date book from January 1, 2020, to the present;

o. Global Positioning System ("GPS") coordinates and other information or records identifying interstate travel routes from January 1, 2020, to the present; and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

p. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

q. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

a. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

3. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications or work product:

Non-Digital Evidence

4. Law enforcement personnel conducting the investigation ("the Investigation Team") may be present at the search, but may not search or review any item prior to it being given to them by the "Privilege Review Team" (previously designated individual(s) not participating in the investigation of the case).

5. The Privilege Review Team will review documents to see whether or not the document appears to contain or refer to communications between an attorney and any person or containing the work product of an attorney ("potentially privileged information"). Those documents not containing or referring to such communications or work product may be turned over to the Investigation Team for review.

6. In consultation with a Privilege Review Team Assistant United States Attorney ("PRTAUSA"), if appropriate, the Privilege Review Team member will then review any document identified as appearing to contain potentially privileged information to confirm that it contains potentially privileged information. If it does not, it may be returned to an Investigation Team member. If a member of the Privilege Review

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Team confirms that a document contains potentially privileged information, then the member will review only as much of the document as is necessary to determine whether or not the document is within the scope of the warrant. Those documents which contain potentially privileged information but are not within the scope of the warrant will be set aside and will not be subject to further review or seizure absent subsequent authorization. Those documents which contain potentially privileged information and are within the scope of the warrant will be seized and sealed together in an enclosure, the outer portion of which will be marked as containing potentially privileged information. The Privilege Review Team member will also make sure that the locations where the documents containing potentially privileged information were seized have been documented.

7. The seized documents containing potentially privileged information will be delivered to the United States Attorney's Office for further review by a PRTAUSA. If that review reveals that a document does not contain potentially privileged information, or that an exception to the privilege applies, the document may be returned to the Investigation Team. If appropriate based on review of particular documents, the PRTAUSA may apply to the court for a finding with respect to the particular documents that no privilege, or an exception to the privilege, applies.

Digital Evidence

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

8. The Privilege Review Team will also review seized digital devices as set forth herein. The Investigation Team will review only digital device data which has been released by the Privilege Review Team.

9. The Privilege Review Team will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location.

10. The Privilege Review Team and the Investigation Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

11. The Investigation Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified clients, names of any identified spouses, or their email addresses, and generic words such as "privileged" and "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. Documents or data that are identified by this initial review as not potentially privileged may be given to the Investigation Team.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

12. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Investigation Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRTAUSA. Documents or data identified by the PRTAUSA after review as not potentially privileged may be given to the Investigation Team. If, after review, the PRTAUSA determines it to be appropriate, the PRTAUSA may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Investigation Team. Documents or data identified by the PRTAUSA after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

13. The Investigation Team will search only the documents and data that the Privilege Review Team provides to the Investigation Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Investigation Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

and data within the scope of the search warrant if that is more efficient.

14. In performing the reviews, both the Privilege Review Team and the Investigation Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

15. If either the Privilege Review Team or the Investigation Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

16. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

17. If the search determines that a digital device does contain data falling within the list of items to be seized, the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

government may make and retain copies of such data, and may access such data at any time.

18. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

19. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

20. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

21. In order to search for data capable of being read or interpreted by a digital device, the Investigation Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

22. During the execution of this search warrant, law enforcement is permitted to: (1) depress **MICHAEL LIBMAN's** thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of **MICHAEL LIBMAN's** face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

23. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AFFIDAVIT

I, Julianne Mayfield, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since July 2017. I completed the FBI Basic Field Training Course in Quantico, Virginia, where I received over twenty weeks of training in the investigation of various crimes. I am currently assigned to a Public Corruption Squad, where I specialize in the investigation of corrupt public officials, including bribery, fraud against the government, extortion, and money laundering. In addition, I have received training in the investigation of public corruption and other white-collar crimes. I hold a Bachelor of Science degree in Homeland Security and Emergency Management, and a Master of Counterterrorism and Security Policy degree.

II. PURPOSE OF AFFIDAVIT

2. I make this affidavit in support of an application for a search warrant to search the premises of [redacted], Tarzana, California, 91356 ("**LIBMAN HOME**"), as described more fully in Attachment A-1, and the person of **MICHAEL LIBMAN**, as described more fully in Attachment A-2.

3. The requested search warrants seek authorization to search the above-referenced premise and person for evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 922(o) (Possession of a machine gun); 922(a)(3)

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

(Illegal transportation of firearms); 1030 (Unauthorized access of a computer); 1341 (Mail Fraud); 1343 (Wire Fraud); 1512 (Witness Tampering); 1951 (Extortion); and 1956 (Money Laundering) (the "SUBJECT OFFENSES"), as described more fully in Attachment B.

4. Upon receipt of the information described in Section II of Attachment B, law enforcement agents and/or individuals assisting law enforcement and acting at their direction will review that information to locate the items described in Section III of Attachment B subject to the search protocol and potential privilege review procedures outlined in Attachment B. Attachments A-1, A-2, and B are incorporated herein by reference.

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. RELEVANT PERSONS, ENTITIES, AND TERMS

6. MICHAEL LIBMAN is a Los Angeles-based attorney. Between 2015 and 2019, **LIBMAN** served as local counsel on behalf of the plaintiffs in *Jones v. City* (described below), who were

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

also represented by JACK LANDSKRONER, a Cleveland-based attorney.

7. PAUL PARADIS is a New York-based attorney. Between 2015 and 2019, PARADIS served as Special Counsel to the City of Los Angeles ("City") along with PAUL KIESEL in the *PwC Case* (described below).

a. PARADIS is the target of a related federal investigation into alleged corrupt activities at LADWP and the City Attorney's Office. PARADIS has no criminal history and has agreed to assist the government in exchange for favorable consideration in a future prosecution of him related to his conduct in the related matter.

b. PARADIS has provided the government access to his email account, cell phone, bank accounts, and many other documents during the government's investigation. PARADIS first met with the FBI in March 2019 in the presence of his attorney and has engaged in multiple consensual recordings at the direction of the FBI since then, some of which are detailed in this affidavit.

c. Much of the information provided by PARADIS has been substantially corroborated by other evidence. Where there has been a discrepancy between what PARADIS reported and other evidence, those discrepancies are referenced herein in footnotes 1, 10, and 21.[1]

[1] The government has previously identified a discrepancy unrelated to the investigation into **LIBMAN** in an affidavit by FBI Special Agent Andrew Civetti filed in January 2020. That

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

8. LOS ANGELES DEPARTMENT OF WATER AND POWER ("LADWP") is, according to its website, the nation's largest municipal utility, with a $7.5 billion annual budget for water, power and combined services for the City.

9. THE LOS ANGELES CITY ATTORNEY'S OFFICE, according to its website, "writes every municipal law, advises the Mayor, City Council and all city departments and commissions, defends the city in litigation, brings forth lawsuits on behalf of the people and prosecutes misdemeanor crimes[.]"

10. *Jones v. City of Los Angeles*, Case No. BC577267 ("*Jones v. City*") is a civil class action lawsuit filed against the City on April 1, 2015, in Los Angeles Superior Court, which alleged that LADWP overcharged the ratepayers of Los Angeles. The City resolved the suit, which included paying millions of dollars in attorney's fees to plaintiffs' counsel.

11. *City of Los Angeles v. PricewaterhouseCoopers*, Case No. BC574690 ("*City v. PwC*") is a civil case brought by the City against PricewaterhouseCoopers ("PwC") on March 6, 2015, in Los Angeles Superior Court, which alleged that PwC created a

---

discrepancy related to conflicting reports by PARADIS and KIESEL about a conversation the two of them had that had been initiated by KIESEL. Before returning KIESEL's call, PARADIS contacted the FBI and did not record at the FBI's direction. PARADIS reported that during the call, KIESEL asked a question about whether the two of them had spoken to an attorney for the City in January 2019. PARADIS reported that he did not provide a substantive answer, but attempted to jog KIESEL's memory by reminding him about a location significant to the conversation that PARADIS recalled. KIESEL reported that PARADIS had answered the question in the affirmative. Because of a lack of an apparent reason for either of them to lie about this issue, Agent Civetti concluded that this discrepancy in their accounts was either a misunderstanding or a memory lapse.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

faulty billing system resulting in the overcharges. On September 27, 2019, the City abruptly dismissed the *City v. PwC* lawsuit with prejudice, abandoning its pursuit of hundreds of millions of dollars allegedly owed to the City on behalf of LADWP ratepayers.

12. [redacted]

IV. SUMMARY OF PROBABLE CAUSE

14. The FBI is investigating **LIBMAN** for conspiring to hire an Israeli hacker to illegally access the phone and e-mail accounts belonging to [redacted] for the purpose of advantaging **LIBMAN**'s position in various active and contemplated lawsuits. In March 2020, **LIBMAN** approached PARADIS (who, unknown to **LIBMAN** was at the time actively cooperating with the FBI), and sought PARADIS's participation in this plan. During a series of consensually recorded calls and in-person meetings, including several video conferences with an individual representing himself as an Israeli hacker named "BEN" and located in Portugal, **LIBMAN** (and PARADIS, acting at the direction of the FBI) agreed to jointly pay BEN around $70,000 to access the victims' emails and text messages without their permission.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

15. During the course of their discussions about the computer intrusion scheme, **LIBMAN** also informed PARADIS that **LIBMAN** was in the process of acquiring several firearms, some from out of state, including a "machine gun" and an "Uzi."

V. STATEMENT OF PROBABLE CAUSE

A. Overview of Collusive Litigation Investigation

16. Since 2019, the FBI and U.S Attorney's Office has been investigating collusive litigation practices and several related criminal schemes involving *Jones v. City* and *City v. PwC*.

17. In December 2014, PARADIS approached a contact at the City Attorney's Office and proposed a lawsuit against PwC in connection with the LADWP's overbilling practices. At the time, several class action lawsuits were already pending against the City related to LADWP's overcharges. PARADIS represented a ratepayer, Antwon Jones, and proposed that Jones also file a ratepayer action against PwC.

18. In early 2015, the City Attorney's Office told PARADIS that he could not represent both Jones and the City in connection with the proposed lawsuits against PwC because of practical, strategic, and ethical concerns raised by another outside counsel for the City. PARADIS thereafter referred Jones to LANDSKRONER, an Ohio-based attorney, and **LIBMAN** was brought in to serve as local counsel in California. PARADIS filed *City v. PwC* in March 2015, and **LIBMAN** and LANDSKRONER filed *Jones v. City* in April 2015.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

19. In August 2015, without discovery production or any motion practice, an agreement was reached between LANDSKRONER and **LIBMAN** and the City of Los Angeles to settle *Jones v. City* for $67,000,000. The final settlement included an approximately $10,000,000 fee to LANDSKRONER, with approximately $1,650,000 of that fee being paid to **LIBMAN**. The settlement was eventually approved by Judge Berle in July 2017 over several objections from other plaintiffs with earlier-filed cases who argued that the City exhibited favoritism toward the *Jones v. City* plaintiffs and had agreed to pay LANDSKRONER and **LIBMAN** extraordinarily high fees relative to their comparatively limited hours of work.

20. While the *Jones v. City* case was ongoing, PwC was vigorously challenging the claims brought by the City in *City v. PwC* and alleging collusion between the City and LANDSKRONER (who was suing the City in *Jones v. City*). In early 2019, Judge Berle ordered the deposition of LANDSKRONER, who declined to answer questions regarding fee sharing with other counsel after invoking his Fifth Amendment privilege against self-incrimination. LANDSRKONER thereafter withdrew from the case, and the City terminated its representation by PARADIS as Special Counsel in *City v. PwC*.

21. In April 2019, Judge Berle appointed private attorney Brian Kabateck to replace **LIBMAN** and LANDSKRONER as class counsel for the LADWP ratepayers in the ongoing class action lawsuit due to his reported concerns about the legitimacy of the settlement.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

22. Around the same time, the FBI began investigating PARADIS for his role in several criminal schemes, including, among others: (1) a $2.175 million kickback from LANDSKRONER to PARADIS related to PARADIS's referral of the *Jones v. City* case to LANDSKRONER; (2) an $800,000 hush-money payment to a prospective whistleblower by PARADIS and his co-counsel in exchange for silence as to collusive and potentially fraudulent litigation practices at the City Attorney's Office; (3) the offering of bribes by PARADIS, and acceptance of those bribes by the then-LADWP manager and then-LADWP Board Vice President, in exchange for supporting at least one $30 million LADWP contract with PARADIS's company; and (4) the manipulation of a court-appointed "independent monitor" who was supposed to oversee the *Jones v. City* settlement.[2]

23. The City ultimately dismissed its lawsuit against PwC in September 2019. In a joint filing by the City and Kabateck, the City alleged that there was "substantial evidence of an improper relationship" between the City's former special counsel (including PARADIS) and the private attorneys involved in *Jones v. City* (**LIBMAN** and LANDSKRONER). The same day, the City and Kabateck jointly filed a motion seeking to disgorge

[2] On July 18, 2019, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized several search warrants for 6 premises and 19 email accounts related to the investigation into these collusive litigation practices and other criminal schemes, including for several offices located at the City Attorney's Office and LADWP (the "July 2019 search warrants"). The July 2019 search warrants and their supporting affidavits are available for the Court on request.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

the fees that had been paid to **LIBMAN** and LANDSKRONER and prevent any additional fees from being paid to them.

24. **LIBMAN** remains a subject in the investigation into the alleged collusive litigation practices.

25. In addition to PARADIS, several other individuals are actively cooperating with the government. No charges have yet been filed, and the investigation is ongoing.

B. LIBMAN Approaches PARADIS and Proposes That They Covertly Work Together to "Expose" [redacted] By Obtaining "Dirt" On Them

26. On March 13, 2020, PARADIS informed the FBI that LIBMAN had contacted him through PARADIS's attorney and requested a private meeting. At the FBI's direction, PARADIS then placed a recorded call to **LIBMAN** who asked to meet with PARADIS in person and said it was "not a phone conversation for what I wanted to discuss with you." The two agreed to meet at a restaurant in Tarzana, near **LIBMAN's** office.

27. Before the meeting, the FBI met with PARADIS and outfitted him with a recording device. PARADIS then proceeded to the restaurant and made contact with **LIBMAN**. During their recorded conversation, **LIBMAN** communicated the following to PARADIS:

a. **LIBMAN** told PARADIS that he wanted "to expose" what **LIBMAN** believed to be an unethical relationship between [redacted] and that **LIBMAN** claimed there was a way to get this information "properly" and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

"legally."[3] **LIBMAN** sought to brainstorm with PARADIS how to show a corrupt connection between [redacted] and posited that once this relationship was exposed, the "bullshit dismissal" of the PwC case could be "reversed" and an additional five to ten million dollars in fees which **LIBMAN** believed he was owed in *Jones v. City* would be released. **LIBMAN** also hoped to obtain leverage for three additional lawsuits that he intended to file against the City.

b. **LIBMAN** explained that he recently traveled to Israel in February 2020 and "met with some people and some entities," including some people that "have the capabilities to get the information that needs to be, uh, obtained."[4] **LIBMAN** described how these "people" claimed to have experience with a specific Israeli cyber intelligence unit, "Unit 8200,"[5] and how he was in current contact with them on "how to get this done," but that "they are not going to be cheap."

[3] Based on the full context of **LIBMAN**'s statements, as relayed below, in this and other conversations described herein where **LIBMAN** indicated that he wanted to obtain the information "properly" and "legally," I believe that **LIBMAN** was deliberately using false exculpatory language in order to shield himself from potential criminal liability.

[4] I have reviewed Customs & Border Protection travel records for **LIBMAN** that confirm he took international flights in February 2020 to and from Germany. The travel records show only egress from and ingress to the United States and would not show whether **LIBMAN** took a connecting flight from Germany to Israel.

[5] Based on my training and experience and knowledge of the investigation, I am familiar with the existence and activities of "Unit 8200", a division of the Government of Israel that is responsible for both offensive and defensive cyber operations worldwide. Similar to the United States' National Security Agency, Unit 8200 is an Israeli Intelligence Corps unit that collects signal intelligence and code decryption.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

c. **LIBMAN** said he wanted "to expose the true corruption that is going on now," [redacted] "because we are being thrown under the bus." **LIBMAN** emphasized that "we need the dirt. To expose how deep it goes." To do that, **LIBMAN** explained, "we need the intel." **LIBMAN** also said "we just need hard evidence, hard things that we can use, properly, without getting fucked ourselves, to expose them."

d. In terms of timing, **LIBMAN** explained that his goal was to establish quickly the personal connections between [redacted] "We're going to turn the tables on them, very simple. **Then everyone caves, and everybody compensates us eventually**." PARADIS said he just cared about restoring his reputation, and **LIBMAN** replied in part that "when they pay with money, it says everything." **LIBMAN** indicated that he would be setting up a meeting with his Israeli cybersecurity contacts in person somewhere in the United States, maybe in Miami.

e. During their conversation, **LIBMAN** and PARADIS also discussed finances, including what **LIBMAN** expected to pay for this operation, what he expected to receive financially as a result of it, and his request that PARADIS also contribute money. **LIBMAN** later added "I don't part with money easily. I like to know what I'm getting. **We need to be able to absorb some risk**. It's all going to be, and it has to be, you and I." **LIBMAN** did not want to include PAUL KIESEL in the scheme, because "**the number of people that need to know about this I can count on one hand**: you and I, and the third party" (which, in

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

context, I understood to mean the purported Israeli hacker). **LIBMAN** added that he "**took a risk contacting you**," but that **LIBMAN** and PARADIS "have the same problem." In terms of cost, **LIBMAN** explained that "it's not going to be cheap. Expensive. **Good information always is**." When asked for additional details by PARADIS, **LIBMAN** stated that he estimated the price to be "ballpark it's going to be six figures . . . . We need the info and I want to be as close as possible to certain before I pay a dime." LIBMAN further explained that he had some trust in the hacker and the hacker's associates because, "they are active," "they have a track record," and they "are checked out."

f. During the conversation, PARADIS stated that [redacted] is sloppy with his electronics, between texts and emails it will be clear," and **LIBMAN** replied "we just need to uncover [the connection between [redacted]] and we'll be golden." **LIBMAN** also said that the money would be "spent judiciously and wisely to produce results," and PARADIS replied that he hoped the "return on investment is high," to which **LIBMAN** responded "it needs to be very high, otherwise it's bullshit."

g. In the same conversation, **LIBMAN** made several references to establishing secure communications between himself and PARADIS. **LIBMAN** stated, "**we don't communicate, this is the last time we communicate like this**," and asked PARADIS if he used Protonmail or Signal (which, based on my training and experience and knowledge of the investigation, I know are an encrypted e-mail service and an encrypted messaging application,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

respectively).[6] PARADIS confirmed he had used Signal or Confide, another encrypted messaging application that also utilizes disappearing messages, and **LIBMAN** confirmed they would "use Confide," and "then we'll exchange the information." PARADIS asked **LIBMAN** if he had a "burner" phone[7] through which to discuss their plans and offered to procure one for **LIBMAN**.

C. During a Series of Recorded Calls, LIBMAN and PARADIS Plan How to Obtain Information about their Intended Victims Using LIBMAN's Israeli Cybersecurity Contact

28. On March 16, 2020, in a consensually recorded call, **LIBMAN** and PARADIS continued to discuss their plans:

a. **LIBMAN** confirmed that he had spoken to his Israeli cybersecurity contact and stated that he and PARADIS needed to provide more information to the contact "and then coordinate where we meet." PARADIS proposed that they consider

---

[6] Based on my training and experience and knowledge of the investigation, I am aware that encrypted e-mail and messaging applications use a form of file transfer protection where only the sender and recipient can view the communication. Installation, setup, and use of encrypted services usually involves verification through the cellular telephone number of the intended user. The use of encrypted services can make outside surveillance of such communications very difficult, thereby further concealing the sender and recipient's conversations.

[7] Based on my training and experience and knowledge of the investigation, I am aware that "burner phones" and their corresponding telephone numbers are phones that are typically purchased in cash without identification, thereby concealing the true owner and method of payment. Burner phones are often used to conceal the activities of their owners (phone calls, texts, Internet searches, etc.), and are often used between two parties who may be planning to commit an illegal act. While engaging in recorded communications with another target of the LADWP investigation at the direction of the FBI, PARADIS and that other target used burner phones.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

using a contact of PARADIS's (which would allow the FBI to introduce an undercover agent).[8] **LIBMAN** asked if they could trust that PARADIS's guy was "not somebody who could be a double agent and sell the information back at a higher price to . . . our detractors or our opponents?" PARADIS responded "listen, he's doing something that's illegal for us . . . it's not going to be something where he's going to be in a position to be selling anything," and that "he got me some incredible shit" in other cases "but he had to break several laws doing it." **LIBMAN** did not comment on or object to these references by PARADIS to illegality or breaking laws. PARADIS stated that he was simply offering his contact as an alternative to someone from outside the United States who would need to navigate pandemic-related travel restrictions. **LIBMAN** and PARADIS continued to discuss other areas to meet, including Mexico, and the likelihood that **LIBMAN's** contact would not be able to travel to the United States in the near future.

b. PARADIS indicated that his contact had asked for what specific information they needed. PARADIS asked **LIBMAN**, "we are looking for what from [redacted], all [redacted] emails, some of [redacted] emails, like what are you thinking?" **LIBMAN** replied, "I mean look, **this is not something . . . I want to discuss over the phone**...number one," and "number two, there are ways to get things, information that we need." **LIBMAN** stated, "we need to

[8] PARADIS's "contact" was a fictionalized cybersecurity professional invoked at the direction of the FBI as a proposed alternative to **LIBMAN's** Israeli connection. All references to that contact herein were part of that FBI-directed ruse.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

talk about this thing in terms of legally, whatnot, illegally, my guy is able to do things, I guess, well the word illegally with him never came up, however they are going to do it I don't know, I don't want to know, and I personally do not intend to break any laws. Okay?" But **LIBMAN** opined that he and PARADIS "need to meet" to discuss the matter in person and the "bottom line, is get me the shit."[9]

c. **LIBMAN** explained that he "dug up some things" to provide his contact as a starting point, but his contact "wanted more information so he can give me a better timeline." **LIBMAN** conveyed that the contact would then be able to "follow up on this [information provided by **LIBMAN**] and then come bearing gifts," which I understood from context to be a reference to **LIBMAN**'s desire for proof that the contact was able to access non-public information about the victims.

d. In case it became necessary, **LIBMAN** also gave PARADIS the address for the **LIBMAN HOME** and said it was his private address.

---

[9] Based on my training and experience, my knowledge of the investigation, and the context of this conversation, this exchange reflects another example of **LIBMAN** making false exculpatory statements. As an initial matter, this conversation featured **LIBMAN's** reluctance to speak about the SUBJECT OFFENSES on the phone and his stated preference to discuss those matters in person, which I understand to indicate **LIBMAN's** concerns about incriminating himself over the phone. I am also aware that criminal conspirators often make false exculpatory statements on which to rely later in the event that they or another co-conspirator attracts the attention of law enforcement. I am further aware that deliberate ignorance of the law is not a defense to the SUBJECT OFFENSES, and that **LIBMAN's** claim to be willfully blind to the legality of his co-conspirators' conduct would not shield him from criminal liability.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

e. **LIBMAN** indicated he would speak to his contact again and tell him "we need to move faster," with the goal to "meet face to face as soon as possible." PARADIS asked if **LIBMAN** was comfortable paying his contact in cash so that "there's no fucking receipts, there's no wire, there's no nothing," and **LIBMAN** responded that "that was not discussed yet, but I assumed that that was going to be the form."

29. On March 17, 2020, at the FBI's direction, PARADIS placed a recorded call to **LIBMAN** and, in part, inquired about the status of **LIBMAN's** contacts with the Israeli cybersecurity contact. PARADIS again proposed that they consider using PARADIS's contact, but **LIBMAN** wanted to hear back from **LIBMAN's** contact before pursuing an alternative person. **LIBMAN** indicated that the location of potential meetings was complicated by rapidly evolving travel restrictions and believed his contact was, at some point, located in Portugal. **LIBMAN** proposed that they play the plan "hour by hour."

30. On March 23, 2020, PARADIS placed a consensually recorded call to **LIBMAN**.[10] In this call, PARADIS expressed surprise that he had not heard anything back from **LIBMAN** and asked for the status. **LIBMAN** explained that he had forwarded along some information to his contact but had not heard anything back. Pursuant to their prior discussion, PARADIS

[10] Immediately prior to PARADIS's call with **LIBMAN** on March 23, 2020, I recall instructing PARADIS not to initiate further contact with **LIBMAN**. PARADIS does not recall receiving such an instruction and expressed a belief that he had been instructed to make this contact with **LIBMAN**. Per his normal operating procedure, PARADIS reported the contact to me immediately after placing the call to **LIBMAN**.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

confirmed that he could have burner phones for the two of them to use and suggested meeting in person, and **LIBMAN** agreed that "we need to talk." **LIBMAN** wanted to hold off on "Plan B" (a reference to meeting PARADIS's proposed alternative cybersecurity contact). They made plans to meet over the weekend to exchange the burner phones and discuss further.

31. On March 25, 2020, at the FBI's direction, PARADIS placed a consensually recorded call to **LIBMAN** after receiving a missed call from **LIBMAN**. During their conversation, **LIBMAN** indicated that he had "just heard from my guy" about the information **LIBMAN** had provided, and that he was "waiting for feedback from his, uh, team mate, uh, team member, or, you know, operational guy." PARADIS expressed concern about waiting too long and whether that meant **LIBMAN** was backing out, and **LIBMAN** replied that "yes, I want to see how we proceed -- the issue becomes, if we want to proceed, how?" **LIBMAN** further stated, "from my perspective, I want to move forward, okay?," "we need to expose the corruption, okay?," and "**remember I [LIBMAN] approached you** [PARADIS]." **LIBMAN** also indicated that he wanted to take advantage of the 30-day COVID-19-related hiatus declared by the courts. PARADIS indicated that he understood that **LIBMAN** "want to take advantage now, of the time, of the downtime to have these guys to do the hacking stuff now, if they can," and **LIBMAN** responded "hacking, schmacking, I don't know what it is, but I want to talk to them about what feedback means." In this and other conversations where **LIBMAN** claimed that he did not want to use the word

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

"hacking" and purported to distance himself from knowledge of the contemplated crimes, as described herein, I believe that LIBMAN was deliberately using false exculpatory language in order to shield himself from potential criminal liability. That is, if their plan was uncovered, he could later rely on such statements to falsely indicate that he lacked the requisite intent to commit the crimes they were discussing.

32. On March 31, 2020, in a consensually recorded call between **LIBMAN** and PARADIS, **LIBMAN** and PARADIS continued to discuss the SUBJECT OFFENSES:

a. **LIBMAN** indicated that he had just spoken to his "people" and stated that the "next conversation has to be sort of face to face, or somehow secure," since **his contacts had information that they "don't want to share on an unsecured line**." **LIBMAN** then asked PARADIS if PARADIS had "access to those phones," which I understood from context to be a reference to the burner phones PARADIS offered to obtain in the March 13 conversation.

b. **LIBMAN** then asked whether PARADIS was working for the authorities, including the FBI, and whether PARADIS was recording their conversations, and PARADIS replied he was not. I believe that this and other references by **LIBMAN** to the FBI and the authorities indicate his awareness of the criminality of the SUBJECT OFFENSES that they were discussing.

c. **LIBMAN** said he also wanted "to talk numbers too, if they go nuts on me on us then we're going to have to think about it some other way. . . . They are not the only route let's

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

put it this way." Based on context and my knowledge of the investigation, I understand this to mean that **LIBMAN** wanted to discuss the terms of payment with his contact, and that if **LIBMAN** was not satisfied with those proposed terms, he would find another co-conspirator with whom to work toward the SUBJECT OFFENSES.

d. PARADIS asked if **LIBMAN** had received any indication of the content of the materials that they would be paying for, and **LIBMAN** replied that he had not and that they needed to meet in person with his contact.

e. **LIBMAN** again reiterated the need for a secure line to speak with his contacts,[11] where "**nobody can listen in on, nobody can record, nobody can tap in to [their discussions]**." **LIBMAN** and PARADIS then discussed how to introduce PARADIS to **LIBMAN's** contacts, with **LIBMAN** expressing concern because he had not mentioned PARADIS's existence to them yet and that his contacts already "ran me," which I understood to be a reference to a background check. PARADIS explained that he himself had recently been vetted when he traveled to Israel, and **LIBMAN** responded that "these people, it's not the same . . . it's people from, let's put it this way, to be honest, I don't know how deep or whatnot because they also aren't, no one comes with a resume." Based on this description by **LIBMAN** of the shadowy nature of his contacts, **LIBMAN**'s previous explanation that his contacts had high-level connections with the Israeli

[11] Throughout **LIBMAN** and PARADIS' conversations, **LIBMAN** goes back and forth between referencing multiple Israeli contacts and referencing one specific contact temporarily located in Europe.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

military and specifically cybersecurity organizations, and the type of assistance that **LIBMAN** was seeking, I believe that **LIBMAN's** Israeli contact in Portugal and the contact's colleagues are likely highly sophisticated hackers.

f. **LIBMAN** and PARADIS then continued to brainstorm potential meeting locations given the travel restrictions. The call concluded with **LIBMAN** again urging PARADIS to "get [him] those phones, can you get me those phones," which I understand as a reference to the burner phones that they had previously discussed using as a means of secure communication. PARADIS indicated he would and asked for **LIBMAN's** address for shipping the phones. **LIBMAN** then told PARADIS that his home address was the **LIBMAN HOME** at the address specified above.

33. On April 2, 2020, in a consensually recorded call, PARADIS and **LIBMAN** agreed to meet at PARADIS's hotel the following Saturday, April 4, 2020, to exchange the burner phone in person.

D. LIBMAN and PARADIS Meet in Person on April 4, 2020, and Agree to Meet with an Israeli Hacker Virtually on April 8, 2020, to Discuss Terms

34. On April 4, 2020, **LIBMAN** and PARADIS met in PARADIS's hotel room as planned. Before the meeting, I met with PARADIS and outfitted him with several recording devices and provided him with two burner phones that the FBI had purchased and configured.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

35. During their in-person meeting, **LIBMAN** again discussed the benefit of retrieving private information between [redacted] via the Israeli hackers.

a. PARADIS inquired as to **LIBMAN's** connection to the Israeli hackers, asking, "So when you spoke to your guy in Israel, and then he put you in touch with these people? **LIBMAN** replied, "Correct . . . it's legit, I met with a whole team of people . . . in Israel." **LIBMAN** stated that he "met with people that have the, uh, entity in place, it's a big entity, it's not Black Box."[12] **LIBMAN** opined that Black Box was "too slick," and that another Israeli technology firm, NSO,[13] was "too hot." **LIBMAN** described his current contacts as "way below the radar...the ones who I'm talking to is the operational." **LIBMAN** stated that he communicated with his contacts using an encrypted messaging application.

b. **LIBMAN** told PARADIS that on the upcoming call with his contact, he planned to tell his contact that his "partner," referring to PARADIS, wanted to join their call.

---

[12] Based on my training and experience and knowledge of the investigation, I know that Black Cube is a private Israeli intelligence agency founded by former Israeli intelligence officers that specializes in high-profile intelligence operations for private parties. According to Black Cube's website, they claim, "we never use intimidation, blackmail or hacking to obtain information." Given the context, I believe that **LIBMAN's** reference to "Black Box" was a reference to Black Cube.

[13] Based on my training and experience and knowledge of the investigation, I know that NSO Group Technologies is another private Israeli technology company that develops software that can be used to enable remote surveillance of smartphones.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

c. **LIBMAN** explained that his contact would not personally be executing the contemplated hacking, and that his contact was an "operational" actor rather than a technical actor. Specifically, **LIBMAN** stated, "This is not the hacker, I don't get the sense, he's not acting like a hacker. He is the operational guy . . . **quite frankly, I don't want to know [the hackers],** do you? I don't give a fuck. I want to know what results they can deliver." Based on context, I believe that **LIBMAN's** description of his contact as "operational" is referring to the fact that his contact was coordinating the hacking operation with **LIBMAN** and PARADIS and was likely working in conjunction with others who would assist in the underlying collection of information. I further believe that **LIBMAN's** statement that he "[doesn't] want to know" who is doing the hacking is an attempt to create plausible deniability should their plot become uncovered.

36. During the meeting, PARADIS also gave **LIBMAN** the FBI-acquired burner phone ending in -0858 (the "**BURNER PHONE**"). PARADIS asked **LIBMAN** not to communicate with the Israeli hackers without him present. **LIBMAN** agreed to abide by that request.

37. On April 6, 2020, the Honorable Charles F. Eick issued an order authorizing the installation and continued use of a pen register and trap and trace device, on (1) the **BURNER PHONE**, and (2) the cellular telephone number ending in -6009 subscribed to by **LIBMAN** with AT&T ("**LIBMAN PHONE**"). The

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

resulting records show that **LIBMAN** has used both the **BURNER PHONE** and the **LIBMAN PHONE** to contact PARADIS.

38. On April 7, 2020, in a consensually recorded call with PARADIS, **LIBMAN** advised that he had informed his contact that PARADIS was a participant. **LIBMAN** further relayed that his contact had asked **LIBMAN** if **LIBMAN** trusted PARADIS, and that **LIBMAN** had replied, "as much as I trust you buddy." **LIBMAN** explained that the conversation with the Israeli contact would occur in "two steps": first the technical discussions, and then the discussions about money. **LIBMAN** stated that he liked this two-phased approach. **LIBMAN** stated that the hacker had cautioned him not to be "too open and comfortable talking, over, you know, on the phones . . . no matter how secure you think it is."

39. PARADIS asked if he and **LIBMAN** would be able to speak after the call with the Israeli contact, and **LIBMAN** confirmed that they could, stating, "we are the masters of the deal." **LIBMAN** agreed to meet with PARADIS again in person in the same hotel once PARADIS could get a room.

40. On April 8, 2020, **LIBMAN** and PARADIS met as planned at a hotel for approximately two hours (after PARADIS met with the FBI and was outfitted with recording devices) and had the following conversation before speaking with the Israeli contact:

a. Before calling the hacker, PARADIS asked **LIBMAN** for clarification on what **LIBMAN** had already provided to his contact. **LIBMAN** explained that he had provided [redacted] email

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

address, home address, and cell phone number via "email, or actually the secure website," but that he had not yet provided any information about [redacted] because he claimed he could not find anything. **LIBMAN** encouraged PARADIS to be quiet, stating, "if it sounds like you're interrogating him, you'll spook him." **LIBMAN** stated that he planned to describe his relationship with PARADIS as follows: "We are allies. We are not partners, we are allies. We have a common, common adversaries here. . . . We feel are corrupt and they are trying to use their power corruptly to, uh, harm us . . . we need to expose it. We are officers of the court and we are acting as such. I'm an officer of the court, doing my investigation. Simple." I understand the above statement as an attempt by **LIBMAN** to justify and distance himself from doing anything wrong.

b. **LIBMAN** again clarified that the first call would be about "methodology" and the second call "about money." **LIBMAN** advised that he had only spoken briefly "no more than a couple minutes here or there . . . on the phone" and then "the secure texts we have." **LIBMAN** stated that he trusted his contact, reiterating that he had been connected to his Israeli contact through "a big-deal guy in this [Israeli cybersecurity] community" after meeting "face to face . . .in Israel."

c. PARADIS asked whether, on this call, LIBMAN expected his Israeli contact to "tell us some shit he found to entice us?" **LIBMAN** replied, "I hope so. I told him flat out if you want business, gotta give us something to legitimize the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

information that they're gonna give us is worth something. I'm not gonna pay for something I can get myself on the Internet, I'm not paying you to do a Google search." **LIBMAN** further stated, "**We need information . . . that's not publicly available**. Fucking get it. Tell me, show me that you can get it, first, okay? . . . and then tell me how much you want. . . . Give me a taste. Give me a good taste."

41. Following the above-described preliminary conversation between **LIBMAN** and PARADIS during this meeting on April 8, 2020, **LIBMAN** used the BURNER PHONE to contact his Israeli contact via videoconference using an encrypted application.[14] **LIBMAN** and PARADIS then had the following discussion, in part, with the Israeli contact, whom **LIBMAN** called "BEN":

a. BEN explained his general experience and method of operation. BEN described the operational phase of his business as "three isolated solutions: investigation, intelligence, and influence." BEN stated that his team handles "the intelligence and investigations," that the "methods that we use is the, as they say, you know by way of deception," and that the work could also involve human intelligence. BEN explained that his group's specialty "is that we don't get credit." His group "does not exist in the system" even if you were to Google it, you would find nothing. "We not Black Cube . . . they are

[14] During the meeting, **LIBMAN** also expressed concern that the BURNER PHONE was an Android, noting that "the FBI can fucking hack. That's why I started doing this shit with Apple." I believe that this and other references by **LIBMAN** to his attempts to evade detection by the FBI suggests his awareness that the SUBJECT OFFENSES are illegal.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

friends of mine. . . . We prefer to be a boutique company. . . . Tell us what you want, and we deliver." Based on context and my knowledge of the investigation, I understand BEN's statements to convey that his company offers a variety of investigative and intelligence services (including "human intelligence," meaning information gained from human sources, and "technology," meaning information gained from technical sources), and that it operates in the shadows.

b. The timetable, BEN explained, would depend on whether **LIBMAN** and PARADIS wanted human intelligence. That process could take "one month to four months" to build the network of human sources required for such work. **LIBMAN** explained that "what we need is the two targets that we identified so far," which based on context I understood to mean [redacted], and asked for evidence of a "lead that there is quality information between the connection that will show us, that yes, we're on the right track and we need to invest money in that specific direction." BEN replied "there is nothing I can tell you, because if you do OSINT,[15] today, if you look at OSINT, just to go deeper, and then we start charging." Based on context and my knowledge of the investigation, I understand this to mean that **LIBMAN** was asking for a sample of information that BEN could provide demonstrating

[15] From my training and experience and knowledge of the investigation, I understand "OSINT" as a commonly used shorthand for open-source intelligence, or a gathering of information using publicly available resources.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

the connection between [redacted], and that BEN replied that he could not provide such a sample for free.

c. **LIBMAN** asked what BEN needed from them to start, and BEN replied that he would "send you a few questions" soliciting information that would help BEN understand what **LIBMAN** wanted. BEN also explained that the money would go to pay for infrastructure to conceal who was behind their work, because "**you can never point a finger, not against you, and not against us**. . . I never work differently . . . I work anonymous . . . we're not working with a, a, high profile. We are working with low profile, totally dark. So this is the infrastructure. You have to create good infrastructure that in any future, the backward investigation, they are going to end with nothing." Based on the context, I understand that BEN was explaining that he and his colleagues planned to conceal their conduct for their and **LIBMAN**'s mutual benefit because everyone understood that the SUBJECT OFFENSES were illegal.

d. **LIBMAN** again asked BEN for what BEN could "give us, tell us, show us . . . that you can have the potential to deliver what we need to deliver." As an example of his work, BEN provided some information about a project he had done for a Brazilian telecommunications company, implying that he had helped resolve a personnel issue within the company involving a person who was suspected of taking kickbacks, and offered to

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

send additional information that would confirm that BEN's work had been behind the successful resolution of the issue.[16]

e. The next step, BEN explained, would be for BEN to give a price and then for **LIBMAN** and PARADIS to "say okay. And that's it. A Jewish way of doing business, no contract, no contract, no nothing." **LIBMAN** replied "I like that. What contract? Enforceable where? In what court?," and everyone laughed. BEN indicated he would send the above-described additional information regarding his successful work in another case, as well as his questions, to **LIBMAN** "from another number" (referencing a Spanish number and a Turkish number).

f. Near the end of the call, BEN and **LIBMAN** had a brief exchange in Hebrew.

g. After concluding the call with the Israeli hacker, **LIBMAN** and PARADIS continued to discuss the plan and what they had learned, as described below:

h. Immediately after disconnecting the call, **LIBMAN** opined that BEN's use of Hebrew at the end meant "they're legit," because "I never told them that I know Hebrew and that I'm an Israeli citizen. They ran me . . . they were able to get that information that's not publicly available anywhere. They have their sources."

i. **LIBMAN** again told PARADIS that when he traveled to Israel, **LIBMAN** met "with Black Cube," who "wanted a half a million to a million, I told them fuck no . . . . First of all,

[16] The additional information that BEN sent to **LIBMAN** is described below.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

show me what you can, and they start talking about money too fast." **LIBMAN** explained that he "used" his daughter's exchange trip to Israel "as cover and an opportunity" to approach these Israeli cybersecurity contacts in Black Cube. LIBMAN added, "I went to see my daughter, I have pictures of my daughter . . . but my purpose was . . . you know . . . to meet with some people. . . . I did meet with several, and this guy he's talking with put me in touch with him, Roy, he's the heavy hitter." **LIBMAN** also stated, "I've been communicating with this guy [Roy] since back in February." Based on the context, I understand this to mean **LIBMAN** was taking steps toward the SUBJECT OFFENSES as early as February 2020.

j. **LIBMAN** asked PARADIS, "are you more or less at ease now" after the call with BEN, and PARADIS advised that he was more at ease. **LIBMAN** then stated to PARADIS, "you're like me, you're fucking paranoid" and PARADIS agreed. **LIBMAN** further stated, "I'd rather be alive paranoid than a dead hero, or imprisoned hero," which I believe was another statement conveying **LIBMAN's** awareness that they were discussing engaging in illegal activity.

k. **LIBMAN** and PARADIS agreed to wait and review the article about the Brazilian company that BEN agreed to send and also see what his questions were, at which point then **LIBMAN** would call PARADIS to discuss next steps.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

E. LIBMAN and PARADIS Continue to Discuss the SUBJECT OFFENSES Via Phone Calls

42. On April 9, 2020, in a consensually recorded call between **LIBMAN** and PARADIS, **LIBMAN** indicated that he had received from BEN via WhatsApp an article about the work for the Brazilian company that BEN had described, but that he could not glean anything relevant from it aside from an oblique reference to "Israel," which could in part be due to the translation of the article from Portuguese into English. At PARADIS's suggestion, **LIBMAN** agreed to inquire with BEN about the status of the questions BEN was going to send, and the two would reserve judgment until seeing what the questions were.

43. On April 10, 2020, in a consensually recorded call between **LIBMAN** and PARADIS, PARADIS informed **LIBMAN** that he had reviewed the article provided by BEN and believed that BEN was "much more valuable than you might have given him credit for."

44. The following morning, on April 11, 2020, in a consensually recorded call between **LIBMAN** and PARADIS, PARADIS explained that he believed that the materials from BEN showed a very "thorough job," that "there was no way this was just hacking, this is human intel," to which **LIBMAN** replied "got it, got it, got it." PARADIS stated, "I'm sure they did hack as well, and/or phone messages, texting, whatever," to which LIBMAN replied "uh huh, uh huh." **LIBMAN** indicated that he had texted BEN to inquire about the status of the questions BEN was going to send, but had not heard back. **LIBMAN** expressed confidence in BEN's work, reminding PARADIS that **LIBMAN** "flew

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to Israel" because he "didn't want this over telephone, I wanted in person, I took the effort, initiative . . . vetted out the guy . . . who referred me," who **LIBMAN** described as "very legit." **LIBMAN** and PARADIS then discussed their shared dislike of [redacted], with **LIBMAN** describing [redacted] not omnipotent, we're going to do something else with [redacted] where [redacted] gonna be impotent . . . **we're going to castrate them both. Because I'm not here to take any prisoners or give them an opportunity to get back at me. When they are down we are going to put them down in such a way that they can't get up at us. You understand that. Gloves are off, gloves are off**." Specifically, **LIBMAN** explained that he wanted information to include in a lawsuit against [redacted] on the basis that they tortiously interfered with his contract.

45. On April 12, 2020, **LIBMAN** used the BURNER PHONE to send PARADIS via text message a series of questions that **LIBMAN** indicated were the anticipated questions from BEN. The questions sought basic biographical information about the victims, including "electronic address," mobile telephone numbers, address, social media information, cars, and relatives.

46. On April 14, 2020, in a consensually recorded call between **LIBMAN** and PARADIS, **LIBMAN** and PARADIS had a lengthy conversation about what they contemplated paying for with BEN:

a. **LIBMAN** asked PARADIS what he thought, and PARADIS replied that PARADIS was confused about what BEN could do based

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

on the questions. Specifically, PARADIS explained that when they met at the Tarzana restaurant, he understood **LIBMAN** to be seeking "email and texts" for [redacted], not human intelligence, and "if I understood you correctly, you wanted stuff that we could not get access to other than electronically, by hacking the emails, hacking the texts . . . is that a fair assessment? . . . . Because then we can talk about . . . what we want to pay for, I want to make sure you and I are on same page mentally." **LIBMAN** responded that he "would not use the word hacking," since that is a "pretty strong word to use," and he would prefer to use the word "access" or "sources of information," including "access to information not available to us, and not easily publicly available."[17] They then continued to discuss what they were paying for in this first stage with BEN, and PARADIS said, "I call it hacking, you call it access, whatever. I don't care what you call it. It's texts and emails, that's where the shit's buried."

b. PARADIS posited that BEN was offering electronic access that would not leave any "fingerprints," and that BEN had "unique ways to get access with emails and texts." **LIBMAN** explained that he did not know the details of how they worked, that they "don't necessarily need to know, and frankly don't really care." PARADIS said that just because they don't know the details of how BEN operated did not mean they wouldn't be

[17] As stated above, based on the entirety of their conversations and my knowledge of this investigation, I believe **LIBMAN** again to be utilizing false exculpatory statements and semantics in attempt to later protect himself should their plot be uncovered by law enforcement.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

legally responsible for his actions, and "if he's accessing electronically emails for [redacted], [redacted] texts, their texts, and stuff like this, I get that. That's what we want. **But to pretend I don't know, you don't know, I don't know, to me that's more dangerous frankly**." **LIBMAN** replied, "**Okay, I see your point**." I believe this exchange is further evidence that **LIBMAN** was attempting to create plausible deniability as to the criminality of the SUBJECT OFFENSES with his statements that he was unaware of or uninvolved in criminal activity related to their pursuit of information related to [redacted]. **LIBMAN** offered his opinion that the only way to proceed was in "phases," with "no commitment to full-blown thing until we know what we can get access to."

c. **LIBMAN** repeated several times in the conversation that he did not want to know the details of how BEN would get the information. Specifically **LIBMAN** noted that even though they were talking on a "secure phone," "in terms of legal and pretending and what not, I'm not pretending anything, all I know is that, and all I want it to be, in terms of obtaining information that is difficult to obtain, I don't necessarily need to know the methodology, and the methodology may be exactly what it is, a trade secret, and if I don't know, all I know is we hired a private investigator to obtain information for us, okay? That's it." **LIBMAN** then gave the example of a court case where attorneys had hired a private investigator who had in fact hacked into phones illegally, and "the investigator went down, the lawyers did not." From **LIBMAN**'s point of view, "as long as

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

I'm not directing it, I'm not giving him any specific instructions . . . I don't need to know. . . . Sometimes ignorance is bliss."[18] When PARADIS again referenced BEN potentially "accessing [redacted] email," **LIBMAN** interrupted to say, "I don't know what the fuck he's going to do. Bottom line is this. Here is what we need. Go get it." Based on my knowledge of the investigation and the context, including other statements by **LIBMAN** as described herein, I understand this exchange to mean that **LIBMAN** wanted BEN to obtain non-public information on [redacted] via unauthorized access to their email accounts and cell phones, but that **LIBMAN** also wanted to distance himself from the specific methods of unauthorized access because **LIBMAN** believed that doing so would insulate him from criminal liability for the SUBJECT OFFENSES.

d. **LIBMAN** and PARADIS discussed their confusion about BEN's biographical questions. **LIBMAN** wondered aloud why BEN was asking for publicly available information that BEN should have been able to get, but **LIBMAN** ultimately concluded that it would save them money to not have to pay BEN to get that information when they could easily obtain it themselves. PARADIS stated that he did not understand why BEN needed license

[18] From my conversations with the assigned AUSAs, I am aware that, under Ninth Circuit Model Jury Instruction 5.8 (Deliberate Ignorance), one may be found to have "knowingly" committed a crime if the defendant "(1) was aware of a high probability that [e.g., drugs were in the defendant's automobile], and (2) deliberately avoided learning the truth. You may not find such knowledge, however, if you find that the defendant actually believed that [e.g. no drugs were in the defendant's automobile], or if you find that the defendant was simply negligent, careless, or foolish."

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

plate numbers, when what they were looking for was "text and email." **LIBMAN** opined that since they did not know BEN's methodology, they should "hope for the best, prepare for the worst," because "the fact that they are asking us for this information means they can dig deep."

e. The two agreed that they wanted to see what BEN could do at a distance first, especially given the pandemic. **LIBMAN** stated, "all we are doing is we are essentially hiring a sophisticated investigator to obtain information for us. That's it." **LIBMAN** stated, "Right now everybody is electronic. The whole world is overwhelmed. Now is the time to address electronic information gathering aspect." **LIBMAN** also stated that he wanted the issue of money and payment to come first from BEN, not from them. PARADIS asked **LIBMAN** what he was comfortable paying depending on what BEN was able to deliver, and **LIBMAN** said "everything in baby steps." **LIBMAN** asked PARADIS whether he thought they were "talking about a few dozen thousands, or up to a hundred grand," in terms of an advance for BEN. **LIBMAN** and **PARADIS** agreed they were comfortable with that range of $25-50 thousand from each of them.

f. With regard to how they would respond to the specific requests for information from BEN, **LIBMAN** noted he had already provided BEN with [redacted] information using publicly accessible databases. PARADIS suggested that they could probably get some of [redacted] information from KIESEL, but **LIBMAN** rejected the idea because he believed KIESEL to be "under FBI microscope." **LIBMAN** stated that the "more people you involve in

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

this shit, the more weak links in the chain you create." **LIBMAN** also expressed concerns about "leav[ing] a trail," which I believe further demonstrates his awareness that what he was doing was wrong.

47. On April 21, 2020, in a consensually recorded call between **LIBMAN** and PARADIS, PARADIS inquired about the status of **LIBMAN**'s communications with BEN. **LIBMAN** stated that he had not located [redacted] information and opined that they now needed to find "[redacted] private email," in case [redacted] was using that while working from home during the pandemic. **LIBMAN** stated that his motive in pursuing this information again was "**to fuck them [redacted] up and get our damages and money out of it** that we're entitled to," and he discussed the lawsuits he intended to file. **LIBMAN** and PARADIS agreed to arrange another video conference with BEN for the following Friday or whenever he was available.

F. LIBMAN and PARADIS Meet in Person on April 24, 2020, and Speak Again with the Israeli Hacker and Each Other about the SUBJECT OFFENSES

48. On April 24, 2020, **LIBMAN** and PARADIS met again in PARADIS's hotel room as planned. Before the meeting, the FBI met with PARADIS and outfitted him with several recording devices. During this in-person meeting, **LIBMAN** and PARADIS again discussed their plan before eventually contacting BEN:

a. **LIBMAN** stated that he still wanted to get additional information to BEN on [redacted].

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. **LIBMAN** believed that "[redacted] email is the easiest and best connection," and that they should tell BEN that they needed his help in getting "all these emails, personal, can you get those email addresses in the first place, get em. . . . However you gather the information through them, first let's get the emails. . . . **Get us [redacted] private email accounts and the contents of the communication, as far back as you can**."

c. PARADIS asked **LIBMAN** to clarify whether they were talking about just the email addresses or the content of emails, asking, **"You want the content as well**, obviously the emails?" **LIBMAN** replied "**Of course.** . . . By the way, the word hacking does not come out of our mouths. At all." PARADIS asked what phrasing **LIBMAN** wanted to use in place of "hacking." **LIBMAN** replied, "sourcing, information sourcing. . . . I don't want to use a word, some buzzwords that somebody else can use against us."

d. PARADIS stated his understanding that they were seeking both [redacted] "personal email address" and the "personal email content," and asked **LIBMAN** how far back he wanted to go. **LIBMAN** replied, "Let's go back as far as, early October 2018." PARADIS then suggested they not limit themselves to a timeframe, and **LIBMAN** agreed. PARADIS asked whether they were also seeking text messages. **LIBMAN** confirmed his interest in also obtaining text messages.

e. The two also discussed payment, and **LIBMAN** suggested that they just ask BEN how he wants to get paid. PARADIS asked whether LIBMAN wanted to consider using bitcoin to

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

conceal their transaction. **LIBMAN** expressed skepticism, because he did not "want any other intermediaries, the less intermediaries the better." **LIBMAN** preferred to just ask BEN how to transfer the money. At some point in the conversation, **LIBMAN** suggested that they could pay the money through Cypress or Lichtenstein.

f. During the discussion of payment, **LIBMAN** indicated that he had a separate contact and implied that he could consult with his separate contact about issues relating to the operation with BEN, including payment. **LIBMAN** described his separate contact as "**a real hacker in the unit**." PARADIS asked whether LIBMAN's reference to "the unit" meant Unit 8200 (described above), and LIBMAN replied "much higher." **LIBMAN** stated that this other contact was reluctant to get involved because of the FBI involvement and other sensitivities.[19] However, this individual was willing to advise "behind the scenes."

g. On the question of price, **LIBMAN** and PARADIS agreed that they were comfortable with $25-50,000 apiece, meaning $50,000 to $100,000 total, for this opening installment, with the hopes that BEN would deliver "meaningful" information as a "taste." When **LIBMAN** asked PARADIS what PARADIS would consider a "taste," PARADIS replied, "we need content . . . if the content is not meaningful to us, right? If it's about [redacted] fucking flat tire in [redacted] car . . . who cares . . . give me a

[19] I understand the reference to the FBI in this context to reflect publicly available information about the FBI investigation into the collusive litigation and related matters.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

taste that I can use as opposed to . . . you collected [redacted] fucking useless e-mail," with PARADIS adding that he would not "pay $50 grand for that," referring to e-mails without any substantive relevance. **LIBMAN** stated that they needed "**texts, meaningful texts**." **LIBMAN** also stated to PARADIS, "I don't want [BEN] to know too much...the less he knows, the better."

h. Following the above-described conversation between **LIBMAN** and PARADIS, **LIBMAN** made contact with BEN via an encrypted app on **LIBMAN**'s **BURNER PHONE**. **LIBMAN** and PARADIS discussed with BEN details of the contemplated hacking of [redacted] email and text accounts. **LIBMAN** asked BEN, "can you make it happen and how much." LIBMAN then referenced the access to [redacted] account as an "investigation," and BEN objected to that phrasing, replying, "Ehhh, investigation is different . . . we'll call it a compromise", **LIBMAN** replied, "Okay".

i. From the recording, it is my understanding that LIBMAN sent [redacted] name to the hacker via one of his phones (on the recording, the two can be heard spelling out [redacted] name, and then the "swoosh" sound of a text being sent from a smart device can be heard).

j. BEN called back on **LIBMAN's BURNER PHONE** again and explained to **LIBMAN** and PARADIS that the first stage of his services would start at $70,000. BEN then explained how the services would be invoiced, stating that a "buck slip"[20] would be used. BEN advised that they would meet someplace outside of the

[20] Based on my training and experience and knowledge of the investigation, a "buck slip" is a routing slip with a specific sales offer.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

United States after the initial stage was complete, and that the next phase was "not cheap." BEN advised **LIBMAN** that he could deposit the fee via a bank account to one of BEN's 172 shell companies.

k. **LIBMAN** and PARADIS advised BEN that they would like to speak privately to each other. Following the termination of the call, **LIBMAN** stated to PARADIS that the buck slip would be used to make the payment falsely appear to be, in **LIBMAN**'s terms, "a legitimate transaction." **LIBMAN** and PARADIS discussed negotiating with BEN and their mutual need for proof that BEN could deliver the desired information. **LIBMAN** stated that if BEN could show "proof," that both he and PARADIS would "send the money", but BEN would have to "show that [he] can get into those email addresses" first.

l. Following this discussion, **LIBMAN** and PARADIS reestablished contact with BEN through **LIBMAN's BURNER PHONE**. **LIBMAN** explained to BEN that they would need a "sample" of "[redacted] texts or email" before they would pay or meet with BEN. BEN responded that he would not provide such a sample, and that this information would come in the "second stage", and that he can't provide a "sample" from an "[redacted]" for $70,000. PARADIS asked BEN what the "second stage" would include, and BEN replied that in the second stage, "**you get everything you want**." The three then discussed travel plans, with LIBMAN asking where BEN was able to meet overseas. **LIBMAN** expressed his desire to meet with BEN in person.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

m. After the call, **LIBMAN** said to PARADIS "you want the $70,000 right now, fine," apparently indicating that **LIBMAN** was ready to proceed with payment of $70,000 to BEN. PARADIS responded, "I want concrete steps in place...I want a plan with a deadline in it" for the next phone call. The two discussed wiring money to BEN, and the fact that **LIBMAN** trusted BEN and thought it was worth the risk, given that **LIBMAN** had "vetted" BEN, and **LIBMAN**'s belief that BEN was "legit." **LIBMAN** reminded PARADIS that although **LIBMAN** had not met BEN before, **LIBMAN** had been introduced to BEN through "a very legitimate company that does this shit" during his visit to Israel. **LIBMAN** and PARADIS both stated that $35,000 apiece was worth the "risk" of losing $70,000 in total. **LIBMAN** then offered ideas on how to wire BEN his fee, including having BEN send a pro forma invoice. The two discussed how the wire transfer would take place, and that **LIBMAN** and PARADIS "can't set up a joint account" in order to accomplish this. **LIBMAN** suggested using banks in Delaware, because Delaware "**is the best," that "they will not fucking give Uncle Sam, or the FBI, any fucking information**."

49. Later that same night, on April 24, 2020, in a consensually recorded call between **LIBMAN** and PARADIS, **LIBMAN** told PARADIS that he wanted to travel to Switzerland soon so that they could meet with BEN in person. **LIBMAN** stated that he had settled on Switzerland after researching COVID-19 travel restrictions, and he asked PARADIS to look into his availability to travel as soon as May 6, 2020. **LIBMAN** indicated that being in Switzerland would also "make it a lot

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

easier for a banking transaction," because they could just "open up a Swiss account tomorrow" to pay BEN. **LIBMAN** still considered the whole operation "pretty risky" and "very pricy," but viewed it as a reasonable "gamble" and wanted to see BEN "eyeball to eyeball."

50. On April 30, 2020, in a consensually recorded call between **LIBMAN** and PARADIS, PARADIS expressed concern about traveling to Europe given the current pandemic climate and suggested that they delay travel, and **LIBMAN** agreed. PARADIS indicated he had some ideas about payment, and **LIBMAN** indicated he did not want to speak about it since the call was on the **LIBMAN PHONE** not the **BURNER PHONE**. **LIBMAN** indicated that he would use Signal to tell BEN that they wanted to talk to him in a few days, and **LIBMAN** and PARADIS agreed to speak further about payment another time. LIBMAN also expressed urgency and suggested that they needed to move quickly in executing their plans.

51. On May 1, 2020, in a consensually recorded call between **LIBMAN** and PARADIS, **LIBMAN** asked PARADIS if PARADIS would be able to get [redacted] home address. **LIBMAN** again expressed urgency in moving forward with the plan. **LIBMAN** told PARADIS that he had relayed to BEN that they would not be coming to Europe, and that BEN understood. **LIBMAN** and PARADIS again discussed methods of paying BEN for his services, and PARADIS explained that they needed to be careful to disguise the transaction to look "legitimate." **LIBMAN** agreed that "our goal is . . . **we need to come up with the information without**

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

having our fingerprints on it." **LIBMAN** again said he wanted to "**teach them** [redacted] **a lesson they'll never forget**." The two agreed to discuss payment further in person in the next few days. **LIBMAN** stated that he hoped they could "negotiate a better price," and that he had "some ideas of mechanics" for making the payments "depending on the quality of information."

52. On May 5, 2020, **LIBMAN** sent PARADIS a text saying, "??", which PARADIS understood to be in reference to **LIBMAN** wanting PARADIS to send **LIBMAN** information on [redacted].

53. On May 6, 2020, PARADIS sent **LIBMAN**, via text message, information on [redacted] that PARADIS had found using open source research on the internet, including [redacted] home address, phone number, and the names of some of [redacted] immediate family members.[21]

54. Between May 7, 2020 and June 7, 2020, through a series of texts and a brief phone conversation, **LIBMAN** and PARADIS

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

discussed logistics on when they could have another phone conversation.

55. On June 8, 2020, **LIBMAN** and PARADIS had a consensually recorded phone conversation where they discussed potential travel plans to meet with BEN. During the conversation, **LIBMAN** asked PARADIS, "Are we still doing this?" Based on the context and my knowledge of the investigation, I believe this question is in reference to hiring BEN to obtain information on [redacted]. PARADIS replied, "Of course. If you want to. I mean, it's up to you." **LIBMAN** replied to PARADIS, "Yeah, man. Listen, they [redacted] haven't forgotten about us. I guarantee you that." **LIBMAN** and PARADIS agreed that it could "draw[] attention" if they were to fly overseas, discussing how it might "look weird" if two Americans were flying to the same location during the pandemic situation. PARADIS posited that the flight lists might get circulated to the FBI and said that he did not want to "pop up on some list that pops up on the FBI's fucking monitors." **LIBMAN** replied, "yup, no, I hear you." **LIBMAN** also stated, "I'm not giving up on these motherfuckers," which I believe is a reference to [redacted]. **LIBMAN** stated that he had not spoken to BEN, nor had he sent to BEN [redacted] personal information. **LIBMAN** and PARADIS agreed that it would be a good option for BEN to travel to the US as opposed to them traveling overseas to meet BEN.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

56. Between June 11, 2020 and June 22, 2020, **LIBMAN** and PARADIS exchanged several text message exchanges to discuss when they could talk or meet in person.

57. On June 22, 2020, **LIBMAN** and PARADIS had a consensually recorded phone conversation. **LIBMAN** stated that he needed to be the "loud one" against [redacted] and that PARADIS should stay quiet for now, which I understand to mean that **LIBMAN** intended to be the one to expose corruption between [redacted]. **LIBMAN** stated his desire to file lawsuits against [redacted] and others, and that he needed to be **"armed with information and quickly,"** which I understand as a reference to **LIBMAN's** intent to obtain information about [redacted] using BEN's services. **LIBMAN** relayed that he had spoken with BEN, and that BEN had explained he did not want to travel to the United States, not only because of COVID, but because **"things that need to be said . . .I would not say them on American soil."** **LIBMAN** then asked PARADIS, "You understand?" I believe that by asking PARADIS if he understood, **LIBMAN** was referring to **LIBMAN's** and PARADIS's shared understanding that the matters under discussion —— namely the SUBJECT OFFENSES —— were illegal. **LIBMAN** also discussed his desire to "create the appearance" that PARADIS and **LIBMAN** were "adversarial." **LIBMAN** stated, "We're not colluding to do anything fraudulent," and that they were working "behind the scenes, collaborating against mutual enemies." I believe this was another attempt by **LIBMAN** to issue false exculpatory statements in an effort to shield

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

himself from criminal liability for conduct that he knew to be illegal.

G. LIBMAN Has Made Repeated References to Obtaining Firearms, Including Machine Guns, And Transporting Firearms from Other States Into California[22]

58. On March 16, 2020, during the same consensually recorded call with PARADIS described above, **LIBMAN** complained that all of the California stores were sold out of firearms, and that he "can't even get a shotgun or a rifle...from Big 5!" **LIBMAN** added that he knew he couldn't get anything from Nevada, but asked PARADIS what the situation was in Arizona. PARADIS replied that guns were available in Arizona, and that long guns[23] would be easier than pistols. **LIBMAN** replied, "All I need is long guns. . . . I'd fucking drive myself tonight, tomorrow night, if I have to . . . . If everybody around them is arming themselves, I don't want to be the one left unarmed." After PARADIS said he would check on the gun situation in Arizona, **LIBMAN** said, "If I need to drive to Arizona, I'll

---

[22] This section relates to the following SUBJECT OFFENSES:

a) 18 U.S.C. 922(o) (Possession of a machine gun), which provides that it shall be unlawful for any person to transfer or possess a machinegun (subject to certain clearly delineated exceptions, such as public authorization, that I do not believe apply here).

b) 922(a)(3) (Illegal transportation of firearms), which provides in pertinent part that it shall be unlawful for any person to transport into or receive in the state where he resides any firearm purchased or otherwise obtained by such person outside that state (subject to certain clearly delineated exceptions that I do not believe apply here, as noted below).

[23] I understand "long guns" as a common colloquial reference to long-barreled firearms, including certain rifles, shotguns, and machine guns.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

drive." **LIBMAN** asked PARADIS to look at pricing three "high powered" AR-15 rifles and three semi-automatic, 12-gauge shotguns while PARADIS was working in Arizona. I believe that **LIBMAN** wanted PARADIS to check on gun prices in Arizona so that LIBMAN could drive to Arizona to purchase the guns that he could not find in California.

59. On April 4, 2020, during a consensually recorded meeting between **LIBMAN** and PARADIS, **LIBMAN** stated, **"I got my guns. I'm waiting for a Skorpion to come in."** I understand from my training and experience, consultation with other law enforcement agents, and review of open-source materials that a Skorpion is a submachine gun pistol made by weapons manufacturer CZ, which is sold in both semiautomatic and fully automatic versions. LIBMAN further advised that he had obtained the guns from his "Russian connections". LIBMAN also stated that he "was supposed to get a Kriss Vector" but that "they fucked me up on" that. After PARADIS stated that he was unfamiliar with that, LIBMAN explained, **"It's a machine, it's a little machine gun, with extended clip."** I understand from my training and experience, consultation with other law enforcement agents, and review of open-source materials that weapons manufacturer Kriss Vector makes a 9-millimeter submachine gun pistol that is available in both semi-automatic and fully automatic versions. LIBMAN also confirmed that his CZ "9 millimeter semi" (which I understand to mean that it would be semiautomatic) pistol would have an "extended clip."

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

60. On April 8, 2020, during a consensually recorded meeting, I believe PARADIS and **LIBMAN** were discussing high-capacity magazines on their walk to the hotel room from the lobby.[24] The audio from this portion of the recording is difficult to hear because of background noise due to the location of the recording device. **LIBMAN** can be heard saying in response to an inaudible question from PARADIS, "oh, the clip? . . . Ten." Based on my training and experience, I believe **LIBMAN** was referring to a clip he had acquired or would acquire that contained ten rounds of ammunition, which would be inserted into a magazine to be loaded into a firearm. PARADIS then asked about an "extended clip," and **LIBMAN** replied, "40, 45," which I believe referred to an additional clip or clips that could contain up to 40 to 45 rounds and would then be inserted into a high-capacity magazine. PARADIS asked, "just one clip?" and **LIBMAN** replied "of course not."

61. On April 24, 2020, during the same consensually recorded meeting between **LIBMAN** and PARADIS described above, LIBMAN and PARADIS continued their discussion of firearms:

a. During the meeting, **LIBMAN** took a brief call from an unknown person, which was audibly related to firearms. **LIBMAN** excused himself from that call by saying "I'm in the

[24] Based on my training and experience, and information obtained from various law enforcement personnel, a high-capacity magazine is a firearm magazine which is typically capable of holding more than 10 or 15 rounds of ammunition. I understand from review of open-source material that California law bans magazines with a capacity of more than ten rounds, that this law was declared unconstitutional by a federal district judge in 2019, and that the constitutionality of that state law is being litigated in the appellate courts.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

middle of a meeting right now." A few moments later, PARADIS inquired about the status of **LIBMAN's** firearms, stating "Remind me again . . . because I want to talk about guns . . . I bought one, and I can't get the other one that I want." **LIBMAN** then stated, "this [the call he had just received] was a call about this [purchasing additional guns]." **LIBMAN** continued, stating to PARADIS "I'm working on a deal" with an unnamed individual who LIBMAN would "call back later" to acquire additional weapons, adding that he (**LIBMAN**) had already obtained "his CZ," and "another gun that I got." **LIBMAN** then stated, "I'm trying to get the Tavor." LIBMAN also stated that "somebody wanted to sell me some Colts, some Kriss Vectors and whatnot, but they wanted $2500, it's a $1700 gun." Based on my training and experience and knowledge of the investigation, I know that a CZ, Tavor, and Kriss Vector are three brand names of weapons manufacturers.

b. **LIBMAN** then advised PARADIS that he had "another contact, hopefully through Oregon," through which he (**LIBMAN**) could purchase a firearm. PARADIS inquired if this contact was the same contact who sold LIBMAN his "CZ", to which LIBMAN replied "I got that (the CZ) through a contact here." PARADIS then asked "but it didn't come from California?" to which **LIBMAN** stated "fuck no." **LIBMAN** stated that he wanted to obtain firearms through Oregon, due to "better gun laws."

c. PARADIS offered to buy two weapons for $5,000, if it would get **LIBMAN** a better deal on his next firearms purchase. Referring to the aforementioned phone call that interrupted

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

their meeting, **LIBMAN** stated that "this was a very excited call", and "we've been working on something, so he's got something to tell me." PARADIS also asked if **LIBMAN's** contact was a "gun seller," to which **LIBMAN** replied "no". **LIBMAN** referred to this contact as "friends in high places, and friends in low places". **LIBMAN** said he'd "text (to PARADIS) a picture of what's available." **LIBMAN** also stated he hopes to be "getting the stuff" by next week, since Oregon "has no waiting period". When PARADIS asked about shipping the weapons to California, **LIBMAN** replied "**shipping is a felony, especially with intent to sell, there are other ways to get it in**." **LIBMAN** stated he was looking at purchasing a "Tavor" or an "Uzi." PARADIS commented that the Tavor was "fully automatic," and **LIBMAN** did not confirm this statement but did not contradict or object to that characterization. Based on my training and experience, I know that (1) a "Tavor" is a type of assault rifle made by the Israel Weapons Industries and is available in both fully automatic and semi-automatic modes, and (2) an "Uzi" is traditionally a fully automatic submachine gun, although it can be sold as a semi-automatic weapon.

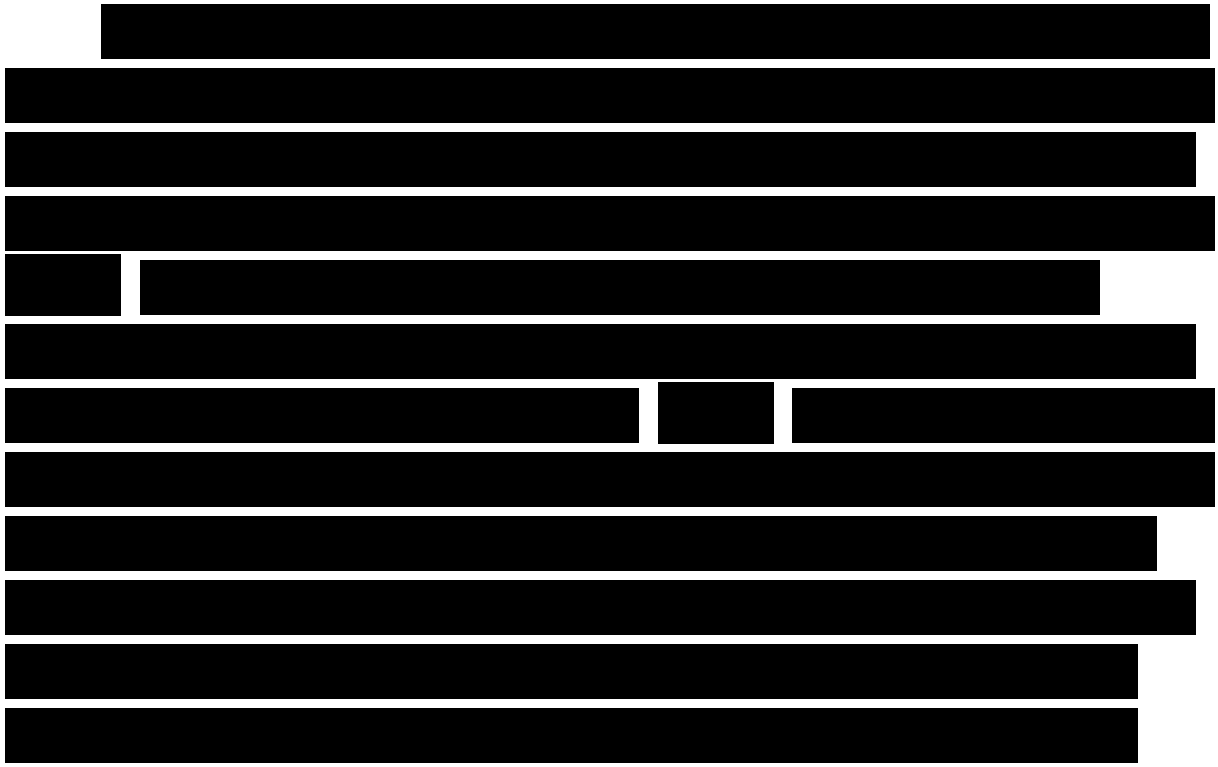
62. Based on the conversations between **LIBMAN** and PARADIS about **LIBMAN**'s desire to protect himself and his family with firearms, I believe that the guns **LIBMAN** has purchased, or was pursuing, will be found at **LIBMAN's HOME**. Additionally, although many of the guns **LIBMAN** expressed interest in are available in both automatic and semi-automatic modes, I believe there is probable cause to believe that **LIBMAN** has acquired or

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

attempted to acquire a fully automatic machine gun based on his statements to PARADIS that he was interested in obtaining weapons that are commonly sold as fully automatic, the reference in their discussions to his efforts to obtain "fully automatic" firearms, and the efforts **LIBMAN** has described undertaking to conceal his purchase of firearms, as further described above.

63. On June 24, 2020, a special agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") confirmed to me that according to a check of the relevant ATF database, **LIBMAN** did not hold and had never held a Federal Firearms License.

H. Other Information



Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

[redacted]

65. I believe that there is probable cause to believe that evidence of the SUBJECT OFFENSES will be located at the **LIBMAN HOME** and on the **LIBMAN PHONE** and the **BURNER PHONE**, for the reasons set forth herein.

VII. PREMISES INFORMATION

66. The **LIBMAN HOME** is a two-story single-family home located in Tarzana, California. I believe that **LIBMAN** lives at the LIBMAN HOME because it is listed as his home address in Accurint reports stating same, **LIBMAN** told PARADIS his address in a recorded call, and Special Agents have conducted surveillance outside the home on or about April 4, 8, and 24, 2020, and have seen **LIBMAN** leaving the **LIBMAN HOME** in a car registered to him at the same address.

67. Additionally, on **LIBMAN's** consensually recorded calls with PARADIS, he provided PARADIS with the address for the **LIBMAN HOME** when seeking to have PARADIS mail the **BURNER PHONE** to him. **LIBMAN** has also advised PARADIS that, due to the COVID-19 threat, **LIBMAN** spends most of his time working from home. Given this information, I believe that evidence, fruits, and instrumentalities of the SUBJECT OFFENSES, including the **BURNER PHONE** and the **LIBMAN PHONE**, are like to be found on **LIBMAN's** person or in the **LIBMAN HOME**.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

VIII. TRAINING AND EXPERIENCE ON FIREARMS OFFENSES

68. From my training, personal experience, and the collective experiences related to me by other law enforcement officers who conduct firearms investigations, I am aware of the following:

a. Persons who possess, purchase, or sell firearms generally maintain records of their firearm transactions as items of value and usually keep them in their residence, or in places that are readily accessible, and under their physical control, such in their digital devices. It has been my experience that individuals who own, deal, or transport firearms illegally will keep the contact information of the individual who is supplying firearms or other individuals involved in criminal activities for future purchases or referrals. Such information is also kept on digital devices.

b. Many people keep mementos of their firearms, including digital photographs or recordings of themselves possessing or using firearms on their digital devices, or of firearms that they wish to sell to others. These photographs and recordings are often shared via social media, text messages, and over text messaging applications.

c. Correspondence between persons buying and selling firearms, or transporting firearms, including correspondence between co-conspirators in the dealing of firearms without a license or illegally transporting them across state lines, often occurs over phone calls, e-mail, text message, and social media message to and from smartphones, laptops, or other digital

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

devices. This includes sending photos of the firearm between the seller and the buyer, as well as negotiation of price. In my experience, individuals who engage in street sales of firearms frequently use phone calls, e-mail, and text messages to communicate with each other regarding firearms that they sell or offer for sale. In addition, it is common for individuals engaging in the unlawful sale of firearms to have photographs of firearms they or other individuals working with them possess on their cellular phones and other digital devices as they frequently send these photos to each other to boast of their firearms possession and/or to facilitate sales or transfers of firearms.

69. Individuals engaged in the illegal purchase or sale of firearms often use multiple digital devices.

IX. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[25]

70. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

71. Forensic methods may uncover electronic files or remnants of such files months or even years after the files

[25] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

72. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

73. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

74. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

75. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

76. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

77. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

78. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

XII. CONCLUSION

79. Based on the foregoing, there is probable cause to believe that evidence, fruits, and instrumentalities of the offenses described in Attachment B will be found in the LIBMAN HOME or on the person of LIBMAN as described in Attachments A-1 and A-2.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 26th day of June, 2020.

Patrick J. Walsh

HONORABLE PATRICK J. WALSH
UNITED STATES MAGISTRATE JUDGE

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of:
[redacted], Tarzana, California, 91356

Case No. 2:20-MJ-2994

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California:

See Attachment A-1

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 6/26/2020 2:55 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

U.S. Magistrate Judge Patrick J. Walsh
Printed name and title

AUSA: Melissa Mills

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-1

PROPERTY TO BE SEARCHED

The premises to be searched is located at [redacted], Tarzana, California, 91356, believed to be the residence of MICHAEL LIBMAN ("**LIBMAN HOME**") and pictured below. The residence is a detached two-story single-family home with a light beige exterior and a gated front yard. On the front curb of the residence is the number "[redacted]" painted in black. The number "[redacted]" is also painted on the residence next to the garage door.

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 922(o) (Possession of a machine gun); 922(a)(3) (Illegal transportation of firearms); 1030 (Unauthorized access of a computer); 1341 (Mail Fraud); 1343 (Wire Fraud); 1512 (Witness Tampering); 1951 (Extortion); and 1956 (Money Laundering) (together, the "SUBJECT OFFENSES"), namely:

a. Records, documents, communications, or other materials from January 1, 2020, to the present discussing methods or tools for gaining unauthorized access to computers or computer networks, including the usage of encrypted software or surveillance tools to conceal access or the identity of those using them;

b. Records, documents, communications, or other materials from January 1, 2020, to the present involving foreign cybersecurity experts or any individual or entity in communication with **MICHAEL LIBMAN** about computer access, surveillance, intelligence, or other cyber-related operations;

c. Records, documents, communications, or other materials from January 1, 2020, to the present reflecting payments for hacking, computer fraud, electronic surveillance, or gaining unauthorized access to a computer;

d. Records, documents, communications, or other materials from January 1, 2020, to the present reflecting bank accounts or other financial instruments used to send or receive

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

funds derived from hacking, computer fraud, or gaining unauthorized access to a computer;

e. Records, documents, communications, or other materials from January 1, 2020, to the present reflecting plans to collect information about [redacted] or any existing collections of information about the same;

f. Audio recordings, pictures, video recordings, or still captured images involving hacking, computer fraud, electronic surveillance, or gaining unauthorized access to a computer, or the location of **MICHAEL LIBMAN** during the commission of such actions, from January 1, 2020, to the present;

g. Audio recordings, pictures, video recordings, or still captured images reflecting the purchase, sale, transportation, or distribution of firearms or ammunition, or the location of **MICHAEL LIBMAN** during the commission of such actions, from January 1, 2020, to the present;

h. Firearms, including handguns, shotguns, rifles, assault weapons, and machine guns, and records, documents, and tools used for or reflecting the ownership, manufacture, or maintenance of firearms or ammunition;

i. Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with sources of firearms;

j. Data, records, documents, or information (including electronic mail, messages over applications and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

social media, and photographs) from January 1, 2020, to the present reflecting efforts by **MICHAEL LIBMAN** to obtain, possess, use, apply for, or transfer money over $1,000, such as bank account records, cryptocurrency records, and accounts;

k. Address book information, including all stored, saved, or deleted telephone numbers, from January 1, 2020, to the present;

l. Call log information, including all telephone numbers dialed from the any digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls, from January 1, 2020, to the present;

m. SMS text, email communications, instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp) or other text or written communications, including evidence of deleted communications, from January 1, 2020, to the present, sent to or received from any of the digital devices mentioning [redacted], firearms, including machine guns, or the plans to access someone else's computer;

n. Contents of any calendar or date book from January 1, 2020, to the present;

o. Global Positioning System ("GPS") coordinates and other information or records identifying interstate travel routes from January 1, 2020, to the present; and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

p. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

q. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

a. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

3. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications or work product:

Non-Digital Evidence

4. Law enforcement personnel conducting the investigation ("the Investigation Team") may be present at the search, but may not search or review any item prior to it being given to them by the "Privilege Review Team" (previously designated individual(s) not participating in the investigation of the case).

5. The Privilege Review Team will review documents to see whether or not the document appears to contain or refer to communications between an attorney and any person or containing the work product of an attorney ("potentially privileged information"). Those documents not containing or referring to such communications or work product may be turned over to the Investigation Team for review.

6. In consultation with a Privilege Review Team Assistant United States Attorney ("PRTAUSA"), if appropriate, the Privilege Review Team member will then review any document identified as appearing to contain potentially privileged information to confirm that it contains potentially privileged information. If it does not, it may be returned to an Investigation Team member. If a member of the Privilege Review

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Team confirms that a document contains potentially privileged information, then the member will review only as much of the document as is necessary to determine whether or not the document is within the scope of the warrant. Those documents which contain potentially privileged information but are not within the scope of the warrant will be set aside and will not be subject to further review or seizure absent subsequent authorization. Those documents which contain potentially privileged information and are within the scope of the warrant will be seized and sealed together in an enclosure, the outer portion of which will be marked as containing potentially privileged information. The Privilege Review Team member will also make sure that the locations where the documents containing potentially privileged information were seized have been documented.

7. The seized documents containing potentially privileged information will be delivered to the United States Attorney's Office for further review by a PRTAUSA. If that review reveals that a document does not contain potentially privileged information, or that an exception to the privilege applies, the document may be returned to the Investigation Team. If appropriate based on review of particular documents, the PRTAUSA may apply to the court for a finding with respect to the particular documents that no privilege, or an exception to the privilege, applies.

Digital Evidence

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

8. The Privilege Review Team will also review seized digital devices as set forth herein. The Investigation Team will review only digital device data which has been released by the Privilege Review Team.

9. The Privilege Review Team will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location.

10. The Privilege Review Team and the Investigation Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

11. The Investigation Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified clients, names of any identified spouses, or their email addresses, and generic words such as "privileged" and "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. Documents or data that are identified by this initial review as not potentially privileged may be given to the Investigation Team.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

12. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Investigation Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRTAUSA. Documents or data identified by the PRTAUSA after review as not potentially privileged may be given to the Investigation Team. If, after review, the PRTAUSA determines it to be appropriate, the PRTAUSA may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Investigation Team. Documents or data identified by the PRTAUSA after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

13. The Investigation Team will search only the documents and data that the Privilege Review Team provides to the Investigation Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Investigation Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

and data within the scope of the search warrant if that is more efficient.

14. In performing the reviews, both the Privilege Review Team and the Investigation Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

15. If either the Privilege Review Team or the Investigation Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

16. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

17. If the search determines that a digital device does contain data falling within the list of items to be seized, the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

government may make and retain copies of such data, and may access such data at any time.

18. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

19. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

20. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

21. In order to search for data capable of being read or interpreted by a digital device, the Investigation Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

22. During the execution of this search warrant, law enforcement is permitted to: (1) depress **MICHAEL LIBMAN's** thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of **MICHAEL LIBMAN's** face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

23. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 922(o) (Possession of a machine gun); 922(a)(3) (Illegal transportation of firearms); 1030 (Unauthorized access of a computer); 1341 (Mail Fraud); 1343 (Wire Fraud); 1512 (Witness Tampering); 1951 (Extortion); and 1956 (Money Laundering) (together, the "SUBJECT OFFENSES"), namely:

a. Records, documents, communications, or other materials from January 1, 2020, to the present discussing methods or tools for gaining unauthorized access to computers or computer networks, including the usage of encrypted software or surveillance tools to conceal access or the identity of those using them;

b. Records, documents, communications, or other materials from January 1, 2020, to the present involving foreign cybersecurity experts or any individual or entity in communication with **MICHAEL LIBMAN** about computer access, surveillance, intelligence, or other cyber-related operations;

c. Records, documents, communications, or other materials from January 1, 2020, to the present reflecting payments for hacking, computer fraud, electronic surveillance, or gaining unauthorized access to a computer;

d. Records, documents, communications, or other materials from January 1, 2020, to the present reflecting bank accounts or other financial instruments used to send or receive

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

funds derived from hacking, computer fraud, or gaining unauthorized access to a computer;

e. Records, documents, communications, or other materials from January 1, 2020, to the present reflecting plans to collect information about [redacted] or any existing collections of information about the same;

f. Audio recordings, pictures, video recordings, or still captured images involving hacking, computer fraud, electronic surveillance, or gaining unauthorized access to a computer, or the location of **MICHAEL LIBMAN** during the commission of such actions, from January 1, 2020, to the present;

g. Audio recordings, pictures, video recordings, or still captured images reflecting the purchase, sale, transportation, or distribution of firearms or ammunition, or the location of **MICHAEL LIBMAN** during the commission of such actions, from January 1, 2020, to the present;

h. Firearms, including handguns, shotguns, rifles, assault weapons, and machine guns, and records, documents, and tools used for or reflecting the ownership, manufacture, or maintenance of firearms or ammunition;

i. Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with sources of firearms;

j. Data, records, documents, or information (including electronic mail, messages over applications and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

social media, and photographs) from January 1, 2020, to the present reflecting efforts by **MICHAEL LIBMAN** to obtain, possess, use, apply for, or transfer money over $1,000, such as bank account records, cryptocurrency records, and accounts;

k. Address book information, including all stored, saved, or deleted telephone numbers, from January 1, 2020, to the present;

l. Call log information, including all telephone numbers dialed from the any digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls, from January 1, 2020, to the present;

m. SMS text, email communications, instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp) or other text or written communications, including evidence of deleted communications, from January 1, 2020, to the present, sent to or received from any of the digital devices mentioning [redacted], firearms, including machine guns, or the plans to access someone else's computer;

n. Contents of any calendar or date book from January 1, 2020, to the present;

o. Global Positioning System ("GPS") coordinates and other information or records identifying interstate travel routes from January 1, 2020, to the present; and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

p. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

q. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

a. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

3. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications or work product:

Non-Digital Evidence

4. Law enforcement personnel conducting the investigation ("the Investigation Team") may be present at the search, but may not search or review any item prior to it being given to them by the "Privilege Review Team" (previously designated individual(s) not participating in the investigation of the case).

5. The Privilege Review Team will review documents to see whether or not the document appears to contain or refer to communications between an attorney and any person or containing the work product of an attorney ("potentially privileged information"). Those documents not containing or referring to such communications or work product may be turned over to the Investigation Team for review.

6. In consultation with a Privilege Review Team Assistant United States Attorney ("PRTAUSA"), if appropriate, the Privilege Review Team member will then review any document identified as appearing to contain potentially privileged information to confirm that it contains potentially privileged information. If it does not, it may be returned to an Investigation Team member. If a member of the Privilege Review

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Team confirms that a document contains potentially privileged information, then the member will review only as much of the document as is necessary to determine whether or not the document is within the scope of the warrant. Those documents which contain potentially privileged information but are not within the scope of the warrant will be set aside and will not be subject to further review or seizure absent subsequent authorization. Those documents which contain potentially privileged information and are within the scope of the warrant will be seized and sealed together in an enclosure, the outer portion of which will be marked as containing potentially privileged information. The Privilege Review Team member will also make sure that the locations where the documents containing potentially privileged information were seized have been documented.

7. The seized documents containing potentially privileged information will be delivered to the United States Attorney's Office for further review by a PRTAUSA. If that review reveals that a document does not contain potentially privileged information, or that an exception to the privilege applies, the document may be returned to the Investigation Team. If appropriate based on review of particular documents, the PRTAUSA may apply to the court for a finding with respect to the particular documents that no privilege, or an exception to the privilege, applies.

Digital Evidence

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

8. The Privilege Review Team will also review seized digital devices as set forth herein. The Investigation Team will review only digital device data which has been released by the Privilege Review Team.

9. The Privilege Review Team will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location.

10. The Privilege Review Team and the Investigation Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

11. The Investigation Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified clients, names of any identified spouses, or their email addresses, and generic words such as "privileged" and "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. Documents or data that are identified by this initial review as not potentially privileged may be given to the Investigation Team.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

12. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Investigation Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRTAUSA. Documents or data identified by the PRTAUSA after review as not potentially privileged may be given to the Investigation Team. If, after review, the PRTAUSA determines it to be appropriate, the PRTAUSA may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Investigation Team. Documents or data identified by the PRTAUSA after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

13. The Investigation Team will search only the documents and data that the Privilege Review Team provides to the Investigation Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Investigation Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

and data within the scope of the search warrant if that is more efficient.

14. In performing the reviews, both the Privilege Review Team and the Investigation Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

15. If either the Privilege Review Team or the Investigation Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

16. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

17. If the search determines that a digital device does contain data falling within the list of items to be seized, the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

government may make and retain copies of such data, and may access such data at any time.

18. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

19. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

20. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

21. In order to search for data capable of being read or interpreted by a digital device, the Investigation Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

22. During the execution of this search warrant, law enforcement is permitted to: (1) depress **MICHAEL LIBMAN's** thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of **MICHAEL LIBMAN's** face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

23. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of:
Michael Libman
DOB: [redacted] 1967

Case No. 2:20-MJ-2995

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-2

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by reference and attached hereto

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 6/26/2020 2:55 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

U.S. Magistrate Judge - Patrick J. Walsh
Printed name and title

AUSA: Melissa Mills

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-2

PERSON TO BE SEARCHED

The person to be searched is MICHAEL LIBMAN, date of birth [redacted] 1967, as pictured below:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 922(o) (Possession of a machine gun); 922(a)(3) (Illegal transportation of firearms); 1030 (Unauthorized access of a computer); 1341 (Mail Fraud); 1343 (Wire Fraud); 1512 (Witness Tampering); 1951 (Extortion); and 1956 (Money Laundering) (together, the "SUBJECT OFFENSES"), namely:

a. Records, documents, communications, or other materials from January 1, 2020, to the present discussing methods or tools for gaining unauthorized access to computers or computer networks, including the usage of encrypted software or surveillance tools to conceal access or the identity of those using them;

b. Records, documents, communications, or other materials from January 1, 2020, to the present involving foreign cybersecurity experts or any individual or entity in communication with **MICHAEL LIBMAN** about computer access, surveillance, intelligence, or other cyber-related operations;

c. Records, documents, communications, or other materials from January 1, 2020, to the present reflecting payments for hacking, computer fraud, electronic surveillance, or gaining unauthorized access to a computer;

d. Records, documents, communications, or other materials from January 1, 2020, to the present reflecting bank accounts or other financial instruments used to send or receive

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

funds derived from hacking, computer fraud, or gaining unauthorized access to a computer;

e. Records, documents, communications, or other materials from January 1, 2020, to the present reflecting plans to collect information about [redacted] or any existing collections of information about the same;

f. Audio recordings, pictures, video recordings, or still captured images involving hacking, computer fraud, electronic surveillance, or gaining unauthorized access to a computer, or the location of **MICHAEL LIBMAN** during the commission of such actions, from January 1, 2020, to the present;

g. Audio recordings, pictures, video recordings, or still captured images reflecting the purchase, sale, transportation, or distribution of firearms or ammunition, or the location of **MICHAEL LIBMAN** during the commission of such actions, from January 1, 2020, to the present;

h. Firearms, including handguns, shotguns, rifles, assault weapons, and machine guns, and records, documents, and tools used for or reflecting the ownership, manufacture, or maintenance of firearms or ammunition;

i. Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with sources of firearms;

j. Data, records, documents, or information (including electronic mail, messages over applications and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

social media, and photographs) from January 1, 2020, to the present reflecting efforts by **MICHAEL LIBMAN** to obtain, possess, use, apply for, or transfer money over $1,000, such as bank account records, cryptocurrency records, and accounts;

k. Address book information, including all stored, saved, or deleted telephone numbers, from January 1, 2020, to the present;

l. Call log information, including all telephone numbers dialed from the any digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls, from January 1, 2020, to the present;

m. SMS text, email communications, instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp) or other text or written communications, including evidence of deleted communications, from January 1, 2020, to the present, sent to or received from any of the digital devices mentioning [redacted] firearms, including machine guns, or the plans to access someone else's computer;

n. Contents of any calendar or date book from January 1, 2020, to the present;

o. Global Positioning System ("GPS") coordinates and other information or records identifying interstate travel routes from January 1, 2020, to the present; and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

p. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

q. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

a. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

3. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications or work product:

Non-Digital Evidence

4. Law enforcement personnel conducting the investigation ("the Investigation Team") may be present at the search, but may not search or review any item prior to it being given to them by the "Privilege Review Team" (previously designated individual(s) not participating in the investigation of the case).

5. The Privilege Review Team will review documents to see whether or not the document appears to contain or refer to communications between an attorney and any person or containing the work product of an attorney ("potentially privileged information"). Those documents not containing or referring to such communications or work product may be turned over to the Investigation Team for review.

6. In consultation with a Privilege Review Team Assistant United States Attorney ("PRTAUSA"), if appropriate, the Privilege Review Team member will then review any document identified as appearing to contain potentially privileged information to confirm that it contains potentially privileged information. If it does not, it may be returned to an Investigation Team member. If a member of the Privilege Review

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Team confirms that a document contains potentially privileged information, then the member will review only as much of the document as is necessary to determine whether or not the document is within the scope of the warrant. Those documents which contain potentially privileged information but are not within the scope of the warrant will be set aside and will not be subject to further review or seizure absent subsequent authorization. Those documents which contain potentially privileged information and are within the scope of the warrant will be seized and sealed together in an enclosure, the outer portion of which will be marked as containing potentially privileged information. The Privilege Review Team member will also make sure that the locations where the documents containing potentially privileged information were seized have been documented.

7. The seized documents containing potentially privileged information will be delivered to the United States Attorney's Office for further review by a PRTAUSA. If that review reveals that a document does not contain potentially privileged information, or that an exception to the privilege applies, the document may be returned to the Investigation Team. If appropriate based on review of particular documents, the PRTAUSA may apply to the court for a finding with respect to the particular documents that no privilege, or an exception to the privilege, applies.

Digital Evidence

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

8. The Privilege Review Team will also review seized digital devices as set forth herein. The Investigation Team will review only digital device data which has been released by the Privilege Review Team.

9. The Privilege Review Team will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location.

10. The Privilege Review Team and the Investigation Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

11. The Investigation Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified clients, names of any identified spouses, or their email addresses, and generic words such as "privileged" and "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. Documents or data that are identified by this initial review as not potentially privileged may be given to the Investigation Team.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

12. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Investigation Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRTAUSA. Documents or data identified by the PRTAUSA after review as not potentially privileged may be given to the Investigation Team. If, after review, the PRTAUSA determines it to be appropriate, the PRTAUSA may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Investigation Team. Documents or data identified by the PRTAUSA after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

13. The Investigation Team will search only the documents and data that the Privilege Review Team provides to the Investigation Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Investigation Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

and data within the scope of the search warrant if that is more efficient.

14. In performing the reviews, both the Privilege Review Team and the Investigation Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

15. If either the Privilege Review Team or the Investigation Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

16. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

17. If the search determines that a digital device does contain data falling within the list of items to be seized, the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

government may make and retain copies of such data, and may access such data at any time.

18. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

19. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

20. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

21. In order to search for data capable of being read or interpreted by a digital device, the Investigation Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

22. During the execution of this search warrant, law enforcement is permitted to: (1) depress **MICHAEL LIBMAN's** thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of **MICHAEL LIBMAN's** face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

23. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

TRACY L. WILKISON
Attorney for the United States,
Acting Under Authority Conferred By 28 U.S.C. § 515
SCOTT GARRINGER
Assistant United States Attorney
Deputy Chief, Criminal Division
MELISSA MILLS (Cal. Bar No. 248529)
FRANCES LEWIS (Cal. Bar No. 291055)
Assistant United States Attorneys
Public Corruption and Civil Rights Section
DIANA KWOK (Cal. Bar No. 246366)
Assistant United States Attorney
Environmental and Community Safety Crimes Section
1500 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-0627
Facsimile: (213) 894-2927
E-mail: Melissa.Mills@usdoj.gov

Attorneys for Applicant
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

IN RE: CELLULAR TELEPHONES	No. 2:20-MJ-3828 GOVERNMENT'S *EX PARTE* APPLICATION FOR A WARRANT AUTHORIZING THE DISCLOSURE OF PROSPECTIVE CELL SITE AND GPS INFORMATION, AND REQUEST TO SEAL; AFFIDAVIT OF ANDREW CIVETTI **(UNDER SEAL)**

The United States of America, by and through its counsel of record, the United States Attorney for the Central District of California, hereby applies for a warrant requiring cellular telephone service provider(s) to furnish the Federal Bureau of Investigation (the "Investigating Agency") with information relating to the following cellular telephones:

a. [redacted] a cellular telephone issued by Verizon ("Carrier 1"), subscribed to by MICHAEL FEUER and believed to be used by MICHAEL FEUER ("**Subject Telephone 1**");

b. [redacted] a cellular telephone issued by Carrier 1, subscribed to by [redacted] and believed to be used by LEELA KAPUR ("**Subject Telephone 2**"); and

c. [redacted] a cellular telephone issued by AT&T ("Carrier 2" and, together with Carrier #1, collectively referred to as the "Carriers"), subscribed to by an as-yet-unidentified person and believed to be used by JOSEPH BRAJEVICH ("**Subject Telephone 3**" and, together with **Subject Telephones 1 and 2**, collectively referred to as the "**Subject Telephones**").

Specifically, authorization is sought to obtain prospective cell-site information, that is, information reflecting the location of cellular towers (cell-site and sector/face) related to the use of the **Subject Telephones** ("cell-site information"), as well as the physical location of the **Subject Telephones**, to include E-911 Phase II data and latitude and longitude data gathered for the **Subject Telephones**, including Global Positioning Satellite and/or network timing information, including Sprint's Per Call Measurement Data, Verizon's Real Time Tool, AT&T's Network Event Location System and T-Mobile's True Call data, and including information from such programs as Nextel Mobile Locator, Boost Mobile Loopt, Sprint/Nextel Findum Wireless, which will establish the approximate location of the **Subject Telephones**, and which information is acquired in the first instance by the Carriers ("GPS information"), at such intervals and times as the government may request, and the furnishing of all information, facilities, and technical assistance

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

necessary to accomplish said disclosure unobtrusively, for a period of 45 days.

The application is made in connection with an investigation of offenses committed by MICHAEL FEUER, PAUL PARADIS, JACK LANDSKRONER, and others known and unknown (the "Target Subjects"), specifically, violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding) (the "Target Offenses"), and is based upon the attached agent affidavit. There is probable cause to believe that federal crimes are being committed and that the information likely to be received concerning the approximate location of the **Subject Telephones**, currently within, or being monitored or investigated within, the Central District of California.

The information sought by this application first includes information about the location (physical address) of the "cell-sites" and also (for prospective data) linked to the **Subject Telephones** at call origination (for outbound calling), call termination (for incoming calls), and, if reasonably available, during the progress of a call. This information, which is acquired in the first instance by the Carrier, includes any information, apart from the content of any communication, that is reasonably available to the Carrier and that is requested by the Investigating Agency, concerning the cell-sites/sectors receiving and transmitting signals to and from the **Subject Telephones** whether or not a call is

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

in progress. This information is sought based first on 18 U.S.C. § 2701 et seq. (the "Stored Communications Act"). The Stored Communications Act provides:

> A governmental entity may require a provider of electronic communication service . . . to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only[1] when the governmental entity --
>
> (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction[.][2]

18 U.S.C. § 2703(c)(1); see also Carpenter v. United States, 138 S.Ct. 2206 (2018) (holding that a warrant is required to obtain seven or more days' worth of historical cell-site information).[3]

---

[1] This section also provides other methods to compel disclosure, including via subpoena or court order. However, the government in this case is proceeding under the highest threshold, that is, obtaining a warrant as described in § 2703(c)(1)(A).

[2] This Court is a "court of competent jurisdiction" because it is a "district court of the United States (including a magistrate judge of such a court) . . . that . . . has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). This is true even if the subject of the investigation, and/or his or her phone, is in another district. See, e.g., United States v. Ackies, 918 F.3d 190, 201-02 (1st Cir. 2019) (finding in the context of a warrant issued in one district for location information regarding phones physically located in another district that § 2703's plain text and structure, supported further by legislative history and Congressional intent, make clear that § 2703 permits searches not governed by Rule 41's geographic limitations).

[3] The definition of terms in the Stored Communications Act makes clear that the "record or other information" that a court may order a provider to disclose to the government under Section 2703(c)(1)(A) includes both cell site and other location information. First, the Stored Communications Act expressly adopts the definition of statutory terms set forth in 18 U.S.C. § 2510. See 18 U.S.C. § 2711 ("As used in this chapter. . . (1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section"). Thus, the term "provider of electronic communication service" used in Section 2703(c) covers cellular telephone service providers, because 18 U.S.C. § 2510(15) defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Further, cell site and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Prospective cell-site information is also sought based on the authority of 18 U.S.C. § 3121 et seq. (the "Pen Register Statute").[4] The government therefore also complies with the provisions of that statute, including by providing the required certification by the attorney for the government at the end of this application. Pursuant to the Pen Register Statute, upon an application made under 18 U.S.C. § 3122(a)(1) a court "shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." 18 U.S.C. § 3123(a)(1).[5]

Cellular telephone companies routinely create and maintain, in the regular course of their business, records of information

---

other location information is "a record or other information pertaining to a subscriber to or customer of" an electronic communications service – another term used in Section 2703(c) – because cellular telephone service providers receive and store the information, if sometimes only momentarily, before forwarding it to law enforcement officials. See In Re: Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F. Supp. 2d 448, 457-60 (S.D.N.Y. 2006).

[4] 18 U.S.C. § 3127(3) defines "pen register" as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication." A "trap and trace" device is similarly defined for any device or process which captures incoming data. See 18 U.S.C. § 3127(4).

[5] While 47 U.S.C. § 1002, which is part of the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"), would preclude seeking physical location information based on the Pen Register Statute alone, the Stored Communications Act provides the requisite additional authority for this Court to authorize the production by the Carrier of cell-site information to the government.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_000971
Page 971 of 1425

concerning their customers' usage. These records typically include for each communication a customer makes or receives (1) the date and time of the communication; (2) the telephone numbers involved; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer was connected at the end of the communication; and (5) the duration of the communication. The records may also, but do not always, specify a particular sector of a cell tower used to transmit a communication. Cell-site information is useful to law enforcement because of the limited information it provides about the general location of a cell phone when a communication is made.

This application also seeks GPS information for the **Subject Telephones**, which is sought based on 18 U.S.C. § 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41. As discussed above, data that provides information about the location of a customer's phone falls within 18 U.S.C. § 2703(c)'s definition of "a record or other information pertaining to a subscriber to or customer of [an electronic communication service]." Thus, the United States may obtain a warrant requiring a cell phone company to disclose GPS information "using the procedures described in the Federal Rules of Criminal Procedure," that is, Federal Rule of Criminal Procedure 41, as is contemplated by this application and order.

Some, but not all, cellular telephone service providers have the technical means to obtain GPS information. GPS information is not generated specifically for law enforcement, but is the product of United States Federal Communications Commission requirements that cellular telephone service providers maintain and access location information for emergency responders. To obtain GPS information, a

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

"ping" (electronic signal) is sent to the cellular telephone, which unobtrusively activates the GPS chip in the telephone. This information is not provided in a streaming fashion regardless of the cellular telephone activity, but instead is sent only in response to specific law-enforcement agency requests. Location data through GPS information can be delivered as accurately as within three meters; however, if the cellular telephone is in motion, such as while in a moving vehicle, the error range in meters may be greater, or the cellular telephone service provider may simply provide cell-site information. In addition, the cellular telephone must be powered on and, usually, not in the middle of a telephone call, for GPS information to be obtained. Moreover, if the cellular telephone is inside a building, or is in some other way blocked from the satellite, GPS information may not be obtainable. In such cases, the service provider will often provide law enforcement with cell-site information instead.

This application also seeks authorization under 18 U.S.C. § 3103a(b), for reasonable cause shown, to delay any notification the government is required to give regarding the requested warrant to the subscriber(s) and user(s) of the **Subject Telephones** for a period of 30 days from the date that the disclosure ends. 18 U.S.C. § 3103a(b) states that any notice required following the issuance of a warrant may be delayed if, inter alia, the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result. An adverse result is defined in 18 U.S.C. § 2705(a)(2) to include endangering the life or physical safety of a person, flight from prosecution, destruction of or tampering with evidence, intimidation of potential

witnesses, or otherwise seriously jeopardizing an investigation or unduly delaying a trial. Moreover, the Advisory Committee Notes for Fed. R. Crim. P. 41(f)(3) (2006 Amendments) state that delay of notice may be appropriate where "the officer establishes that the investigation is ongoing and that disclosure of the warrant will compromise that investigation." The attached agent affidavit provides reasonable cause to believe that immediate notification of the execution of the warrant may have an adverse result. The proposed warrant both provides for the giving of such notice within 30 days after the date that the disclosure ends and prohibits, as part of the receipt of the requested information, the seizure of any tangible property or any other prohibited wire or electronic information as stated in 18 U.S.C. § 3103a(b)(2). As discussed in the attached agent affidavit, immediate notification of this warrant to the user(s) of the **Subject Telephones** may have an adverse result.

Similarly, pursuant to 18 U.S.C. § 2705(b) and 18 U.S.C. § 3123(d)(2), this application requests that the Court enter an order commanding the Carrier not to notify any person, including the subscriber(s) of the **Subject Telephones**, of the existence of the warrant until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date the Carrier complies with the warrant or such later date as may be set by the Court upon application for an extension by the United States, for the reasons outlined in the attached agent affidavit.

This application also seeks an order that: (1) authorizes the disclosure of the requested information whether the **Subject Telephones** are located within this District, outside of the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

District, or both, pursuant to 18 U.S.C. § 2703(c)(1)(A) and Rule 41(b), and, for good cause shown, at any time of the day or night pursuant to Rule of Criminal Procedure 41; (2) authorizes the disclosure of not only information with respect to the **Subject Telephones**, but also with respect to any additional changed telephone number(s) and/or unique identifying number, whether the changes occur consecutively or simultaneously, listed to the same wireless telephone account number as the **Subject Telephones** within the period of disclosure authorized by the warrant; and (3) orders the Investigating Agency to reimburse the applicable cellular telephone service provider for its reasonable expenses directly incurred in providing the requested information and any related technical assistance.

Finally, this application requests that it, the proposed warrant that has been concurrently lodged, and the return to the warrant be sealed by the Court until such time as the Court directs otherwise. Allowing disclosure to the public at large would likely

//

//

jeopardize the ongoing investigation for the reasons outlined in the attached agent affidavit.

Dated: August 13, 2020

Respectfully submitted,

TRACY L. WILKISON
Attorney for the United States,
Acting Under Authority Conferred By
28 U.S.C. § 515

SCOTT D. GARRINGER
Assistant United States Attorney
Deputy Chief, Criminal Division

MELISSA MILLS
Assistant United States Attorney

Attorneys for Applicant
UNITED STATES OF AMERICA

CERTIFICATION

In support of this application, and pursuant to 18 U.S.C. § 3122, I state that I, Melissa Mills, am an "attorney for the Government" as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure. I certify that the information likely to be obtained from the requested warrant is relevant to an ongoing criminal investigation being conducted by the Investigating Agency of the Target Subjects for violations of the Target Offenses.

I declare under penalty of perjury under the laws of the United States of America that the foregoing paragraph is true and correct.

August 12, 2020
DATE

MELISSA MILLS
Assistant United States Attorney
Public Corruption and Civil Rights Section

AFFIDAVIT

I, Andrew Civetti, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since September 2015. I am currently assigned to a Public Corruption Squad, where I specialize in the investigation of corrupt public officials, including bribery, fraud against the government, extortion, money laundering, false statements, and obstruction of justice. In addition, I have received training in the investigation of public corruption and other white collar crimes.

2. The FBI and United States Attorney's Office ("USAO") are investigating alleged corrupt activities at the Los Angeles Department of Water and Power ("LADWP") and the Los Angeles City Attorney's Office ("City Attorney's Office"), ("the Federal Investigation").

3. I am aware that the City receives in excess of $10,000 annually in federal funds through various programs.

II. PURPOSE OF AFFIDAVIT

4. This affidavit is made in support of an application for a warrant authorizing the disclosure of prospective cell-site information, as well as GPS information, as defined within the application, at such intervals and times as the government may request, and the furnishing of all information, facilities, and technical assistance necessary to accomplish said disclosure unobtrusively, which disclosure will establish the approximate

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

location of the following cellular telephones for a period of 45 days:

a. [redacted] a cellular telephone issued by Verizon ("Carrier 1"), subscribed to by MICHAEL FEUER and believed to be used by MICHAEL FEUER ("**Subject Telephone 1**");

b. [redacted] a cellular telephone issued by Carrier 1, subscribed to by [redacted] and believed to be used by LEELA KAPUR ("**Subject Telephone 2**"); and

c. [redacted] a cellular telephone issued by AT&T ("Carrier 2" and, together with Carrier #1, collectively referred to as the "Carriers"), subscribed to by an as-yet-unidentified person and believed to be used by JOSEPH BRAJEVICH ("**Subject Telephone 3**" and, together with **Subject Telephones 1 and 2**, collectively referred to as the "**Subject Telephones**").

5. As described more fully below, I respectfully submit there is probable cause to believe that cell-site information, as well as GPS information, likely to be received concerning the approximate location of the **Subject Telephones**, will constitute or yield evidence of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding) (the "Target Offenses"), being committed by MICHAEL FEUER, PAUL PARADIS, JACK LANDSKRONER, and others known and unknown (the "Target Subjects").

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information

obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of, or investigation into, this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. STATEMENT OF PROBABLE CAUSE

7. The probable cause articulated in the affidavit and exhibits attached hereto as Exhibit A is offered in support of this warrant.

8. The owners of the SUBJECT TELEPHONES, as officials and employees of the City of Los Angeles, are known to reside in the Central District of California and spend most of their time there. In addition, the Target Offenses occurred in the Central District of California.

9. I seek prospective cell-site/GPS information via this application because this information will assist me in gathering evidence in the ongoing investigation I have described above in the following ways: (1) I am investigating a conspiracy, and determining concert of action and contact between the conspirators is of value to my investigation; (2) the information will enable me to identify members of the conspiracy that I have not previously identified; (3) the information will provide insight into the roles and actions of the members of the conspiracy, and the criminal conduct committed by the people being investigated; (4) it will provide information regarding whether the individuals being investigated meet or have contact prior to, or after, committing any criminal conduct; and (5)

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

the information will often identify locations where evidence is stored and where search warrants may be appropriate. Moreover, it will assist in targeting surveillance conducted in this case, and reduce the risk of being detected and revealing the nature or fact of the investigation. People who are involved in criminal activity are often conscious of being followed and keep a close eye out for surveillance units. The chance of being discovered increases with the more surveillance that is done and the closer the surveillance units must get to the target subjects. Use of the prospective cell-site/GPS information enables the investigative team to be more focused and judicious in its use of surveillance to those times when it appears that events of significance are going to occur. It also enables the investigative team the ability to conduct surveillance at a greater distance, because the fear of losing the target is reduced when surveillance is maintained via GPS/cell-site information.

IV. GROUNDS FOR SEALING AND DELAYING NOTICE

10. Based on my training and experience and my investigation of this matter, I believe that reasonable cause exists to seal this application and warrant, as well as the return to the warrant. I also believe that reasonable cause exists to delay the service of the warrant by the Investigating Agency as normally required for a period of 30 days beyond the end of the disclosure period pursuant to 18 U.S.C. § 3103a(b) and, pursuant to 18 U.S.C. § 2705(b), to enter an order commanding the Carrier not to notify any person, including the subscriber(s) of the **Subject Telephones**, of the existence of the warrant until further order of the Court, until written notice is provided by the United States Attorney's Office

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

that nondisclosure is no longer required, or until one year from the date the Carrier complies with the warrant or such later date as may be set by the Court upon application for an extension by the United States. There is reason to believe that such notification will result in (1) destruction of or tampering with evidence; (2) intimidation of potential witnesses; or (3) otherwise seriously jeopardizing the investigation.

11. Furthermore, there is good cause for the warrant to be issued such that the information may be provided to law enforcement at any time of the day or night because in my training and experience, and knowledge of this investigation, the subjects of the investigation do not confine their activities to daylight hours, and it is often even more difficult to conduct surveillance at night.

///

///

///

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

V. CONCLUSION

12. For all of the above reasons, there is probable cause to believe that prospective cell-site information, as well as GPS information, likely to be received concerning the approximate location of the **Subject Telephones**, currently within, or being monitored or investigated within, the Central District of California.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this ____ day of August, 2020.

_____
HON. PATRICK J. WALSH
UNITED STATES MAGISTRATE JUDGE

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Exhibit A

AFFIDAVIT

I, Andrew Civetti, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since September 2015. I am currently assigned to a Public Corruption Squad, where I specialize in the investigation of corrupt public officials, including bribery, fraud against the government, extortion, money laundering, false statements, and obstruction of justice. In addition, I have received training in the investigation of public corruption and other white collar crimes.

2. The FBI and United States Attorney's Office ("USAO") are investigating alleged corrupt activities at the Los Angeles Department of Water and Power ("LADWP") and the Los Angeles City Attorney's Office ("City Attorney's Office"), ("the Federal Investigation").

3. I am aware that the City receives in excess of $10,000 annually in federal funds through various programs.

II. PURPOSE OF AFFIDAVIT

4. I make this affidavit in support of applications to seize and search the following cellular telephones:

a. Telephone number [redacted] located at the following office address, residence address, or alternatively on the person of **MICHAEL "MIKE" FEUER** ("**FEUER's PHONE**"):

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

i. **MICHAEL FEUER**, described in more detail in Attachment A-1;

ii. Los Angeles City Hall East, 200 N. Main Street, 8th Floor, Los Angeles, CA, Office of the City Attorney, identified and pictured in Attachment A-2 ("**FEUER's OFFICE**");

iii. [redacted], Los Angeles, California, identified and pictured in Attachment A-3 ("**FEUER's RESIDENCE**");

b. Telephone number [redacted] located at the following office address, residence address, or alternatively on the person of **LEELA KAPUR** ("**KAPUR's PHONE**"):

i. **LEELA KAPUR**, described in more detail in Attachment A-4;

ii. Los Angeles City Hall East, 200 N. Main Street, 8th Floor, Los Angeles, CA, Office of the Chief of Staff to the City Attorney, identified and pictured in Attachment A-5 ("**KAPUR's OFFICE**");

iii. [redacted], Toluca Lake, California, identified and pictured in Attachment A-6 ("**KAPUR's RESIDENCE**");

c. Telephone number [redacted] located at the following office address, residence address, or alternatively on the person of **JOSEPH BRAJEVICH** ("**BRAJEVICH's PHONE**"):

i. **JOSEPH BRAJEVICH**, described in more detail in Attachment A-7;

ii. Los Angeles Department of Water and Power, 221 N. Figueroa Street, 10th Floor, Los Angeles, CA, Office of

the General Counsel ("**BRAJEVICH'S OFFICE**"), identified and pictured in Attachment A-8;

iii. [redacted], Los Angeles, California, identified and pictured in Attachment A-9 ("**BRAJEVICH's RESIDENCE**").

5. In connection with the investigation into this matter, the requested search warrants seek authorization to search the respective offices, residences,[1] and persons of FEUER, KAPUR, and BRAJEVICH, described in more detail in Attachments A-1 through A-9, **FEUER's PHONE, KAPUR's PHONE,** and **BRAJEVICH's PHONE** (collectively, the **TARGET PHONES**, described in Attachment B), and seize any data on a **TARGET PHONE** that constitutes evidence of the criminal schemes identified herein and evidence or fruits of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding) (collectively, the "Subject Offenses"), and any **TARGET PHONE** that is itself an instrumentality of the criminal schemes and Subject Offenses, as also set forth in Attachment B. Attachments A-1 through A-9 and Attachment B are incorporated herein by reference.

[1] Based on my review of open source databases, California Department of Motor Vehicle records, and/or subscriber information for the **TARGET PHONES**, I believe the identified residences are the residences of FEUER, KAPUR, and BRAJEVICH respectively.

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, information obtained from other agents and witnesses [redacted] consensually recorded conversations, and information obtained from the prior related search warrants, as detailed further below. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

7. On January 28, 2020, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized search warrants for the seizure of information associated with iCloud accounts belonging to FEUER and BRAJEVICH (20-MJ-396), as well as Google accounts belonging to FEUER and KAPUR (20-MJ-397) (collectively, the "January 2020 search warrants"). On September 12, 2019, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized two search warrants (19-MJ-3813 and 19-MJ-3814) for PETERS's residence and person to seize PETERS's cell phone (collectively, the "September 2019 search warrants"). On July 18, 2019, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized two search warrants (19-MJ-2915 and 19-MJ-2923) for the seizure of information associated with nineteen e-mail accounts from two Internet Service Providers, and six search warrants (19-MJ-2913, 19-MJ-2914, 19-MJ-2917, 19-MJ-2919, 19-MJ-2920, and 19-MJ-2922) for the premises of sixteen

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

locations (collectively, the "July 2019 search warrants"). All of the July 2019 search warrants were supported by my single omnibus affidavit (the "omnibus affidavit"). The January 2020, September 2019, and July 2019 search warrants and my supporting affidavits are incorporated herein by reference. A copy of my supporting affidavit to the January 2020 search warrants is attached hereto as **Exhibit 1**. Copies of the affidavits supporting the September 2019 and July 2019 search warrants can be made available for the Court upon request.

III. RELEVANT BACKGROUND ON SUBJECTS

8. **MICHAEL FEUER** is the City Attorney for the City of Los Angeles. On July 22, 2019, during the execution of a search warrant at the City Attorney's Office, FEUER provided a voluntary recorded interview, portions of which are detailed herein.[2] Thereafter, FEUER provided certain additional information to the prosecution team via telephone or in person, either directly or via his Chief of Staff, LEELA KAPUR. [redacted] FEUER has indicated to the government on multiple occasions that he had plans to run for Mayor of Los Angeles in 2022 and he believed he would be among the favorites.[4]

[2] I was not present for this interview, but I have reviewed the FBI report and corresponding transcript.

[redacted]

[4] I was present for some, but not all, of such communications. Where I was not, I learned of FEUER's statements from other government personnel who were present.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. Based on my review of Apple ID subscriber information which registered **FEUER's PHONE** ([redacted] to an Apple ID account ([redacted] utilized by FEUER, my review of subscriber records for [redacted] and FEUER's use of [redacted] as recently as July 2020 to contact the prosecution team relating to the investigation, among other evidence, I believe that FEUER uses **FEUER's PHONE**.

b. Based on my review of an iCloud back-up produced by Apple, Inc., in response to the January 2020 search warrants, I believe that while **FEUER's PHONE** was used to register the Apple ID [redacted] as described in the affidavit supporting the January 2020 warrants, FEUER did not utilize that specific Apple ID to back up **FEUER's PHONE** to the iCloud, resulting in a lack of any iCloud data for that phone.[5]

9. **LEELA KAPUR** is FEUER's Chief of Staff, a position she has held since 2013. Based on my review of a contact card in FEUER's [redacted] iCloud back-up, as well as my review of KAPUR's emails, among other evidence, I believe that KAPUR uses **KAPUR's PHONE**.

10. **JOSEPH BRAJEVICH** is an Assistant City Attorney and the General Counsel for LADWP. Based on my review of subscriber records for **BRAJEVICH's PHONE**, iCloud records produced by Apple, Inc., in response to the January 2020 search warrants, and BRAJEVICH's use of **BRAJEVICH's PHONE** to contact the prosecution

[5] The Apple ID [redacted] was used to back-up (at least in part) another phone [redacted] utilized by FEUER and subscribed to FEUER's wife [redacted].

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

team, among other evidence, I believe that BRAJEVICH uses **BRAJEVICH'S PHONE**.

17. Other than what has been described herein to my knowledge, the United States has not attempted to obtain the contents of the **TARGET PHONES** by other means.

IV. STATEMENT OF PROBABLE CAUSE

25. As further detailed in the affidavits referenced above and incorporated herein, the FBI and USAO are conducting an ongoing investigation into the City Attorney's Office and LADWP, including a suspected bribery-fueled collusive litigation settlement that allegedly defrauded LADWP ratepayers out of many millions of dollars, an $800,000 hush-money payment made in order to conceal those collusive litigation practices, and obstruction of justice and perjury relating to this investigation.

26. As described in the attached January 2020 search warrants, there is probable cause to believe that FEUER made false or misleading statements to the investigation team, [redacted] wherein he denied knowledge of any hush money payment to conceal his office's litigation practices as well as knowledge of specific other details about the collusive litigation. As further detailed in that affidavit, the evidence supporting probable cause included text messages between BRAJEVICH, THOMAS PETERS (FEUER's then-Chief of Civil Litigation), and others; calendar entries for FEUER, KAPUR, BRAJEVICH, and PETERS; a surreptitious

audio recording of PETERS' contemporaneous statements detailing **FEUER's** knowledge; and corroborating proffer statements[6] by PETERS, among other evidence. The affidavit additionally set forth probable cause to believe that evidence of the Subject Offenses and criminal schemes identified above would be located in, among other places, the iCloud back-ups then believed to be linked to **FEUER'S PHONE** and **BRAJEVICH'S PHONE**, and in the City email accounts of FEUER, KAPUR, and BRAJEVICH.

27. Upon receiving the filtered data from FEUER's Apple ID [redacted] and the associated iCloud back-up pursuant to the January 2020 search warrants, the FBI learned that the data produced by Apple associated with FEUER's Apple ID [redacted] was from another phone that FEUER appeared to use primarily for personal purposes, but not from **FEUER's PHONE**, although **FEUER's PHONE** was the phone number used to register this Apple ID ([redacted] Based on my training and experience, I understand this to mean that **FEUER** utilized the Apple ID [redacted] for the other phone and backed up data from the other phone to this iCloud account, but did not back up data from **FEUER's PHONE** to this iCloud account. The FBI is not aware whether FEUER utilized a different Apple ID for **FEUER's PHONE** and if so, is currently unable to identify such an account. In the event that an Apple ID was identified for **FEUER's PHONE**, it is unknown whether

[6] Proffer statements provide use immunity for statements by a person in return for the information they provide. The written agreement, however, allows the government to use such information derivatively, including in search warrant applications.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

FEUER's PHONE utilized an iCloud back-up, what data/content, if any, existed in the back-up, and how much data/content was available based on how often back-ups occurred for the relevant time period. Based on my training and experience, individuals who utilize iCloud can select what content is and is not backed up. In addition, some applications and content is not backed up and therefore the only way to obtain the information would be from the phone itself. As such, the best way to obtain data is directly from **FEUER's PHONE**.

28. The filtered data from BRAJEVICH's iCloud account pursuant to the January 2020 search warrants indicated that while data from **BRAJEVICH's PHONE** was periodically backed up to BRAJEVICH's iCloud account, iMessages, text messages, SMS messages, and chats were not available or present in the records produced by Apple. As such, the only way to obtain that data from **BRAJEVICH's PHONE** would be from the phone itself.

29. Pursuant to the January 2020 search warrants, the FBI obtained from Google a substantial volume of data from the City email accounts of FEUER and KAPUR.[7] The review of that data is ongoing, and has been complicated and slowed by the government's protocols of filtering all data through a team of attorneys and the required ingestion and processing of voluminous data into a document-management database at multiple stages. Some of the relevant evidence reviewed to date is detailed below.

[7] The January 2020 search warrants also directed Microsoft to produce data from BRAJEVICH's email account. However, following service of the warrant, Microsoft advised that the contents of that account were not hosted by Microsoft and were likely stored on a server on LADWP premises.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

A. FEUER's Potentially False or Misleading Statements [redacted] That He Was Not Apprised of Key Portions of CLARK's Deposition Testimony

30. Filtered evidence from mike.feuer@lacity.org ("FEUER's CITY EMAIL") indicates that he may have provided misleading or false information to investigators [redacted] on at least one other topic beyond the two areas of apparent misleading or false statements described in the affidavit supporting the January 2020 search warrants and summarized briefly above. Specifically, FEUER [redacted] stated in his July 22, 2019 interview that he was not aware of the substance of the February 2019 deposition testimony of his Chief Deputy, JAMES CLARK, with the exception of one exchange that FEUER had inadvertently learned about from a reporter.[8] The single exchange about which FEUER [redacted] stated that he was aware centered around CLARK's testimony that he was sure that he had advised FEUER of the existence of the draft *Jones* complaint. According to FEUER, after learning of

[8] As noted in the prior affidavits referenced and incorporated herein, CLARK was selected to represent the City in a Person Most Qualified, or "PMQ," deposition in February 2019. During that deposition, CLARK gave significant testimony that was contrary to the City's official position and highly advantageous to the litigation position of the City's opponent, PwC. For example, CLARK testified that he was aware of the class action complaint against the City before it was filed, and that the City deliberately selected an opposing counsel because of his willingness to settle on terms favorable to the City. Following his PMQ testimony, CLARK met with counsel for the City and subsequently issued an errata purporting to change or reverse approximately 55 answers, many of them in a substantive manner that more closely adhered to the City's narrative. Following CLARK's first day of testimony on February 26, 2019, his PMQ deposition subsequently continued on April 9, 2019, and April 29, 2019.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

this exchange from the reporter, he told CLARK, "I don't recall such a conversation. We never had that conversation."

31. As detailed below, apart from that one exchange, FEUER was emphatic that he was otherwise not apprised of the substance of CLARK's testimony. [redacted] FEUER expounded on why it was important that he not be involved in or apprised of CLARK's ongoing PMQ deposition testimony before it was concluded (in late April 2019), because FEUER felt that CLARK needed to tell "his version of the truth without any influence from me." FEUER repeatedly stated that he was only aware of the one aforementioned exchange that he inadvertently learned about from a reporter.

32. In an interview with the investigation team on July 22, 2019, FEUER's statements about CLARK's deposition testimony included the following colloquy:

> Q. What about Mr. Clark's testimony? I understand that he testified in February of 2019. Did you read his transcripts?
>
> A. **I have not read the transcript, no.**
>
> Q. Did you speak with him in the wake of that deposition testimony?

33. FEUER apparently interpreted the above question as an inquiry about an instance in the deposition wherein a media outlet reported that CLARK testified about speaking with FEUER on a particular issue. FEUER stated that after CLARK's statement was brought to FEUER's attention via the media, FEUER spoke with CLARK about it. Specifically, according to FEUER:

A: I said to Mr. Clark at that point, "I don't recall such a conversation. We never had that conversation." And he did not recall even saying it in the deposition. So that was that. So we responded to the Daily Journal. Mr. Clark was -- I was told -- going to be correcting his deposition.

Q. Did you have conversations with him about that before it happened?

A. No. What I wanted to say to you is I did not want in any manner to have any conversation with Mr. Clark that would have any effect on his testimony, either the corrections or if he was then redeposed. So, obviously, I have views about these issues because I did not have such conversations. But I said to my staff, I want there to be no conversations and no inference that he could even draw about anything I think about this until his depositions are done.

34. FEUER further stated that although he was aware that his staff would be working with CLARK to correct any inaccuracies to the portion of his PMQ deposition that had already taken place, he directed his staff that, "I do not want Mr. Clark to draw or to have any sense of my views of his testimony." FEUER further stated that notwithstanding the brief conversation he initiated with CLARK about the above-referenced portion of testimony that FEUER had learned from the media, "I was very sensitive to the fact that Mr. Clark needed to be able to tell his version of the truth without any influence from me since my name was associated with his quote . . . . I did not want for a second for him to infer one way or the other my views on the topic until his testimony was finished."

35. In further describing his role with respect to CLARK's deposition and the many measures he purportedly took to remain distanced from it, FEUER stated as follows: "**I was never**

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

involved in, very purposely, with Mr. Clark's deposition testimony. I did not prepare him for the testimony. I did not accompany him to the deposition. **I was not apprised of his testimony after it was conducted**."

[redacted]

[9] [redacted] repeated explanations to the prosecution team [redacted] about the single instance of CLARK's PMQ deposition testimony that he was apprised of is consistent with his testimony in his own civil deposition in the *City v. PwC* case. When asked whether he was aware of a portion of CLARK's testimony, FEUER replied, "**I am not aware of the content of Mr.**

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

[redacted]

37. The review to date of FEUER's CITY EMAILS, which is ongoing, indicates that FEUER was in fact "aware of the content of Mr. Clark's deposition" because he was apprised by his staff in details as to numerous aspects of CLARK's PMQ deposition, [redacted].

38. On March 24, 2019, after CLARK's errata was issued but before his deposition testimony continued in April, KAPUR sent FEUER, via iPad, a lengthy email, partially provided below and in full (**Exhibit 2**), entitled, "Jim's Deposition," relaying excerpts from CLARK's first day of PMQ deposition and the subsequent corrections to his testimony as follows:

Clark's deposition, with one exception." He elaborated by detailing the above-referenced occasion on which he was contacted by a reporter with a question about CLARK's testimony, and then again confirmed that he had not read CLARK's testimony or the errata thereto. While false or misleading sworn testimony at a civil deposition in a state case would not, standing alone, violate federal law, it is consistent with what I perceive as FEUER's misleading or false narrative in an [redacted] intended to convey that FEUER had not been apprised of any portion of CLARK's deposition testimony, apart from that one clearly delineated exception.

> [Email from KAPUR to FEUER] Mike: **The following are some excerpts from Jim's depo.** I am paraphrasing but you will get the gist. O: indicates his original response and R: his revised. A: answers that weren't amended. Statements in quotation marks are statements Jim made (again sometimes paraphrased) but without the question attached. While I suspect much of this can be explained as the questions were less than precise, etc., I wanted you to get a feeling for the breadth of the confusing responses – many of which are not objectively clarified through documentation.
>
> Did Mr. Tom tell you he was aware that P[10] [PARADIS] had an atty/client relationship with Jones?
>
> O: I think so
>
> R: He did not
>
> Did P brief any (of our DWP attorneys) on nature of his representation of Jones?
>
> O: I don't know
>
> R: They say he did not.

39. Between one and eight hours[11] after KAPUR's March 24, 2019 email summarizing CLARK's deposition testimony and the corrections thereto was sent, FEUER forwarded it to his same City email address. It does not appear that any other address

[10] Based on my knowledge of the investigation, I believe all references to "P" are PAUL PARADIS, former special counsel for the City.

[11] The timestamp on KAPUR's email is 11:28 p.m. on March 24. The timestamp on FEUER's forward of the email is 12:31 a.m. on March 25; however; his email indicates the timestamp of KAPUR's original email as 4:28 p.m on March 24. In my review of FEUER'S and KAPUR'S CITY EMAILS, I have noted other instances of a time lag of seven hours between the timestamp on an email and the timestamp of the same email as indicated in a reply. Based on this review, I believe that the time lag is due to a computer reversion to Greenwich Mean Time (+0 hours) versus Pacific Standard Time (+7 hours).

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

was blind-copied, and I do not know why FEUER forwarded this email to himself.

40. Additionally, on two occasions, KAPUR emailed CLARK's deposition transcript to FEUER's secretary.[12] On March 12, 2019, KAPUR sent CLARK's rough deposition transcript without any text in her email. On March 18, 2019, KAPUR emailed CLARK's deposition transcript with "corrections interlineated," (which appeared to indicate that the changes that the City intended for CLARK to make in his errata were written into the transcript for each segment of purportedly erroneous testimony) and asked that it be printed, cautioning that it was "sensitive."

B. FEUER's Potentially False or Misleading Statement That He Was Not Aware of CLARK's Deposition Notes That CLARK Later Destroyed

41. In a recorded interview with the investigation team on July 22, 2019, FEUER was asked whether he was aware that CLARK testified that he had taken notes to prepare for his PMQ deposition. FEUER replied that he was not aware of that. When asked whether he would be concerned if CLARK had taken notes and had then destroyed or discarded them, FEUER described, at length, the circumstances in which CLARK's hypothetical destruction of notes would or would not have concerned FEUER, had he known about it. The interview contained the following colloquy:

[12] Based on my review of FEUER's and KAPUR's CITY EMAILS, while KAPUR was apparently assigned to a different secretary, KAPUR did occasionally send tasks or requests to FEUER's secretary, indicating that FEUER's secretary may have occasionally filled in for KAPUR's.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Q. **Are you familiar with that, during his own -- during some preparation for the deposition Mr. Clark was taking notes to prepare himself for the deposition?**

A. **No.** Again, I wasn't involved with the preparation.

Q. **And just -- if you grant that indulgence -- that, say, Mr. Clark had prepared notes or taken notes as part of his own preparation for his deposition, that he had done that, would you have any concerns about him destroying those notes prior to the deposition?** And destroyed, just thrown them away, shredded them up so they weren't available. Would that concerned you?

A. **You know, I'd have to -- the answer is I don't know.** I'd have to go back and look to see – I don't recall rules around preservation around -- certainly if we're in the middle of litigation and they were a document and we were required to preserve it, the destruction of that document as evidence would be wrong to do. Notes that he was taking in the course of that, I'd have to go back and look. I don't know what the rules are about that.

Q. **And then if during that deposition he referenced the fact that he didn't remember things that he had taken notes on that were then thrown away, would that concern you as just in terms of his own preparation for a deposition?** Where, if your employees take notes for a deposition, throws them away, and then at the deposition says they can't answer certain questions because he threw away his notes? It just strikes us as a little weird, a little odd for a preparation for a deposition.

A. **You know, I don't know.** Again, I think in retrospect, simple things are true. Hindsight is easy. But in retrospect, Mr. Clark had just returned from a couple-month medical leave. In retrospect, Mr. Paradis, if I had my druthers, would not have been preparing him for this deposition.

42. As noted above, in the aforementioned March 24, 2019 email summary of CLARK's PMQ deposition, KAPUR advised FEUER that CLARK had substantively testified as follows:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

> **"I discarded my notes last Friday. I don't need them (4-5 pages).**
>
> **Doesn't know and didn't ask if a retention order in place."**

43. Based on my training, experience, and knowledge of the investigation, I am aware that the emails of City officials and employees are subject to broad public disclosure obligations, including pursuant to the California Public Records Act, and that City officials and employees are often careful to refrain from including sensitive details in emails for that reason. From the ongoing review of FEUER's and KAPUR's CITY EMAILS obtained pursuant to the January 2020 search warrants, I am further aware that FEUER and KAPUR are cognizant of those disclosure obligations. As such, I believe that FEUER and KAPUR are likely more cautious in discussing sensitive matters, which would include issues related to the Subject Offenses and criminal schemes, via email, and more likely to discuss such matters by other means, including using the **TARGET PHONES**.

44. In reviewing FEUER's CITY EMAILS, I learned that he habitually created for himself draft emails (which were apparently not sent to anyone) with notes to himself about certain meetings, conversations, or other events, including several relating to the fallout from the DWP billing litigation. I believe that FEUER's practice of using email to memorialize his strategies, state of mind, and plans relating to the DWP billing litigation problems suggests a possible use of the Notes, Reminders, Pages, or other note-taking functions or applications on **FEUER's PHONE** to capture similar writings.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Examples of such draft emails that appear to relate to the Subject Offenses and criminal schemes include the following:

a. January 28, 2019 draft email:

From: 'Mike Feuer' <mike.feuer@lacity.org>
To:
Sent: 1/28/2019 9:51:14 PM
Subject:

any chance revealing could expose us to more than otherwise?
should we roll out last 2 piece first?
review 5 aspects:

- no obj
- jim
- mediation priv
- depo of indep monitor

how confer with jim? wasn't most of what berle did in dwp, not pwc case?

- mediation priv waiver
- depo of indep monitor
- jim as pmq

retain new counsel?

Based on my knowledge of the investigation, as further detailed in the attached affidavit, I believe that FEUER's statement in this January 28, 2019 draft email on the PwC matter asking himself, "any chance revealing could expose us to more than otherwise?" is likely a reference to his then-ongoing deliberations over whether to reveal information about PARADIS's and KIESEL's work on behalf of the plaintiff in the *Jones v. City* case, which — according to PETERS — PETERS discussed at length with FEUER and KAPUR in several conversations between January 25, 2019, and January 30, 2019. As further described in the attached affidavit, PETERS's proffer statements to that effect are corroborated by 1) a phone call, surreptitiously recorded by a third party, wherein PETERS related such a

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

conversation with FEUER; 2) calendar entries reflecting ongoing meetings between FEUER, KAPUR, and PETERS, on those dates (including January 28, 2019); and 3) voicemails from BRAJEVICH to PETERS.

b. March 8, 2019 and March 11, 2019 draft emails: Two draft unsent emails dated March 8, 2019 (entitled "Theory of the case"), and March 11, 2019 (no subject header), contained FEUER's articulated bullet-form narratives about his office's laudable achievement on behalf of the ratepayers in the *Jones* settlement, his adherence to the highest ethical standards, his plan for hiring an outside ethics expert, and his intent to hold PwC accountable for DWP's billing problems. This narrative was mirrored in FEUER's multiple public statements on the matter, as well as his [redacted] interview statements to the investigation team, and deposition testimony.

c. March 23, 2019 draft email: Another draft unsent email dated March 23, 2019, about his strategy for containing the fallout contains bullet points including the following: "depos —— DWP lawyer revelations," "email review —— no surprises/worst of worst," "criminal investigation," and "recs for my action —— th and j (implication)." The context and significance of these and other references is not entirely clear, but because the instant investigation was not public (and indeed was in its infancy) by that date, I believe the reference to "criminal investigation" may reflect FEUER's consideration of instigating a criminal investigation from his office, or his awareness of the possibility that other entities might commence

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a criminal investigation. I further believe that FEUER's reference to recommendations for his action as to "th and j" likely means ["THOM"] PETERS and ["JIM"] CLARK may relate to FEUER's consideration of whether to take employment or other measures relating to PETERS and CLARK for their role in the billing litigation and its fallout.

d. August 9, 2019 draft email: In another unsent draft email dated August 9, 2019, FEUER listed what appeared to be his talking points for a meeting with an individual appointed by City Council to oversee the City Attorney's Office's handling of the Jones/DWP/PwC situation. These talking points reflected FEUER's strategy for handling the various investigations and cases then pending. Additionally, FEUER set forth his bulleted arguments against the notion that FEUER should be recused from ongoing litigation in the matter.

e. August 29, 2019 draft email: In a draft unsent email dated August 29, 2019, FEUER itemized his vision for the optimal way forward in the DWP billing litigation morass, including the text of a statement that he hoped to obtain from the U.S. Attorney's Office asserting that neither he nor anyone from his office was a target or subject of this investigation.

45. Similarly, the limited data available from BRAJEVICH's iCloud account included three Notes, one of which appeared to briefly reflect a meeting at the mayor's office on March 27, 2019, relating to the DWP billing litigation. As described further in Exhibit 1 and in my other affidavits incorporated herein, multiple developments unfurled in the DWP billing

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

litigation during March 2019 that were detrimental to the City, including the resignation of the City's Special Counsel in the PwC litigation, a finding by the judge overseeing that litigation that there was evidence sufficient to establish a prima facie case of fraud by the City, and invocation of the Fifth Amendment by the plaintiff's attorney who had been recruited by the City's Special Counsel, among other events. As such, I believe that a meeting at the mayor's office on March 27, 2019, would likely have discussed facts relevant to the Subject Offenses and criminal schemes. I believe that this evidence suggests that BRAJEVICH may also have additional Notes or similar writings stored on his phone relevant to the Subject Offenses and criminal schemes.

C. Additional Evidence

a. I have reviewed Verizon toll records from **KAPUR's PHONE** for the calendar year 2019, which reflect 12 calls, on seven different dates, between **KAPUR's PHONE** and **FEUER's PHONE** from that year.[13] Based on my review of FEUER's and KAPUR's CITY EMAILS, most of these 12 calls appear to be temporally proximate to events reflected in those emails related to the collusive

[13] Based on information learned in the investigation as to the importance of the Chief of Staff position and FEUER's and KAPUR's close professional relationship, as detailed in the attached prior affidavit, I believe that FEUER and KAPUR would likely have engaged in calls on more than seven dates during 2019, which suggests that they may have been using other technology, such as FaceTime or another telephone application, to do so. Based on my training and experience, the Verizon phone tolls that I reviewed would only reflect direct cell-to-cell and would not indicate iMessages, FaceTime calls, or messages or calls using other secure applications. However, evidence of such messages or calls would potentially be stored on **FEUER's PHONE** and **KAPUR's PHONE**.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

litigation and the City's attempts to cast itself in a positive light following public revelation of details thereof. Moreover, all but one of these 12 calls are temporally proximate to email exchanges involving outside counsel for the DWP cases, suggesting that the substance of those calls likely included discussion of the DWP cases, possibly with outside counsel joining the calls.

46. Based on my training and experience and knowledge of this investigation, including information that I have received about the role of KAPUR as Chief of Staff to FEUER, I believe that the above-described evidence may suggest that FEUER and KAPUR primarily engaged in cell-to-cell communications when outside counsel was involved, and that they may have used other channels, such as FaceTime or another secure telephone application, for one-on-one verbal communications. I am aware from my training and experience that any such communications would not be reflected in the toll records for either subscriber, but that evidence of any such communications might be contained in their respective phones.

47. One call with **FEUER's PHONE** during 2019 reflected on KAPUR's toll records —— specifically at 2:02 a.m. on February 9, 2109 —— took place before the City's outside counsel was brought into the case (and thus would not have involved a call on FEUER's PHONE with them). I reviewed an email from that date wherein FEUER asked KAPUR, at 1:31 a.m., to call him, and he could explain when they spoke. In a follow-up email at 1:32 a.m., FEUER stated, "Shoulda said to use cell: [redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

[**FEUER's PHONE**]." I believe that FEUER's clarifying email asking KAPUR to call him on **FEUER's PHONE** and providing the number to her —— his longtime Chief of Staff —— may further suggest that their one-on-one verbal communications usually took place via some channel other than cell-to-cell calls.

D. Disclosure of Information Unrelated to Probable Cause

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

X. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[14]

51. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents,

[14] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

52. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

53. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress FEUER's, KAPUR's, or BRAJEVICH's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of FEUER's, KAPUR's, or BRAJEVICH's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

54. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

XI. CONCLUSION

55. Based on the foregoing, I request that the Court issue the requested search warrants.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this ____ day of August, 2020.

_____
HONORABLE PATRICK J. WALSH
UNITED STATES MAGISTRATE JUDGE

EXHIBIT 1

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of: Information associated with accounts identified as [redacted] joseph.brajevich@ladwp.com; and associated with the phone number [redacted] that is within the possession, custody, or control of Apple Inc.	)	Case No. 2:20-MJ-00396

APPLICATION FOR WARRANT PURSUANT TO 18 U.S.C. § 2703

I, a federal law enforcement officer, request a warrant pursuant to Title 18, United States Code, Section 2703, and state under penalty of perjury that I have reason to believe that within the following data:

See Attachment A-1

There are now concealed or contained the items described below:

See Attachment B

The basis for the search is:

☑ Evidence of a crime;
☑ Contraband, fruits of crime, or other items illegally possessed;
☐ Property designed for use, intended for use, or used in committing a crime.

The search is related to a violation of:

Code section(s)	*Offense Description*
18 U.S.C. §§ 371; 666; 1001; 1341; 1343; 1346; 1505; 1510; 1951; 1956; and 1621	Conspiracy; Bribery and Kickbacks Concerning Federal Funds; False Statements; Mail Fraud; Wire Fraud; Deprivation of Honest Services; Obstructing Federal Proceeding; Obstruction of Justice; Extortion; Money Laundering; and Perjury in a Federal Proceeding (collectively, the "Target Offenses").

The application is based on these facts:

See attached Affidavit, which is incorporated herein by reference.

Applicant's signature
Andrew Civetti, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: _____

Judge's signature

City and State: _____

Patrick J. Walsh, U.S. Magistrate Judge
Printed name and title

AUSA: Melissa Mills- Ext. 0627

ATTACHMENT A-1

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the Apple accounts associated with the below, and specifically including associated iCloud and iTunes accounts, that is within the possession, custody, or control of Apple Inc., a company that accepts service of legal process at 1 Infinite Loop, M/S 36-SU, Cupertino, California, 95014, regardless of where such information is stored, held, or maintained.

a. The Apple iCloud account, [redacted] associated with the phone number [redacted] and the name MIKE FEUER (**"FEUER's ACCOUNT"**);

b. The Apple iCloud account, [redacted] and Apple iCloud account, joseph.brajevich@ladwp.com, associated with the phone number [redacted] and the name JOSEPH BRAJEVICH (**"BRAJEVICH's ACCOUNT"**);

c. The Apple iCloud account associated with the phone number [redacted] and the name JAMES CLARK (**"CLARK's ACCOUNT"**).

ATTACHMENT B

I. SEARCH PROCEDURES INCLUDING PRIVILEGE REVIEW PROCEDURE

1. The warrant will be presented to personnel of Apple, Inc. (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below in Section IV.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.15.a. below), law enforcement agents and/or other individuals assisting law enforcement agents who are not participating in the investigation of the case and who are assigned as the "Privilege Review Team" will review the content records, according to the procedures set forth herein, to determine whether or not any of the content records appears to contain or refer to communications between an attorney, or to contain the work product of an attorney, or between a spouse and any person ("potentially privileged information"). The "Search Team" (law enforcement personnel conducting the investigation

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

and search and other individuals assisting law enforcement personnel in the search) will review only content records which have been released by the Privilege Review Team. With respect to the non-content information produced by the PROVIDER (see Section II.15.b. below), no privilege review need be performed and the Search Team may review immediately.

5. With respect to content records, the Search Team will provide the Privilege Review Team and/or appropriate litigation support personnel[1] with an initial list of "scope key words" to search for on the content records, to include words relating to the items to be seized as detailed below. The Privilege Review Team will conduct an initial review of the content records using the scope key words, and by using search protocols specifically chosen to identify content records that appear to be within the scope of the warrant. Content records that are identified by this initial review, after quality check, as not within the scope of the warrant will be maintained under seal and not further reviewed absent subsequent authorization or in response to the quality check as described below.

6. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for among the content records that are identified by the initial review and quality check described above as appearing to fall within the

[1] Litigation support personnel and computer forensics agents or personnel, including IRS Computer Investigative Specialists, are authorized to assist both the Privilege Review Team and the Investigation Team in processing, filtering, and transferring documents and data seized during the execution of the warrant.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

scope of the warrant, to include specific words like names of any identified attorneys or law firms and names of any identified spouses] or their email addresses, and generic words such as "privileged" and "work product". The Privilege Review Team will conduct an initial review of these content records by using the privilege key words, and by using search protocols specifically chosen to identify content records containing potentially privileged information. Content records that are not identified by this initial review as potentially privileged may be given to the Search Team.

7. Content records that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Content records determined by this review not to be potentially privileged may be given to the Search Team. Content records determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a Privilege Review Team Assistant United States Attorney ("PRTAUSA"). Content records identified by the PRTAUSA after review as not potentially privileged may be given to the Search Team. If, after review, the PRTAUSA determines it to be appropriate, the PRTAUSA may apply to the court for a finding with respect to particular content records that no privilege, or an exception to the privilege, applies. Content records that are the subject of such a finding may be given to the Search Team. Content records identified by the PRTAUSA after review as privileged will be maintained under seal by the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

investigating agency without further review absent subsequent authorization.

8. The Search Team will search only the content records that the Privilege Review Team provides to the Search Team at any step listed above in order to locate, extract and seize content records that are within the scope of the search warrant (see Section III below). The Search Team does not have to wait until the entire privilege review is concluded to begin its review for content records within the scope of the search warrant. The Search Team and the Privilege Review Team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

9. During its review, the Search Team may provide the Privilege Review Team and/or appropriate litigation support personnel with a list of additional "scope key words" or search parameters to capture the items to be seized as detailed below; any additional content records identified through this quality check must first be reviewed by the Privilege Review Team subject to the terms set forth herein before being released to the Search Team. This quality check is intended only to ensure that the initial scope key word review successfully eliminated only data outside the scope of the search warrant from seizure.

10. If, while reviewing content records or non-content information, either the Privilege Review Team or the Search Team encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

shall immediately discontinue its search pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

11. The Privilege Review Team and the Search Team will complete the search of non-content information and both stages of the search of the content records discussed herein as soon as is practicable but not to exceed 180 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the records beyond this 180-day period without first obtaining an extension of time order from the Court.

12. Once the Privilege Review Team and the Search Team have completed their review of the non-content information and the content records and the Search Team has created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the Search Team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, neither the Privilege Review Team nor the Search Team will access the data from the sealed original production which fell outside the scope of the items to be seized or was determined to be privileged absent further order of the Court.

13. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

14. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDER

15. To the extent that the information described in Attachment A is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each **TARGET ACCOUNT** listed in Attachment A:

a. All contents of all wire and electronic communications associated with the **TARGET ACCOUNT**, limited to that which occurred on or after December 1, 2014,[2] including:

i. All e-mails, communications, or messages of any kind associated with the **TARGET ACCOUNT**, including stored or preserved copies of messages sent to and from the account, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information

[2] To the extent it is not reasonably feasible for the PROVIDER to restrict any categories of records based on this date restriction (for example, because a date filter is not available for such data), the PROVIDER shall disclose those records in its possession at the time the warrant is served upon it.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

associated with each e-mail or message, and any related documents or attachments.

ii. All records or other information stored by subscriber(s) of the **TARGET ACCOUNT**, including address books, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files.

iii. All records pertaining to communications between the PROVIDER and any person regarding the **TARGET ACCOUNT**, including contacts with support services and records of actions taken.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), any alternate names, other account names or e-mail addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, **and including any changes made to any subscriber information** or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of

services used, and including the dates on which such changes occurred, for the following accounts:

(I) the **TARGET ACCOUNT**.

ii. All user connection logs and transactional information of all activity relating to the **TARGET ACCOUNT** described above in Section II.15.a., including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations, and including specifically the specific product name or service to which the connection was made.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

16. For each **TARGET ACCOUNT** listed in Attachment A, the search team may seize all information between December 1, 2014, and the present described above in Section II.15.a. that constitutes evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding), namely:

a. Information relating to who created, accessed, or used the **TARGET ACCOUNT**, including records about their identities and whereabouts.

b. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Retention of PAUL PARADIS and PAUL KIESEL, or entities related thereto, to represent the City of Los Angeles;

ii. Communications involving or relating to any party to, or to counsel for any party to, *Jones v. City of Los Angeles* (the "*Jones* matter") or *City of Los Angeles v. PricewaterhouseCoopers* (the "*PwC* matter"), including communications with or referencing MICHAEL FEUER, JAMES CLARK, THOMAS PETERS, PAUL PARADIS, PAUL KIESEL, GINA TUFARO, LEELA KAPUR, JOSEPH BRAJEVICH, Julissa Salgueiro, and other counsel and parties;

iii. Any lawsuit where the City was a party to the lawsuit and appears to have had a legal, representational, and/or financial interest in both sides of the lawsuit, including the *Jones* matter;

iv. The litigation of the *Jones* matter and the *PwC* matter, including discovery disputes, the deposition of the City's "person most qualified," and emails and other materials arguably or allegedly responsive to discovery demands or court orders;

v. Efforts to conceal the litigation practices of the City Attorney's Office's or members or representatives thereof in the litigation related to the LADWP billing system, including knowledge or direction of payments made or benefits

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

given to individuals or entities in an effort to discourage their revelation of those practices;

vi. Efforts to conceal actions by the City Attorney's Office or members or representatives thereof in the litigation related to the LADWP billing system, including shielding documents from production, filing false or misleading documents with the court, and offering false or misleading testimony;

vii. The City's actions, strategy, or tactics in responding to revelations or allegations of fraud, discovery violations, and unethical conduct in the litigation related to the LADWP billing system, including media outreach and contacts, litigation decisions, notification or lack of notification to the court of relevant developments, authorization of payment of hush money, and other actions;

viii. Negotiations or agreements relating to hush money payments offered to or solicited by any individual or entity to conceal business practices related to the LADWP billing litigation by the City Attorney's Office or members thereof, and communications relating thereto;

ix. Obstruction of justice, perjury, or false official statements related to the LADWP billing litigation;

x. Destruction or concealment of evidence related to the LADWP billing litigation.

c. Calendar or date book entries and notes, including calendars or date books stored on digital devices;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

d. All records and information described above in Section II.15.b.

IV. PROVIDER PROCEDURES

17. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. The PROVIDER shall send such information to:

[redacted]

18. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

19. IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 2705(b), that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A, of the existence of the warrant, until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date this warrant is signed by the magistrate judge or such later date as may be set by the Court upon application for an extension by the United States. Upon expiration of this order, at least ten business days prior to disclosing the existence of the warrant, the PROVIDER shall notify the filter attorney identified above of its intent to so notify.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AFFIDAVIT

I, Andrew Civetti, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since September 2015. I am currently assigned to a Public Corruption Squad, where I specialize in the investigation of corrupt public officials, including bribery, fraud against the government, extortion, money laundering, false statements, and obstruction of justice. In addition, I have received training in the investigation of public corruption and other white collar crimes.

2. I am currently one of the agents assigned to an investigation of alleged corrupt activities at the Los Angeles Department of Water and Power ("LADWP") and the Los Angeles City Attorney's Office ("City Attorney's Office"). As discussed in more detail herein, these activities include the following criminal schemes, among others:

a. Collusive litigation practices related to lawsuits involving the City Attorney's Office and LADWP, which were fueled in at least one instance by a $2.175 million kickback from plaintiff's attorney JACK LANDSKRONER to attorney PAUL PARADIS, a Special Counsel retained by the City Attorney's Office.

b. The concealment of an $800,000 hush-money payment to a prospective whistleblower by Special Counsels PARADIS and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

PAUL KIESEL in exchange for silence as to collusive and potentially fraudulent litigation practices involving PARADIS, KIESEL, and THOMAS PETERS, then the Chief of Civil Litigation at the City Attorney's Office, among others.

3. I am aware that the City receives in excess of $10,000 annually in federal funds through various programs.

II. PURPOSE OF AFFIDAVIT

4. I make this affidavit in support of applications for search warrants to Apple, Inc., Google, Inc., and Microsoft Corporation for the seizure of information associated with the following accounts (collectively, the "**TARGET ACCOUNTS**"):

Apple, Inc. Accounts

a. The Apple iCloud account,[1] [redacted] associated with the phone number [redacted] and the name MIKE FEUER (**"FEUER's ACCOUNT"**);

b. The Apple iCloud account, [redacted] and Apple iCloud account, joseph.brajevich@ladwp.com, associated with the phone number [redacted] and the name JOSEPH BRAJEVICH (**"BRAJEVICH's ACCOUNT"**);

[1] According to Apple's website, "iCloud stores your content securely and keeps your apps up to date across all your devices. That means all your stuff—photos, files, notes, and more—is safe and available wherever you are. iCloud comes with 5 GB of free storage and you can add more storage at any time." Based on my review of Apple's website and my review of Apple subscriber information, I understand that phone numbers are linked to iCloud Accounts to secure and retrieve data. Specifically, the use of iCloud with an Apple device and associated phone number may have content capturing an individual's utilization of that device.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

c. The Apple iCloud account associated with the phone number [redacted] and the name JAMES CLARK (**"CLARK's ACCOUNT"**);

Google, Inc. Accounts

d. Mike.Feuer@lacity.org (**"FEUER's EMAIL"**);

e. Leela.Kapur@lacity.org (**"KAPUR's EMAIL"**);

Microsoft Corporation Account

f. Joseph.Brajevich@ladwp.com (**"BRAJEVICH's EMAIL"**).

5. Apple Inc. ("PROVIDER #1") is a provider of electronic communication and remote computing services, headquartered at Cupertino, California. Google, Inc. ("PROVIDER #2") is a provider of electronic communication and remote computing services, headquartered at Mountain View, California. Microsoft Corporation ("PROVIDER #3") is a provider of electronic communication and remote computing services, headquartered at Redmond, Washington (collectively, the "PROVIDERS").[2]

[2] Because this Court has jurisdiction over the offenses being investigated, it may issue the warrant to compel the PROVIDERS pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). See 18 U.S.C. §§ 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction") and 2711 ("the term 'court of competent jurisdiction' includes -- (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that -- (i) has jurisdiction over the offense being investigated; (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title").

6. The information to be searched is described in Attachments A-1 through A-3. This affidavit is made in support of applications for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A) and 2703(d)[3] to require the PROVIDERS to disclose to the government copies of the information (including the content of communications) described in Section II of Attachment B. Upon receipt of the information described in Section II of Attachment B, law enforcement agents and/or individuals assisting law enforcement and acting at their direction will review that information to locate the items described in Section III of Attachment B subject to the search protocol and potential privilege review procedures outlined in Attachment B. Attachments A-1 through A-3 and Attachment B are incorporated herein by reference.

7. As described more fully below, I respectfully submit there is probable cause to believe that the information associated with the **TARGET ACCOUNTS** constitutes evidence, contraband, fruits, or instrumentalities of criminal violations

[3] The government is seeking non-content records pursuant to 18 U.S.C. § 2703(d). To obtain the basic subscriber information, which do not contain content, the government needs only a subpoena. See 18 U.S.C. § 2703(c)(1), (c)(2). To obtain additional records and other information--but not content--pertaining to subscribers of an electronic communications service or remote computing service, the government must comply with the dictates of section 2703(c)(1)(B), which requires the government to supply specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation in order to obtain an order pursuant to 18 U.S.C. § 2703(d). The requested warrant calls for both records containing content as well as subscriber records and other records and information that do not contain content (see Attachment B).

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding) (collectively, the "Target Offenses").

8. The facts set forth in this affidavit are based upon my personal observations, my training and experience, information obtained from other agents and witnesses [redacted] consensually recorded conversations, and information obtained from the prior related search warrants, as detailed further below. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

9. On September 12, 2019, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized two search warrants (19-MJ-3813 and 19-MJ-3814) for PETERS's residence and person to seize PETERS's cell phone (collectively, the "September 2019 search warrants"). On July 18, 2019, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized two search warrants (19-MJ-2915 and 19-MJ-2923) for the seizure of information associated with nineteen e-mail accounts from two Internet Service Providers, and six search warrants (19-MJ-2913,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

19-MJ-2914, 19-MJ-2917, 19-MJ-2919, 19-MJ-2920, and 19-MJ-2922) for the premises of sixteen locations (collectively, the "July 2019 search warrants"). All of the July 2019 search warrants were supported by a single omnibus affidavit (the "omnibus affidavit"). The September 2019 and July 2019 search warrants and their supporting omnibus affidavit are incorporated herein by reference, and copies can be made available for the Court.[4]

III. BACKGROUND ON SUBJECTS

10. MICHAEL FEUER is the City Attorney for the City of Los Angeles. On July 22, 2019, during the execution of a search warrant at the City Attorney's Office, FEUER provided a voluntary interview, portions of which are detailed herein.[5] Thereafter, FEUER provided certain additional information to the prosecution team via telephone or in person, either directly or

[4] In addition, on April 18, 2019, the Honorable Jacqueline Chooljian, United States Magistrate Judge, authorized search warrants relating to the Los Angeles Department of Water and Power's then General Manager, DAVID WRIGHT. Specifically, these warrants authorized search warrants for WRIGHT's phone, WRIGHT's laptop, two of WRIGHT's email addresses, and two of WRIGHT's Apple iCloud accounts (collectively, the "April 2019 search warrants"). On June 4, 2019, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized search warrants for two of WRIGHT's residences, WRIGHT's office, WRIGHT's cellular phone, and a burner cellular phone that the FBI had surreptitiously provided to WRIGHT, as well as for an e-mail account used by Deputy Los Angeles City Attorney JAMES CLARK; on June 18, 2019, Judge Walsh authorized a subsequent search warrant for WRIGHT's Riverside residence (collectively, the "June 2019 search warrants"). The April 2019 and June 2019 search warrants and their supporting affidavits are also incorporated herein by reference, and copies can be made available for the Court.

[5] For all interviews and proffer sessions detailed herein, I either attended the interview myself or received information from another FBI agent who attended.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

via his Chief of Staff, LEELA KAPUR. [redacted] FEUER has indicated to the government that he had plans to run for Mayor of Los Angeles in 2022 and he believed he would be among the favorites.

a. Based on my review of Apple iCloud subscriber information which registered **FEUER's ACCOUNT** to FEUER's phone number [redacted]), my review of PETERS's phone, including messages with FEUER at [redacted] my review of subscriber records for [redacted] and FEUER's use of [redacted] to contact the prosecution team relating to the investigation, I believe that FEUER uses **FEUER's ACCOUNT**.

b. Based on my review of e-mail records, I believe FEUER uses **FEUER's EMAIL**.

11. LEELA KAPUR is the Chief of Staff to FEUER.

a. Based on my review of PETERS's phone, I believe KAPUR uses the telephone number [redacted] Based on my review of e-mail records, I believe KAPUR uses **KAPUR's EMAIL**.

12. JOSEPH BRAJEVICH is an Assistant City Attorney and the General Counsel for LADWP.

a. Based on my review of Apple iCloud subscriber information which registered **BRAJEVICH's ACCOUNT** to BRAJEVICH's phone number ([redacted] my review of PETERS's phone, including messages with BRAJEVICH at [redacted] and

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

BRAJEVICH's use of [redacted] to contact the prosecution team about the investigation, I believe that BRAJEVICH uses **BRAJEVICH's ACCOUNT.**

b. Based on my review of e-mail records, I believe BRAJEVICH uses **BRAJEVICH's EMAIL**.

13. JAMES CLARK is the Deputy Chief for the Los Angeles City Attorney and a retired partner with Gibson, Dunn & Crutcher, LLP ("Gibson Dunn"). On November 7, 2019, CLARK submitted to a voluntary interview with the prosecution team in the presence of his attorneys and pursuant to a written proffer agreement.[7]

14. Based on my review of PETERS's phone, including messages with CLARK at [redacted] I believe that CLARK uses **CLARK's ACCOUNT**.

15. THOMAS PETERS was the Chief of Civil Litigation at the City Attorney's Office. On or about March 22, 2019, PETERS resigned from that position. PETERS has requested immunity from the government pursuant to 18 U.S.C. § 6001 et seq., as well as other protections and/or recommendations with respect to prospective investigations or actions by other authorities. The government continues to consider those requests and has neither acted on them nor made representations as to whether or not they will be granted. On January 28, 2019, the government

[7] Under the terms of the proffer sessions discussed herein, the government is allowed to make derivative use of the information provided to it. The government agrees only not to use the information against the provider of the information in the government's case-in-chief against that person, provided the person is entirely truthful in proffer sessions.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

interviewed PETERS in the presence of his attorneys and pursuant to a proffer agreement.

15. PAUL PARADIS is an attorney and partner at Paradis Law Group, PLLC, operating in New York and Los Angeles. At relevant times between 2015 and March 2019, PARADIS acted as Special Counsel for the City in a civil lawsuit against PricewaterhouseCoopers ("PwC") regarding an alleged faulty billing system, (Superior Court of California, captioned *City of Los Angeles v. PricewaterhouseCoopers*, Case No. BC574690 ("*PwC* case")).

a. I have interviewed PARADIS on numerous occasions regarding his involvement in the criminal schemes and Target Offenses detailed herein in the presence of his attorneys and pursuant to a proffer agreement. Much of the information provided by PARADIS has been substantially corroborated by other evidence, and other than the details provided in footnote 9 below, I do not have a reason to believe that PARADIS has provided untruthful information.

b. PARADIS has no criminal record and has agreed to assist the government in exchange for favorable consideration in a potential future prosecution of him related to his conduct in this matter.

c. PARADIS has provided the government access to his email account, cell phone, bank accounts, and many other documents relevant to the investigation. PARADIS has also made numerous consensual recordings at the request of the government, some of which are detailed in the omnibus affidavit.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

16. GINA TUFARO was at relevant times a New York attorney and the law partner of PARADIS.

a. On June 19, 2019, I interviewed TUFARO in the presence of her attorney [redacted][8]

b. [redacted]

17. PAUL KIESEL, a Los Angeles-based attorney, was at relevant times a Special Counsel for the City Attorney's Office on litigation relating to the LADWP billing system.

a. The government has conducted voluntary interviews with KIESEL in the presence of his attorney, as detailed in pertinent part below. To date and to my knowledge, information proffered by KIESEL has largely been consistent with other evidence, with the possible exception of the information provided in footnote 9.[9]

[redacted]

[9] In the first part of January 2020, KIESEL informed me that he intended to contact PARADIS about litigation strategy for a federal civil lawsuit (related to the events detailed herein) in which KIESEL and PARADIS were named as defendants. PARADIS contacted me to inform me that KIESEL had contacted him before PARADIS returned the contact. At my direction, PARADIS did not record the contact. Both KIESEL and PARADIS also reported back to me on the contact. Their accounts varied slightly in the following respect:

PARADIS reported that during the course of the discussion about the federal civil lawsuit, KIESEL asked whether they had a

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. KIESEL has also voluntarily provided certain documentary information, including text messages, emails, and a handwritten entry from his diary.

18. JULISSA SALGUEIRO was previously employed as a paralegal by KIESEL until approximately July 2017. Salgueiro submitted to a voluntary interview with the prosecution team [redacted]

19. [redacted] is an attorney affiliated with KIESEL's law firm. On December 5, 2019, [redacted] submitted to a voluntary interview with the prosecution team.

20. [redacted] is a law partner of KIESEL's firm. On January 14, 2020, [redacted] submitted to a voluntary interview with the prosecution team.

21. DAVID WRIGHT was the General Manager of LADWP until his resignation or dismissal on or about July 23, 2019.

a. I have interviewed WRIGHT on several occasions, including one voluntary interview without counsel during the execution of a search warrant at his home in June 2019, and several additional voluntary interviews in the presence of his

---

conversation with PETERS in late January 2019 about documents requested by *PwC* (a situation described in further detail below). PARADIS told me that he did not provide a substantive answer to KIESEL, but that he attempted to jog KIESEL's memory by reminding him about a location significant to the conversation that PARADIS recalled. KIESEL reported that PARADIS answered his substantive question and told KIESEL that they did in fact have such a conversation with PETERS. I do not know whether this discrepancy is attributable to a misunderstanding between KIESEL or PARADIS, a lapse of memory by one of them, or an intentional misstatement by one of them. Based on my history of interactions with both and the lack of any apparent reason for either to lie about this issue, I suspect that it was either a misunderstanding or a memory lapse.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

counsel and pursuant to a proffer agreement. At various points, I believe that WRIGHT provided untruthful information in response to my questions.

22. ROBERT WILCOX is a press spokesman for the City Attorney's Office.

VI. PRESERVATION REQUESTS & SEARCH WARRANTS

23. On or about December 4, 2019, the government sent Google, Inc. a preservation letter for **FEUER** and **KAPUR EMAILS** and Microsoft Corporation a preservation letter for **BRAJEVICH's EMAIL**.

24. On or about December 6, 2019, the government obtained orders pursuant to 18 U.S.C. § 2703(d) for information associated with the **FEUER, BRAJEVICH**, and **KAPUR EMAILS**.

25. On or about January 8 and 9, 2020, the government sent Apple Inc. subpoenas, nondisclosure orders, and preservation letters for subscriber information associated with the **FEUER, BRAJEVICH,** and **CLARK ACCOUNTS**.

26. Other than what has been described herein to my knowledge, the United States has not attempted to obtain the contents of the **TARGET ACCOUNTS** by other means.

IV. SUMMARY OF PROBABLE CAUSE

A. FEUER's Knowledge of Hush Money, [redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

[redacted] the evidence provides probable cause to believe that at FEUER's implied direction, PETERS ordered KIESEL to confidentially settle Salgueiro's demands or face termination of his Special Counsel contract. Specifically, as detailed further below, PETERS informed the government that he advised FEUER of Salgueiro's threats and demands, ordered KIESEL to buy Salgueiro's silence in accordance with FEUER's perceived direction, and apprised FEUER after the hush-money settlement that the matter had been taken care of. This information is corroborated in part by information proffered by PARADIS and KIESEL, as well as by documentary evidence.

B. FEUER's Knowledge of Special Counsel's Collaboration with Opposing Counsel and Collusive Litigation by January 2019, Contrary to His Later Statements [redacted]

28. Multiple sources of evidence provide probable cause to believe that FEUER obstructed justice, made materially misleading statements to the FBI, [redacted] relating to the timing of FEUER's knowledge that his Special Counsel (PARADIS and KIESEL) had collaborated with opposing counsel in a collusive lawsuit that allowed the City to settle multiple class actions on the City's preferred terms. Specifically, FEUER made official statements to the government [redacted] that I believe were intended to misleadingly indicate that

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

FEUER first learned about emails showing collaboration between Special Counsel and the City's opposing counsel on April 24, 2019, and that he immediately disclosed that information to the court, the City's litigation opponent, and the media. Based on my training, experience, and knowledge of the investigation, by misleadingly portraying FEUER's knowledge in this way, it appears FEUER was attempting to personally distance himself from this scandal likely for political gain (or to avoid political fallout).

29. However, the evidence indicates that PETERS apprised FEUER in as early as late January 2019 of the existence of those emails and the facts that they revealed. Specifically, as further detailed below, PETERS proffered that he told FEUER in late January 2019 about the emails and what they would show, that FEUER was very upset, that PETERS withheld them from discovery in the *PwC* matter at what he perceived to be FEUER's direction in order to conceal it from the court and the public, and that PETERS subsequently advised FEUER that FEUER no longer needed to worry about the documents being made public. This information is corroborated in part by a surreptitiously recorded phone call from January 27, 2019, wherein PETERS relayed to PARADIS, KIESEL, and TUFARO the substance of his initial contemporaneous conversation with FEUER. PETERS's proffer information is also partially corroborated by emails and calendar entries showing meetings between FEUER and PETERS related to the LADWP matters during the last week of January 2019, as well as with other evidence.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

V. STATEMENT OF PROBABLE CAUSE

25. The FBI is conducting an ongoing investigation into the City Attorney's Office and LADWP, including a suspected bribery-fueled collusive litigation settlement that allegedly defrauded LADWP ratepayers out of many millions of dollars, an $800,000 hush-money payment made in order to conceal those collusive litigation practices, and obstruction of justice and perjury relating to this investigation. Background facts relating to these and other facets of the investigation are further detailed in the omnibus affidavit referenced above and incorporated herein. The case numbers associated with the search warrants supported by my omnibus affidavit are outlined above.

A. [redacted]

1. Salgueiro's Initial Threats to Reveal Information Related to the Collusive Litigation and Demands for Hush Money

26. As further detailed below, the evidence indicates that Salgueiro obtained certain documents from KIESEL's law firm, including but not limited to documents reflecting coordination between the City's Special Counsel and the plaintiff's counsel in the *Jones* lawsuit, and threatened to reveal the documents if KIESEL did not pay her a large amount of money.

27. KIESEL advised the government of the following information:[10]

[10] As noted below, some of this information is corroborated by a contemporaneous diary entry provided by KIESEL; which I have reviewed.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. Around August or September 2017, KIESEL was approached by Salgueiro, an employee that his law firm terminated in or around July 2017.

b. Salgueiro told KIESEL that she had taken certain documents from the firm, including some that showed the City's entanglement in the representation of an adverse party that had sued the City in the LADWP billing system litigation.

c. Salgueiro initially demanded $1,500,000 from KIESEL, or she would take the materials public.

d. KIESEL was not initially concerned about Salgueiro taking the materials public, because although they might be "embarrassing" to the City, he did not believe that they reflected any wrongdoing.

28. Salgueiro advised the government [redacted] as follows:

a. Before leaving KIESEL's employ, Salgueiro took certain documents from KIESEL's firm that she believed would show that the firm and the City conspired to represent both sides of the litigation in the *Jones v. City of Los Angeles* matter and in other matters, including unrelated cases and employment-related matters (collectively, the "Salgueiro documents").[11]

[11] iro provided to the government, [redacted] electronic files that she described as the documents that she took from KIESEL's firm and threatened to review. These documents were submitted directly to the government's privilege-review team, and I have since reviewed a redacted version. They comprise several folders in different case names, with the documents relevant to the *Jones* matter

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. After Salgueiro was fired by KIESEL in or around July 2017, she demanded a large sum of money, around $900,000, from KIESEL in order to return the Salgueiro documents, refrain from taking the Salgueiro documents public, and resolve certain employment discrimination and harassment complaints.

c. KIESEL countered Salgueiro's demand with a lower five-figure offer, using former Special Counsel PAUL PARADIS as a mediator.

29. PARADIS proffered to the government as follows:

a. Salgueiro took the Salgueiro documents when she left KIESEL's firm and threatened to reveal them if KIESEL did not pay her a large sum of money.

---

marked "Jones." The documents from the "Jones" folder include the following relevant representative items:

- An April 16, 2015 email from KIESEL directing Salgueiro to prepare a notice of related case in the *Jones* matter "as though it was coming from Michael Libman, counsel for Jones, and NOT coming from us."
- Screenshots of apparent metadata indicating Salgueiro's preparation of various pleadings for both LANDSKRONER and the City
- Documents showing that Salgueiro and the KIESEL law firm filed documents for LANDSKRONER and LIBMAN on behalf of plaintiff Jones (including the first amended complaint), paid associated filing fees, and otherwise coordinated plaintiff's counsel's work
- Timesheets showing that Salgueiro billed time for her work preparing, finalizing, and filing documents on behalf of plaintiff Jones

The remainder of the documents (the ones not in the "Jones" folder) as provided to the prosecution team after filtering are heavily redacted, and any relevance they may have to this investigation is not presently clear to me based on the current evidence.

b. PARADIS believed that some of the documents related to the *Jones* matter, and others related to another matter wherein the City played both sides of litigation.

2. Awareness by FEUER, KAPUR, BRAJEVICH, CLARK, and PETERS of Salgueiro's Threats and Demands

30. Information from multiple sources, as detailed below, provides probable cause to believe that PETERS, acting at FEUER's implied direction, instructed KIESEL to pay the hush money that Salgueiro demanded to keep her from going public with her information, including information about secret collaboration between the City and plaintiff's counsel in the *Jones* case. The below information also constitutes probable cause to believe that BRAJEVICH and KAPUR were aware of the Salgueiro threats and demands and their context. The evidence further provides probable cause to believe that CLARK had some awareness of Salgueiro's threats to reveal sensitive documents relating to the *Jones* matter, although he may not have had a full understanding of the details.

a. KIESEL'S and PARADIS'S October 2017 negotiations with Salgueiro

31. On October 10, 2017, Salgueiro sent a text message, which I have reviewed, to PARADIS stating in pertinent part, "Hi Mr. P, I left a written message with Clark's asst. on Fri. re set up of mtg n didn't hear bk. 1. Okay 2 drop off set of docs w/note saying if w/like 2 discuss 2 call me?"

32. [redacted] in October 2017, she went to the City Attorney's Office to try to speak with CLARK, but he

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

was not there. According to Salgueiro, she left with CLARK's assistant a large envelope containing a copy of the Salgueiro documents, along with a message. [redacted]

33. As described below, the evidence indicates that KIESEL engaged in multiple initial attempts to negotiate with Salgueiro, which were unsuccessful due to KIESEL's unwillingness to pay an amount that Salgueiro was willing to accept.

34. KIESEL advised the government as follows:

a. KIESEL met with Salgueiro on October 30 or 31, 2017, in a meeting at LADWP headquarters coordinated by PARADIS, who was serving as a "mediator" between Salgueiro and KIESEL. An individual known as Rosa or "Mama Rosa" (later identified as Rosa Rivas) accompanied Salgueiro. At that time, Salgueiro demanded $900,000, in an offer that she said would remain open for 24 hours. KIESEL agreed to think about it and then countered with an offer of $60,000.

b. KIESEL then received a text message from Salgueiro that she would see him in CCW[12] on December 4, 2017, which KIESEL interpreted as a threat to publicize her information at the next-scheduled hearing in *City of Los Angeles v. PwC*, which was scheduled for that date in the Central Civil West courthouse.

35. PARADIS proffered the following relevant information:

[12] Central Civil West was at the time a Superior Court courthouse in Los Angeles, where the judge presiding over the *City of Los Angeles v. PwC* litigation was located.

a. On October 30, 2017, PARADIS and KIESEL met with Salgueiro and "Mama Rosa" at the LADWP cafeteria in an attempt to "mediate" Salgueiro's demands. At the conclusion of the mediation session, KIESEL informed PARADIS that he was willing to pay Salgueiro $120,000 to prevent her from publicizing the Salgueiro documents. Through PARADIS, Salgueiro countered that offer with a demand for $900,000 that would be open for 24 hours. On October 31, 2017, KIESEL told PARADIS that he rejected Salgueiro's $900,000 demand and would now offer $60,000 instead. PARADIS texted this new offer to Salgueiro, who texted both PARADIS and KIESEL that she would "c u both Dec. 4 at 2pm at CCW."

36. I have reviewed text messages between KIESEL, PARADIS, and Salgueiro which are substantively consistent with the above-referenced information.

b. November meetings with PETERS about Salgueiro

37. PETERS proffered the following information:

a. PETERS learned about Salgueiro's threats and demands from PARADIS during an in-person meeting with PARADIS and likely TUFARO on approximately November 16, 2017, after the first failed mediation with Salgueiro at LADWP headquarters.

b. At that initial meeting, the following took place:

i. PARADIS informed PETERS about the details of Salgueiro's demands, including that Salgueiro had threatened to reveal 1) certain attorney work-product documents that she had

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

taken from KIESEL's office, which included the *Jones v. PwC* draft complaint that the City was actively seeking to shield from production; 2) emails showing the transmittal of documents showing cooperation and coordination between the City and Jones' counsel (LANDSKRONER); 3) information that Salgueiro herself had filed the *Jones* lawsuit against the City (on behalf of KIESEL); and 4) other unidentified documents implicating cases involving the City.

ii. PETERS learned that KIESEL had engaged in a failed attempt to mediate Salgueiro's demands, and that this "mediation" had taken place at LADWP headquarters. PETERS felt that it was improper for the mediation to take place on City property.

iii. PETERS was "livid" to learn about the situation. He was particularly upset that KIESEL had not told him about Salgueiro's threats and demands, which PETERS felt that he had a need and a right to know.

iv. PETERS, PARADIS, and TUFARO agreed that they needed to have a discussion with KIESEL to talk about Salgueiro's threats and demands.

v. PETERS wanted to "impress on KIESEL the gravity of the situation."

vi. PARADIS told PETERS that KIESEL was not taking the situation seriously. PARADIS urged PETERS to be blunt in discussing the situation with KIESEL.

vii. PARADIS told PETERS that he "felt like a narc" for "ratting KIESEL out" and sharing this information with

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

PETERS without KIESEL's knowledge. PARADIS asked PETERS to "cloak" the fact that PARADIS was the source of the information. PETERS agreed to do so.

c. On November 17, 2017, PETERS sent KIESEL a series of text messages demanding that KIESEL come to his office immediately. KIESEL and PARADIS came to PETERS's office that day. At that November 17, 2017 meeting, the following occurred:

i. PETERS "read the riot act" to both KIESEL and PARADIS about the Salgueiro situation. PETERS included PARADIS to "cloak" the fact that he had learned the information from PARADIS, pursuant to PARADIS's request.

ii. PETERS asked KIESEL how KIESEL could not have shared the information with PETERS earlier. PETERS said that both PETERS and FEUER had a need and a right to know about Salgueiro's threats and demands, because this was an issue that could result in negative press coverage for the City Attorney's Office.

iii. PETERS, KIESEL, and PARADIS discussed the merits of Salgueiro's threats and demands, including the fact that Salgueiro was threatening to reveal documents relating to the *Jones* matter and other City litigation if KIESEL did not pay her money. PETERS recalled learning that Salgueiro was seeking "millions of dollars" from KIESEL.

iv. KIESEL was resistant to the idea of paying Salgueiro what she was asking. KIESEL told PETERS that he planned to hire a crisis-management person, an action that

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

PETERS considered ancillary to the City's more pressing concerns.

v. PETERS strenuously imparted to KIESEL that it was in his best interest to pay Salgueiro what she was asking to ensure that she did not make her information public.

vi. PETERS told KIESEL that if he did not take care of the situation, KIESEL would not be able to continue representing the City.

d. PETERS understood that Salgueiro had certain employment-related claims that she would agree not to pursue if KIESEL paid her to get the documents back. From PETERS's experience and his knowledge of Salgueiro, specifically her age, gender, ethnicity, termination after a medical leave for an allegedly work-related injury, and length of employment, PETERS believed that Salgueiro's employment claims might present a litigation risk for KIESEL.[13]

---

[13] Based on information provided by PETERS, KIESEL, PARADIS, and Salgueiro, I understand that Salgueiro was prepared to allege employment claims that included: 1) her termination after a lengthy medical leave; 2) unfulfilled promises that she believed KIESEL had made, including to pay for her to attend law school; and 3) KIESEL's general harsh or demanding treatment of her throughout her employment.

Based on that information and other information described herein, it is my belief that Salgueiro's threat to bring an employment lawsuit against KIESEL might have conferred a credible litigation risk to KIESEL and his firm. However, I further believe that such a lawsuit would not have been substantially damaging to the City. I also believe that the City's primary or sole concern in seeking to convince KIESEL —— who was reluctant to pay and willing to risk public revelation of all the information —— to pay to resolve Salgueiro's claims, was a desire to conceal the documents concerning the City's collaboration with Jones.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

e. PETERS viewed Salgueiro's demands as creating a "crisis situation" for himself and for the City Attorney's Office. PETERS believed that if the Salgueiro information were revealed, it would not only be embarrassing for the City Attorney's Office, but it would also implicate the candor of the process by which the *Jones* settlement had been approved. PETERS believed that the revelation of previously undisclosed cooperation between PARADIS/KIESEL and LANDSKRONER in the preparation of a complaint to sue the City could imperil the *Jones* settlement, including by providing objectors to the settlement with a foundation to reopen the objections that they had already unsuccessfully raised.

38. During CLARK's proffer, he advised the government that he was not familiar with any threats to reveal documents or information relating to the collusive litigation or demands for hush money, and that he did not recall ever receiving any such documents, information, or contacts. CLARK further advised that such events would have been significant and memorable in his opinion, and that he believed he would have recalled them if he observed them.[14]

---

[14] Multiple witnesses, including FEUER and CLARK, have advised that CLARK suffered from [redacted] during a period that included 2017 and 2018, which affected CLARK's functionality at work and culm[redacted]ical leave during late 2018 and early 2019 [redacted] CLARK advis[redacted] that his [redacted] problem was resolved by February 2019, when he recommenced work. However, during the July 22, 2019 court-[redacted]ce, the FBI found approximately [redacted] hidden throughout CLARK's small office space. The government immediately advised FEUER of

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

39. Based on the foregoing and my knowledge of the investigation, I believe that CLARK, at some point, had some awareness of Salgueiro's threats, but may not have had a full understanding of the scope of the information that Salgueiro was threatening to reveal. I further believe that CLARK delegated handling of this situation to PETERS with an express directive that it be taken care of.

40. KIESEL advised the government as follows:

a. On November 17, 2017, KIESEL received a series of text messages from PETERS demanding that KIESEL come to see him immediately.[15]

b. KIESEL left a court proceeding in Orange County to drive to PETERS's office at City Hall East in Los Angeles, where he and PARADIS met with PETERS.

c. During that meeting, PETERS was visibly angry and told KIESEL to make the problem go away or KIESEL and PARADIS would be fired. PETERS told KIESEL and PARADIS that Salgueiro

[redacted]

[15] I have reviewed text messages between PETERS and KIESEL on that date that corroborate this information.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

had called the City Attorney's Office asking to speak with FEUER, that FEUER had not taken the call, and that the call was routed to CLARK, who re-routed the call to PETERS and directed him to handle it. KIESEL further advised that his sense was that CLARK did not have a full awareness of the situation, and that KIESEL did not recall any in depth conversations with CLARK about Salgueiro.

d. During the meeting, PETERS told KIESEL to do "whatever it takes" and "whatever it costs," which KIESEL understood as a directive to pay whatever Salgueiro was asking to buy her silence.

e. KIESEL believed that Salgueiro had a "legitimate severance demand" based on her employment with him. However, KIESEL did not see any issues with the prospect of the Salgueiro documents being publicly revealed, because the City was fully aware of what those documents contained, and KIESEL did not think they would make the City look bad.

f. KIESEL was reluctant to pay what Salgueiro was asking, but he did not want to be fired from the Special Counsel role, particularly after investing substantial time and resources into the case of *City of Los Angeles v. PwC* over approximately three years without any compensation (because the Special Counsel contract provided for compensation for KIESEL and PARADIS only on a contingency-fee basis). KIESEL had by that time spent approximately a quarter million dollars of his own money on costs associated with the case, which contributed to his desire to remain on the case to recoup that investment.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

g. KIESEL could not recall whether PETERS told him that FEUER was aware of Salgueiro's threats and demands, but he believed that PETERS and CLARK would have told FEUER. Based on the circumstances and relationships that KIESEL observed, he "could not imagine" that CLARK and PETERS would not have told FEUER about this situation, because they were "good soldiers" to FEUER.

41. KIESEL further advised the government that after the aforementioned meeting wherein PETERS threatened to fire him, he subsequently met with PETERS again, and that PETERS had calmed down. At that time, PETERS indicated that he would not terminate the contract, and that they would see what happened.

42. KIESEL advised the government that since approximately 1980, he has regularly kept a handwritten diary on noteworthy events in his life. KIESEL showed the government (and provided a copy of) an entry in his diary that was dated December 1, 2017, that appears to recount KIESEL's recollection of the above-described November 2017 meeting in which PETERS called KIESEL up from Orange County to discuss Salgueiro's threat. According to the entry, which described PETERS as "spitting MAD" (emphasis in original), PETERS told KIESEL, "How could you not tell me about this threat, Paul??" The entry further reports, "Thom [PETERS] said you have 2 choices. Either settle with J [Salgueiro] or your FIRED!" (emphasis in original).

43. The above-described diary entry provided by KIESEL dated December 1, 2017, further related KIESEL's efforts to address and resolve Salgueiro's demands following his meeting

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

with PETERS. It then stated as follows: "Last Wed [November 29, 2017], I met, again, with Thom [PETERS] + laid all of this out and thankfully he understood + indicated he would not terminate us + we'll see how things develop."

44. I believe that the contemporaneous information from KIESEL's handwritten diary related herein is consistent with the information provided herein and other evidence described herein as to events surrounding Salgueiro's threat.

45. PARADIS proffered the following relevant information:

a. After Salgueiro's warning that she would see them at the *PwC* hearing, PARADIS grew concerned that the situation with Salgueiro was "rapidly escalating out of control" and that PETERS needed to be apprised of the details.

b. On November 6, 2017, PARADIS left a voicemail for PETERS advising that there were a couple of matters they needed to discuss and asking to meet.[16]

c. On November 16, 2017, PARADIS and TUFARO met with PETERS in PETERS's office and informed PETERS of the status of the Salgueiro situation, including that she was threatening to reveal documents relating to her employment-related claims as well as documents showing potential conflicts in the *Jones* case and other cases. PARADIS related the following relevant information about that meeting:

i. PETERS described CLARK's involvement in the Salgueiro matter, as detailed above.

[16] PETERS's phone does not reflect such a voicemail on that date; rather, it reflects a text message from PARADIS asking for a meeting with PETERS.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

ii. PETERS discussed the merits of Salgueiro's employment claims and noted that he had witnessed first-hand KIESEL's treatment of Salgueiro when PETERS worked at KIESEL's firm.

iii. PETERS stated that KIESEL had been primarily responsible for PETERS's wife being appointed as a Superior Court judge, because KIESEL had exerted his influence in the selection process. PETERS further shared his goal to also be appointed as a judge after leaving the City Attorney's Office, and he stated that he was aware of KIESEL's influence over that process as a member of the Governor's Committee that recommended candidates for judgeships, which was a factor in PETERS wanting the matter resolved promptly without becoming public.

iv. PETERS and PARADIS discussed a variety of approaches and then agreed that PETERS should text KIESEL the following morning to tell KIESEL that PETERS urgently wanted to see him in his office. They further agreed that KIESEL should not be informed that PETERS and PARADIS had met on November 16, 2017. At PARADIS's urging, they also agreed that PETERS should "take a very stern approach" with KIESEL, demand that he resolve the situation with Salgueiro, and threaten KIESEL with termination as Special Counsel if he did not do so. They did not discuss invoking FEUER's name as part of such an approach.

d. After their meeting on November 16, 2017, PETERS called PARADIS that evening to further discuss the planned conversation with KIESEL.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

e. On the morning of November 17, 2017, PARADIS left a voicemail for PETERS and subsequently received a call back from PETERS. PETERS stated that he was going to text KIESEL and PARADIS as they had previously discussed.[17]

f. Later that day, PARADIS and KIESEL met with PETERS in PETERS's office. During that November 17, 2017 meeting, the following took place:

i. PETERS did not disclose to KIESEL that he had met with PARADIS and TUFARO the day before about the Salgueiro matter.

ii. According to PETERS, he had learned from CLARK that CLARK had received from Salgueiro a package and two phone calls requesting a meeting. PETERS relayed that CLARK had advised him as follows: [18]

(I) CLARK was "fucking pissed" about the fact that Salgueiro had brought this to CLARK's attention, and CLARK had not responded because he did not intend to meet with Salgueiro.

(II) CLARK told PETERS that he wanted KIESEL's situation with Salgueiro resolved so that it did not become public.

---

[17] According to the phone records, PETERS had already begun texting KIESEL by the time PARADIS said that he had this conversation with PETERS.

[18] PETERS proffered that he could not remember discussing the Salgueiro matter with CLARK before the settlement was paid, but did specifically remember a conversation with CLARK about it after the matter was resolved.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

(III) CLARK asked PETERS what Salgueiro was complaining about specifically, and PETERS explained to CLARK that Salgueiro was complaining about KIESEL "having been on both sides of several cases" related to the approximately six cases reflected in the documents that Salgueiro had provided in her package to CLARK.

(IV) PETERS stated his understanding that at least two of the cases on which Salgueiro was threatening to reveal information were litigation with the City, and that one was the *Jones v. City* case.

iii. PETERS advised that he had already informed FEUER about this situation. PETERS stated that FEUER was extremely unhappy about it, and that if it was not immediately cleaned up, KIESEL's firm, and probably PARADIS's firm too, would be terminated as Special Counsel to the City in the *PwC* case.

iv. KIESEL was resistant and stated that Salgueiro was unreasonable, that he was not prepared to pay her $900,000, and that he viewed her threats as extortion.

v. PETERS stated that while he understood Salgueiro was demanding a large amount of money, PETERS, FEUER, and CLARK had no choice but to demand that KIESEL work out a deal with Salgueiro to pay her because the City Attorney's Office could not tolerate this situation becoming public.

vi. PETERS ended the meeting by firmly directing KIESEL to work out a deal with Salgueiro to buy her silence and ensure that her information did not become public. PETERS also

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

again made clear that if KIESEL did not comply quickly, he, and likely PARADIS also, would be terminated.

46. PARADIS proffered that after the November 17, 2017 meeting, KIESEL left, and PETERS stopped PARADIS on the way out to instruct PARADIS to reiterate to KIESEL what was going to happen if KIESEL did not agree to pay Salgueiro off. PARADIS indicated that he would do so.

47. PARADIS proffered that at the time of the November 17, 2017 meeting, PARADIS was unsure as to whether PETERS had truly informed FEUER about Salgueiro's threats, or whether that was simply a tactic that PETERS was using to try to convince KIESEL to comply. However, PARADIS did not think that PETERS would take the actions he did without apprising FEUER, because PETERS was afraid of FEUER and would have wanted to "cover his ass."[19]

c. PETERS's November discussions with FEUER and BRAJEVICH about Salgueiro's threats and demands

48. PETERS proffered that at some point after the aforementioned November 17, 2017 meeting and before December 1, 2017, PETERS spoke with FEUER as another meeting was breaking up. PETERS provided the following relevant information as to that conversation:

a. PETERS did not specifically recall whether anyone else was present during this conversation, but he believed that

[19] As noted below, PARADIS proffered that PETERS later confirmed to him that he in had in fact informed FEUER about Salgueiro's threats and demands.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

KAPUR was probably present, and that Robert Wilcox (FEUER's media spokesman) might have been there as well.

b. During this conversation, PETERS told FEUER that a disgruntled former employee of KIESEL's was threatening to reveal documents including the draft *Jones v. PwC* complaint, which FEUER was then aware was the subject of a contested motion to compel in the *PwC* case, as well as other documents showing cooperation and coordination between PARADIS and Jones' counsel (JACK LANDSKRONER) before the *Jones* complaint was filed that had not previously been disclosed to PwC or the court. According to PETERS, FEUER was already aware that there had been some cooperation between PARADIS and the plaintiff's counsel.

c. PETERS advised FEUER that the former employee seemed irrational, was being guided by a "guru," and was "holding the City hostage" by threatening to reveal these documents, which PETERS characterized as the City's attorney work product.

d. PETERS provided this information as a "heads up" to FEUER, as PETERS knew that FEUER always wanted to be made aware of matters that might be reported in the press.

e. FEUER was upset by this information and questioned how KIESEL could have let this happen.

f. It was apparent to PETERS that FEUER, whom PETERS characterized as "a very smart man," immediately saw the risk to the City inherent this situation.

g. PETERS assured FEUER that PETERS was monitoring the situation.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

49. PETERS proffered that on November 30, 2017, PETERS received a call from BRAJEVICH, and they spoke on the phone.[20] PETERS had not told BRAJEVICH about the Salgueiro situation, but BRAJEVICH already had some awareness of it, including the fact that KIESEL and PARADIS had attempted to mediate the dispute with Salgueiro at LADWP headquarters. PETERS proffered the following with respect to that conversation:

a. BRAJEVICH asked PETERS how much PETERS knew about the Salgueiro situation, and PETERS gave BRAJEVICH some details about her threats and demands.

b. PETERS told BRAJEVICH that he was scheduled to discuss the issue with FEUER the following day (Friday, December 1, 2017), and he invited BRAJEVICH to join that discussion.

c. PETERS believed that BRAJEVICH needed to be involved in the discussions about Salgueiro's threats and demands, for two reasons. First, BRAJEVICH was effectively supervising KIESEL's and PARADIS's work on the matter to which Salgueiro's threats related. Second, LADWP headquarters, where the failed "mediation" had taken place, was BRAJEVICH's "domain" (as LADWP General Counsel).

d. The December 1, 2017 meeting with FEUER, KAPUR, BRAJEVICH, and PETERS about Salgueiro

[20] I have reviewed an email from this date to PETERS from his secretary requesting that PETERS call BRAJEVICH. As described below, a subsequent meeting invitation indicates that BRAJEVICH was scheduled to telephonically join a previously scheduled December 1, 2017 meeting with FEUER, KAPUR, and PETERS on the *PwC* case.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

50. PETERS proffered that on Friday, December 1, 2017, PETERS participated in a scheduled meeting with FEUER, KAPUR, and BRAJEVICH (called in) to provide an update on the Salgueiro situation.[21] PETERS proffered the following information about this December 1 meeting:

a. The Salgueiro situation —— which PETERS described as "the issue du jour" at that time, in light of Salgueiro's looming threat to appear at the Monday, December 4 hearing —— was the primary or sole focus of that planned meeting.

b. The meeting took place at the end of the day in FEUER's office.

c. BRAJEVICH was not present in person but instead called in to the meeting to participate by telephone.

d. PETERS provided an "update on the state of play" of the Salgueiro situation, including that Salgueiro still had the documents showing cooperation between the City and Jones, and that Salgueiro had threatened to appear at the hearing set for Monday, December 4, 2017.

e. The participants discussed the likelihood that if Salgueiro appeared at the hearing, she would try to file or give the documents.

---

[21] As noted herein and detailed below, I have reviewed a calendar entry for FEUER and a meeting invitation reflecting this meeting from 4:45 p.m. to 5:00 p.m. PETERS proffered that he could not recall whether anyone else attended this meeting. He opined that FEUER's press spokesman, Rob Wilcox, [redacted]ve here" if available. PETERS also stated that [redacted], FEUER's Chief of Intergovernmental Relations, might also have attended. As noted herein, documents reflecting the scheduling of this meeting do not indicate that either Wilcox or [redacted] was invited.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

f. The participants discussed the possibility that Salgueiro would invite the press to attend the hearing in order to publicize the information to the media.

g. FEUER and BRAJEVICH expressed frustration that KIESEL had not been able to take care of the problem and reach an "accommodation" with Salgueiro.

h. FEUER stated that KIESEL needed to do whatever needed to be done to take care of the situation.

i. Accordingly to PETERS, it was "absolutely clear" and understood by all participants at this meeting that Salgueiro was demanding money from KIESEL in exchange for the return of the documents.

j. PETERS told FEUER that he would personally attend the Monday hearing, in light of Salgueiro's threat to show up. FEUER did not ask PETERS to attend the hearing, but PETERS preemptively offered because he knew from his prior experience with FEUER that this was what FEUER would want.

k. FEUER conveyed that he was confident that PETERS could handle the situation.

l. Both FEUER and BRAJEVICH expressed the view that it was outrageous that the "mediation" had happened on City property.

51. According to an electronic calendar entry, there was a scheduled meeting regarding the *PwC* case between FEUER, KAPUR, PETERS, and BRAJEVICH on December 1, 2017, from 4:45 p.m. to 5:00 p.m. The meeting notice specified that BRAJEVICH would be participating by phone.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

52. In a text message on December 1, 2017, at 5:07 p.m., using **BRAJEVICH's ACCOUNT**, BRAJEVICH said to PETERS, "Thom- when you have a chance **I want to follow on the fact that the mediation took place at DWP**. Not urgent and can wait until Monday. Thanks and have a great weekend." Metadata from PETERS' phone indicates that PETERS opened this message at 9:19:10 p.m on that same date.

a. PETERS proffered that he understood this to refer to KIESEL's attempted "mediation" with Salgueiro on LADWP property, which he and BRAJEVICH and others had discussed in the aforementioned meeting that afternoon.

53. In a text message on December 1, 2017, at 9:18:57 p.m., PETERS told PARADIS, **"Mike is not firing anyone at this point. But he is far from happy about the prospect of a sideshow. Also, mediating Paul's matter at DWP, not a popular move.** We can speak over the weekend. Thanks."[22]

a. PETERS has informed the government that this message meant to convey that FEUER had considered and then rejected the idea of firing PARADIS and KIESEL, but that FEUER considered the threatened release of documents by SALGUEIRO to be a prospective "sideshow" that would impair both the litigation and the reputation of FEUER's office. The "sideshow" was a reference to media attention.

[22] Based on my general knowledge of text messaging services, I am aware that a user receiving a text message can often see a banner containing part or all of a message without opening the message. Based on the sequence of events and timing of these messages, I believe PETERS may have viewed BRAJEVICH's message via such a banner, sent the related message to PARADIS, and then opened BRAJEVICH's message in order to reply to it.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

54. Based on my knowledge of the investigation and the above-described information and timeline, I believe that the "mediation at DWP" discussed in the BRAJEVICH-PETERS and PETERS-PARADIS texts, both from December 1, 2017, referenced KIESEL's unsuccessful attempts to negotiate Salgueiro's demands for hush money, as directed by PETERS at FEUER's implied direction.

55. I further believe that BRAJEVICH's message to PETERS — — which BRAJEVICH sent seven minutes after his meeting with FEUER, KAPUR, and PETERS about the *PwC* matter was scheduled to end, and which asked to "follow on the fact that the mediation took place at DWP" —— suggests that this topic of KIESEL's dispute with Salgueiro and its bearing on the City's interest in the *PwC* case was likely discussed at that meeting. This belief is supported by the language selected by BRAJEVICH. In particular, I believe that BRAJEVICH's request indicated his intent to "follow on" an existing discussion. Moreover, BRAJEVICH's lack of any explanation or background as to what "mediation" he meant suggests to me that BRAJEVICH and PETERS had recently discussed this topic. Finally, I note the fact that his text message identifies two separate but related issues, likely from the meeting: (1) the "sideshow" and (2) "also" the location of the "mediation."

56. PETERS proffered that in one of his multiple conversations with FEUER about the Salgueiro situation, FEUER questioned whether KIESEL should be fired for allowing this to happen, but FEUER ultimately did not decide to terminate KIESEL or PARADIS.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

57. PETERS proffered that in one of his multiple conversations with FEUER about the Salgueiro situation before the settlement, PETERS believed that he conveyed to FEUER that Salgueiro was "looking for seven figures," meaning that Salgueiro was demanding a million dollars or more.

e. *Settlement of Salgueiro's demands on December 4, 2017*

58. Information from multiple witnesses and documents indicate that on December 4, 2017, Salgueiro made good on her above-described threat to appear at a court hearing in the PwC matter and attempted to provide copies of the Salgueiro documents both to the court and to the counsel for PwC. The evidence provides probable cause to believe that after Salgueiro showed up in court and attempted to provide her documents to the court and PwC's counsel in the presence of PETERS, PETERS directed KIESEL to settle with Salgueiro and was later informed that KIESEL had done so by paying $800,000 in hush money.

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

[redacted]

62. PETERS, KIESEL, and PARADIS each (separately) advised the government substantively as follows:

a. PETERS, KIESEL, and PARADIS all attended the aforementioned *PwC* hearing in the LADWP billing litigation.[24]

b. At or after the hearing, Salgueiro approached [redacted], which PETERS, KIESEL, and PARADIS interpreted as a signal that Salgueiro was prepared to carry out her threat to reveal her information.

---

[23] [redacted] confirmed to the government that the described incident took place (he was not certain of the hearing date but believed it to be in that general time frame).

[24] PARADIS proffered that PETERS told him that he was attending the hearing at the express direction of FEUER. PETERS proffered that he told FEUER that he would attend the hearing, because he knew that FEUER would have wanted him to do so, and would have asked him to do so had he not preemptively volunteered.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

c. PETERS, KIESEL, and PARADIS reconvened in PETERS's office after the hearing, and they agreed that KIESEL would met with Salgueiro for the purpose of doing whatever he needed to do to resolve the situation and ensure that she did not reveal her information.

d. KIESEL met with Salgueiro later that day and agreed to pay her $800,000 in exchange for the return of her information and her assent to a confidentiality agreement.

63. Text messages between PETERS and KIESEL reflect the following exchange from December 4, 2017, with times indicated in brackets:

> KIESEL: I am parked on the north west corner of 1st and Los Angeles Street. [12:13 p.m.]
>
> PETERS: I'm with Paradis. Can u come to my office now to meet? [3:06 p.m.]
>
> KIESEL. Yes. [redacted] is at the elevator engaging J [Salgueiro] so [redacted] and I are stuck. Will come down as soon as we can. [3:07 p.m.]
>
> PETERS: She gave [redacted] her card. [3:09 p.m.]
>
> KIESEL: You waiting for me or going back with Paul [3:09 p.m.]
>
> PETERS: Tried to file a bunch of docs. I'm with Paradis. [3:11 p.m.]
>
> KIESEL: Going back to City Hall? I will meet you there if you go with Paul. [3:12 p.m.]
>
> PETERS: Yes. My office please. I will get you parking. [3:14 p.m.]
>
> KIESEL: Thanks. [3:14 p.m.]
>
> PETERS: **Settle the case if you can! I need you to take care of this.** We are in my office. [3:40 p.m.]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

> KIESEL: On my way up now will be there in three minutes. [3:59 p.m.]
>
> KIESEL: I am meeting Julissa tonight at 7:30 PM. With [redacted] **Will get this done**. [6:09 p.m.]
>
> KIESEL: **Deal with J at 800. 450 within 7 days. Have 150 in sixty days balance by May 1.** She will work with attorney [redacted] as her counsel. **Will return all documents when completed. Oyyy** [9:15 p.m.]
>
> PETERS: **Good job. Be sure there is a confidentiality agreement of a sort that would make Marty Singer envious.** [11:43 p.m.]

64. PETERS and KIESEL both (separately) advised the government that these texts corroborate the above-described information that PETERS attended this hearing in the LADWP billing litigation; that Salgueiro showed up at the hearing following her threat to do so if KIESEL did not pay her; that Salgueiro's actions led to KIESEL renewing negotiations to pay Salgueiro $800,000 —— a dramatic increase from KIESEL's previous counteroffer of $60,000 —— in exchange in exchange for her silence and her assent to a confidentiality agreement; that KIESEL advised PETERS of the terms of the settlement; and that PETERS directed KIESEL to obtain a strong confidentiality agreement.

65. I believe that KIESEL's text message, "**Deal with J at 800. 450 within 7 days. Have 150 in sixty days balance by May 1,**" reflects his description to PETERS of his agreement to pay Salgueiro $800,000. This understanding is consistent with information separately provided by both PETERS and KIESEL as to their respective intents and understanding of this message.

66. I believe that PETERS's text message, "**Good job. Be sure there is a confidentiality agreement of a sort that would**

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

make Marty Singer envious," reflects PETERS's endorsement of KIESEL's decision to pay Salgueiro $800,000 to buy her silence as to the City Attorney's Office's litigation practices, and to obtain a strong and enforceable confidentiality agreement. I am aware from open-source media reports that Marty Singer is a prominent Hollywood-based attorney who is known for aggressive tactics including the use and enforcement of strong confidentiality agreements. This understanding is consistent with information separately provided by both PETERS and KIESEL as to their respective intents and understanding of this message. Moreover, based on my experience and knowledge of the investigation, the fact that the City (as conveyed by PETERS) was more concerned with the confidentiality portion of the agreement than its financial terms strongly suggests that the City's primary interest in the hush money payment was to buy Salgueiro's silence because of its potential damage to the City.

67. KIESEL and PARADIS both advised the government that after the confidential settlement agreement between KIESEL and Salgueiro was formalized, KIESEL paid Salgueiro $800,000, and PARADIS paid KIESEL $400,000.[25]

68. [redacted] participated in a voluntary interview with the prosecution team and advised as follows:

---

[25] According to PARADIS, the money that he contributed came from his own funds, and he did not inform PETERS that he had contributed to the settlement. According to PETERS, he believed, based on information later provided to him by PARADIS, that some portion of the settlement was paid by LANDSKRONER. Information from PARADIS and LANDSKRONER and review of their financial records does not indicate any such direct contribution by LANDSKRONER.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. [redacted] had no prior involvement in or knowledge of the issue before KIESEL asked him to attend the December 4, 2017 hearing and intervene with Salgueiro on KIESEL's behalf. [redacted] was aware that the hearing must have some significance to KIESEL but didn't know what it was. [redacted] understood that Salgueiro had taken some papers from KIESEL's office regarding a case, and that KIESEL wanted [redacted]'s help in getting them back. [redacted] volunteered his services and did not get anything in return.

b. At the hearing, [redacted] observed Salgueiro unsuccessfully attempt to give some papers to the court clerk.

c. Following the hearing, [redacted] saw Salgueiro approach [redacted], counsel for PwC, speak with him briefly, and take his business card.

d. [redacted] asked Salgueiro to meet with him and KIESEL over dinner, and she agreed. Salgueiro brought along her friend, Rosa (last name unknown to [redacted]). [redacted] could not recall the details of the negotiation session, but it was relatively short. KIESEL balked at paying the full amount that Salgueiro was demanding because he didn't have access to those funds at that time, and he asked if she would agree to a payment plan. [redacted] believed that they ultimately settled on approximately $800,000.

e. [redacted] knew PETERS from PETERS's tenure at KIESEL's firm, but they were not close. From the time that PETERS accepted a job with FEUER at the City Attorney's Office, it was [redacted]'s belief that PETERS intended to follow FEUER when FEUER proceeded to higher political offices after his tenure as City

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Attorney. [redacted] did not have further evidentiary support for his opinion and stated that it was just [redacted]'s belief.

f. PETERS's post-settlement report to FEUER that KIESEL had paid Salgueiro to resolve her threats and demands, and PETERS's post-settlement discussions of the situation with BRAJEVICH and CLARK

69. PETERS proffered that he did not recall reporting these events to FEUER on the day of the December 4, 2017 hearing, which PETERS described as "very unusual" given how concerned and focused FEUER was with respect to Salgueiro's threat to appear at the hearing that day if she did not receive the money she was demanding.

70. PETERS proffered that shortly after the December 4, 2017 hearing (likely on December 5, 2017, but PETERS was unsure of the exact date), PETERS met with FEUER in person, and the following took place:

a. PETERS reported to FEUER that KIESEL had "stepped up" and "reached an accommodation" with Salgueiro.

b. PETERS advised FEUER that settling the matter had "cost KIESEL a ton of money."

c. PETERS confirmed to FEUER that the City would get its documents back as the result of the settlement with Salgueiro, and that they would not be made public.

d. FEUER responded favorably, telling PETERS that this was "great" and that PETERS had done "good work" in facilitating the settlement.

e. FEUER did not ask PETERS for further details of the settlement, and PETERS did not provide them.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

71. PETERS proffered that he was "quite sure" that he would not have advised FEUER after the settlement as to the specific amount that KIESEL had paid, because FEUER would not have been interested in the dollar figure. Rather, FEUER's concern was that the threat of the documents being exposed had been mitigated.

72. PARADIS proffered that around the time of the December 4, 2017 *PwC* hearing where Salgueiro appeared in court (as described in more detail elsewhere), PETERS confirmed to PARADIS that he had in fact —— as PETERS had previously maintained —— told FEUER about Salgueiro's threats, including the nature of the material that she was threatening to reveal.[26] After PETERS confirmed that he had told FEUER about the Salgueiro threats and demands, PETERS also stated that FEUER knew about the "mediation" of her demands taking place on LADWP property, and that FEUER was "pissed" about it.

73. I believe that FEUER's reported displeasure about the use of LADWP headquarters as the venue for the mediation, as described herein, related to the fact that it linked the City to the mediation of Salgueiro's demands, which would, if discovered, cast the City in a negative light.

74. PETERS proffered that at some point after KIESEL settled the matter with Salgueiro, PETERS discussed it with CLARK. PETERS advised that he did not recall the specifics of

[26] PARADIS further advised that he believed that, based on what he knew of PETERS, PETERS indeed told FEUER about the looming threat, because PETERS would not have wanted to risk FEUER being blindsided if "all hell broke loose" and Salgueiro in fact went public with her information.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

that conversation, and he did not know whether CLARK had details about the Salgueiro matter. PETERS also advised that he could not recall whether he had other conversations with CLARK about the Salgueiro matter.

75. PETERS proffered that at some point after KIESEL settled with Salgueiro, PETERS and BRAJEVICH spoke again about the matter.

3. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

[redacted]

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

[redacted]

79. Based on the foregoing, I believe there is probable cause to believe that FEUER was in fact aware of Salgueiro's threats to reveal information about the City Attorney's Office's litigation practices unless she were paid for her silence, [redacted] Specifically, my belief is based on:

a. PETERS's proffered information that he advised FEUER about the details and context of Salgueiro's threats and demands, that FEUER was very upset and contemplated firing Special Counsel, and that FEUER expressed to PETERS that KIESEL needed to take care of the matter, which PETERS understood to mean that FEUER wanted him to make sure that KIESEL paid Salgueiro to ensure that the information was not revealed.

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. PARADIS's information that at their meeting on November 17, 2017, PETERS told him that he had notified FEUER of Salgueiro's threats, and that FEUER was very upset about the situation.

c. KIESEL's information that PETERS would fire him if he did not settle with Salgueiro, and that he believed PETERS would likely have discussed the matter with FEUER before making such a threat.

d. KIESEL's contemporaneous diary entry corroborating the information provided by both KIESEL and PARADIS that PETERS had threatened to fire KIESEL if he did not settle with Salgueiro.

e. The December 1, 2017 text message from PETERS to PARADIS stating, "Mike is not firing anyone at this point. But he is far from happy about the prospect of a sideshow. Also, mediating Paul [KIESEL]'s matter at DWP, not a popular move." In addition to PETERS's explanation that this message meant that FEUER had considered but rejected the idea of firing Special Counsel, and that he was displeased about the matter, I believe that this message corroborates the substantively consistent information from PETERS, PARADIS, and KIESEL, and from KIESEL's diary entry, as described above.

f. The December 1, 2017 text message from BRAJEVICH to PETERS asking to discuss "the fact that the mediation took place at DWP," the timing of that message contemporaneous to the above-described message from PETERS to PARADIS relating FEUER's displeasure with the situation and the fact that using LADWP as

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a venue for the mediation was "not a popular move," and BRAJEVICH's relationship with FEUER.

g. PETERS's proffered information that FEUER was aware that the "mediation" had taken place at LADWP, and that FEUER was displeased with that fact.

h. PARADIS's proffered information that PETERS had informed him that FEUER knew that the "mediation" of Salgueiro's demands had taken place on LADWP property, and that FEUER was "pissed" about it.

i. PETERS's proffered information that he discussed the matter with FEUER again after the settlement and advised that KIESEL had "stepped up" and settled the matter with Salgueiro, and that the resolution had "cost KIESEL a ton of money."

j. PARADIS's proffered information that shortly after KIESEL reached a settlement with Salgueiro on December 4, 2017, by agreeing to pay her $800,000, PETERS confirmed to PARADIS that PETERS had in fact told FEUER about Salgueiro's threats, including the nature of the material that she was threatening to reveal.

80. I believe that the above information, taken together, constitutes probable cause to believe that [redacted] FEUER not only was aware of Salgueiro's threats and demands, but he impliedly directed PETERS to ensure that KIESEL settled those demands by paying a large sum of hush money.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

B. There Is Probable Cause To Believe That FEUER Obstructed Justice By Giving Misleading [redacted] Statements Indicating That He First Learned In April 2019 About Documents Indicating the Special Counsel's Work On Behalf Of The Jones Plaintiff

81. As further described below, the evidence provides probable cause to believe that in January 2019, PETERS apprised FEUER that KIESEL and PARADIS had documents responsive to PwC's court-authorized discovery demand that would be damaging to the City. Specifically, according to multiple sources of evidence — — including a contemporaneous recorded conversation wherein PETERS recounted his recent conversations with FEUER —— PETERS told FEUER that the documents would reflect previously undisclosed coordination between Special Counsel and Jones's counsel, JACK LANDSKRONER, in filing the *Jones v. City* complaint, including potentially the fact that Special Counsel acting on behalf of the City had drafted the *Jones v. City* complaint.

82. According to PETERS, FEUER was very upset, reacted with extreme shock and dismay, and stated that the revelation of those facts would be a "catastrophe." Based on that interaction and his experience with FEUER, PETERS understood from their discussions that FEUER wanted PETERS to ensure that the documents were not produced or otherwise revealed. KIESEL and PARADIS both sent the documents to PETERS as discussed, but PETERS, at the perceived direction of FEUER, did not produce the documents to PwC or alert the state court or anyone else of their existence. Instead, PETERS, at FEUER's direction, appeared at a hearing in the *PwC* case and represented to the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

state court that "there were documents that were requested of the City through that PMQ deposition notice.[28] We will be producing those documents."

83. As further detailed below, the evidence indicates that the documents that KIESEL sent to PETERS —— which were responsive to the PMQ document demand and which FEUER and PETERS knew would be damaging to the City's litigation position and the City Attorney's Office's, specifically including FEUER's, reputation —— eventually surfaced during a review of PETERS's hard drive that was directed by Browne George, the City's outside counsel. FEUER made official statements to the prosecution team [redacted] on this topic, along with various public statements and filings and sworn civil deposition testimony. The evidence provides probable cause to believe that FEUER's [redacted] official statements to the government were knowingly misleading, in that he did not first learn of the information revealed in the KIESEL Emails in late April 2019, which is when the KIESEL Emails were independently discovered and a need arose for FEUER to publicly address it. In fact, FEUER learned of this information months earlier, namely, not later than January 2019, after which he impliedly directed their concealment. Based on my training, experience, and knowledge of this investigation, I believe FEUER had a strong incentive to personally distance

[28] In California civil litigation, a PMQ deposition requires the "person most qualified" at an entity to testify on behalf of the entity as to certain relevant facts either known to the deponent or gathered through the deponent's investigation.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

himself from any knowledge of the collusive litigation for his own political gain (or to avoid political fallout).

1. The evidence indicates that FEUER, along with KAPUR and BRAJEVICH, learned about the KIESEL Emails in January 2019

84. On the afternoon of January 23, 2019, a hearing took place in the *PwC* case. According to the transcript of the hearing, the judge overruled the City's privilege objections to documents demanded by PwC and ordered the City to submit a "person most qualified" ("PMQ") to represent the City at a deposition. The judge further expressed concerns about the City's privilege assertions and related conduct, and asked KIESEL, who was representing the City at the hearing, to "bring these matters not only to the attention of the internal affairs department, if there is such a department, but also to bring it to the attention of the City Attorney, Mike Feuer, directly."

85. On January 23, 2019, at 4:59 p.m., BRAJEVICH (using **BRAJEVICH's ACCOUNT**) sent PETERS a text message stating, "Lets talk before you speak with mike [FEUER]." BRAJEVICH and PETERS exchanged additional text messages and agreed to speak the next day.

86. At 6:52 p.m. on January 23, 2019, PETERS sent an email to FEUER at **FEUER's EMAIL**. In the email, PETERS summarized the hearing, including the judge's invocation of FEUER's name. PETERS stated that **"[Judge] Berle is now aware of communications between Paradis and Landskroner about the latter taking over Mr. Jones' contemplated case against PwC, and the fact that such representation soon evolved into *Jones v. DWP*."** PETERS further

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

noted that the court "was wondering aloud today whether the *Jones* settlement is somehow vulnerable to being reevaluated due to possible conflicts by Paradis." PETERS opined that there were no ethical lapses by the City, but that they should discuss the matter soon. PETERS suggested a meeting with just PETERS, FEUER, and KAPUR, but he offered to involve PARADIS, KIESEL, or BRAJEVICH if FEUER so desired.

87. At 7:02 p.m. on January 23, 2019, FEUER replied from **FEUER's EMAIL** with a brief email directing PETERS to set up a meeting for January 25, 2019, with PETERS, FEUER, and KAPUR. Later that evening, PETERS replied that he had done so.

88. At 7:06 p.m. on January 23, 2019, FEUER (using **FEUER's EMAIL**) again replied to PETERS's original email, stating, "Although it may be too late to fix all this, it may be a good idea to have someone from our office at the next hearing before Judge Berle." Later that evening, PETERS replied, "I'll be there."

89. On January 24, 2019, KIESEL forwarded to PETERS, TUFARO, and BRAJEVICH (at **BRAJEVICH's EMAIL**) an email from counsel for PwC regarding the City's PMQ document and production of outstanding documents. PETERS replied to all asking whether the City owed documents to PwC, and indicating that if so, it should produce them. KIESEL forwarded the email to PARADIS, who replied to all stating, "Yesterday when we met with Thom [PETERS] (with Joe B. [BRAJEVICH] on the phone), Thom directed us to research and draft a writ to be filed in the very near future." PARADIS opined that the City should await resolution

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

of the writ before proceeding with either the PMQ deposition or the document production. PETERS replied to all asking when the writ could be ready, TUFARO replied with a projected date, and PETERS replied with an acknowledgement.

90. PETERS proffered that on January 24, 2019, he met with PARADIS, and the following took place:

a. PARADIS appeared very upset about the events that were unfolding in the *PwC* case, and he told PETERS, "I'm not going to go down for this bullshit."

b. PARADIS told PETERS that not only had PARADIS aided LANDSKRONER in the drafting of the *Jones v. City* complaint, but PARADIS had in fact personally drafted both the complaint and the settlement demand letter. PARADIS further advised that "everyone" at the City knew about this, including CLARK, DAVID WRIGHT, LADWP Board President MELTON EDISES LEVINE, Assistant City Attorney Eskel Solomon, and others.

c. PETERS told PARADIS that he wanted to review the documents that would reflect these facts.

91. On January 25, 2019, at 8:03 a.m., BRAJEVICH (using the **BRAJEVICH's ACCOUNT**) left a voicemail for PETERS indicating that BRAJEVICH had sent PETERS a couple of emails relating to two declarations filed by LANDSKRONER. BRAJEVICH stated that he had concerns about the declarations, specifically; 1) in a section denying any relationships with counsel in the case, LANDSKRONER omitted reference to PARADIS; and 2) LANDSKRONER stated that he had started working on the case in November 2014, which was inconsistent with the City's timelines in connection

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

with the City's attempt to assert a "common-interest defense" privilege.[29]

92. On January 25, 2019, at 8:42 a.m., BRAJEVICH (using the **BRAJEVICH's ACCOUNT**) left another voicemail message for PETERS, which expressed BRAJEVICH's desire to have TUFARO send legal authority for their position on the common-interest privilege. BRAJEVICH opined that the City needed to identify a common-interest agreement reached between Jones and the City, and that he wasn't sure how they would do that under existing legal authority. BRAJEVICH noted that "when you're making declarations it looks like you're hiding something when you're not disclosing it." BRAJEVICH opined that he thought they would be okay because the ratepayers got 100 cents on the dollar in the *Jones* settlement, but he was concerned about "how we get through all the appearances and the sloppy ass shit."

93. On January 25, 2019, at 8:44 a.m., BRAJEVICH, using **BRAJEVICH's ACCOUNT**, sent PETERS a text message stating that BRAJEVICH had "Left you 2 voicemails on your cell when you have a chance to listen."

94. KIESEL's law partner, [redacted], advised the government that on January 25, 2019, she participated in a conference call with PETERS, KIESEL, PARADIS, and TUFARO, during which the parties discussed whether a privilege would apply to the documents sought by PwC and whether the City would take a writ. [redacted] was generally unfamiliar with the case at that

[29] I have reviewed two emails that BRAJEVICH (using **BRAJEVICH's EMAIL**) sent to PETERS on January 25, 2019, which I believe are the emails referenced here.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

time. She recalled that during this discussion, PETERS appeared inclined to take a writ, but that PETERS said that he was going to discuss the matter with FEUER. [redacted] further recalled PETERS stating that he had a scheduled meeting with FEUER that evening (Friday, January 25), and that PETERS was not looking forward to giving FEUER bad news on a Friday evening.

a. An electronic calendar entry showed that on January 25, 2019, at 12:30 p.m., KIESEL invited PETERS, BRAJEVICH (on **BRAJEVICH's EMAIL**), PARADIS, TUFARO, and [redacted] to a "Follow Up Conference Call" on January 28, 2019, at 9:30 a.m.

b. I believe that this entry scheduling a "follow up" corroborates [redacted]'s recollection that she joined a call with PETERS, KIESEL, PARADIS, and TUFARO on January 25, 2019. I further believe that the inclusion of BRAJEVICH on the invitation, paired with BRAJEVICH's inclusion on the aforementioned January 24 email chain, suggests that BRAJEVICH may also have participated in the January 25 call that [redacted] recalled.[30]

c. I further believe that a voicemail from BRAJEVICH using **BRAJEVICH's ACCOUNT** to PETERS on the morning of January 28, 2019 (described in more detail below), to touch base about their planned 9:30 a.m. conference call set for that morning, additionally supports the other evidence that BRAJEVICH was

[30] A further calendar entry indicates that KIESEL canceled the January 28 call.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

aware of the issues being discussed and planned to take place in this "follow up" call.

95. On January 25, 2019, PETERS took part in a phone call with KIESEL, PARADIS, and TUFARO. [redacted] surreptitiously recorded a portion of the call and later provided the recording to the government.[31] I have reviewed the transcript, which reflects PETERS, PARADIS, and TUFARO discussing matters including: 1) the fact that the City had not disclosed the City's coordination with LANDSKRONER in drafting and filing the complaint, 2) their view that the City had not had an obligation to disclose it in the past, 3) whether or not to disclose it now, and 4) the possible reactions of the court to such a disclosure. PETERS opined that this was an "optical" problem, but stated that as a legal matter, he did not believe the City had done anything wrong.

96. FEUER's daily schedule, which was emailed to PETERS, indicates a scheduled meeting on Friday, January 25, 2019, from 4:30 p.m. to 5:00 p.m., between FEUER, KAPUR, and PETERS.

97. PETERS proffered that on either January 25, 2019, or January 28, 2019, PETERS attended a meeting with FEUER and KAPUR to discuss PwC's court-authorized demand for documents related

---

[redacted]

The metadata from the recording [redacted] suggests that this recording was saved at 11:24 a.m. PST on January 25, 2019. It is unclear to me whether this is part of the same call that [redacted] participated in. [redacted] indicated that she did not speak during that call.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to the City's upcoming PMQ deposition. According to PETERS, the following occurred at that meeting:

a. PETERS advised that there were documents in KIESEL's and PARADIS' possession that would be damaging to the City.

b. PETERS told FEUER that he did not at that time know precisely what the documents contained, but that he believed they would show coordination between KIESEL/PARADIS and LANDSKRONER before the *Jones v. City* complaint was filed.

c. PETERS told FEUER that he anticipated that the documents would show the City providing existing complaints to KIESEL/PARADIS to aid their drafting of the *Jones v. City* complaint.

d. PETERS further stated that the documents would likely show that PARADIS drafted the *Jones v. City* complaint and the settlement demand letter.

e. FEUER's reaction was like nothing PETERS had seen before. FEUER was highly emotional and visibly upset, covering his face with his hands for a long period. FEUER repeated multiple times that this "can't be so." FEUER stated that this would be "catastrophic," which PETERS understood to reference the anticipated effect that disclosure of these facts would have on the *Jones* settlement and the reputation of FEUER's office.

f. PETERS told FEUER not to "panic," and told FEUER that he (PETERS) would look into the situation.

g. FEUER did not at any time ask to see the documents that PETERS had described, nor did he ever ask PETERS

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to obtain them, review them, or show them to FEUER or anyone else.

h. FEUER and PETERS discussed the next hearing before Judge Berle, which was set to occur the following Wednesday, January 30, 2019, in the *Jones* case. FEUER and PETERS agreed that they (officials from the City, not Special Counsel) needed to convey to Judge Berle the message that he had the attention of the City Attorney's Office, and that the City Attorney's Office would not tolerate any unethical conduct.

i. FEUER directed PETERS to draft, over the weekend, a script bearing this message, which PETERS would deliver in person at the *Jones* hearing the following Wednesday.

98. On Saturday, January 26, 2019, in a series of text messages that I have reviewed, PETERS asked KIESEL to set up a call for the next day. KIESEL agreed and asked, "Will Mike [FEUER] give us clearance for disclosure of documents and full disclosure on questions?" PETERS did not reply to that inquiry, and they set a call for 2:00 p.m. the following day with them and PARADIS.

99. On Saturday, January 26, 2019, in a series of text messages that I have reviewed, KIESEL asked PARADIS to participate in a call with PETERS the next day at 2:00 p.m. PARADIS agreed and asked whether KIESEL had "anything to report now." KIESEL replied that PETERS had left a message that FEUER had reached a decision on another issue, but KIESEL stated that PETERS "said nothing about the documents or objections."

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. Based on the context of the above two text exchanges and my knowledge of the investigation, I understand that KIESEL indicated that PETERS had not yet advised whether FEUER would authorize them to disclose the potentially damaging documents that PwC was demanding.

100. On January 27, 2019, at approximately 2:20 p.m. PST, PETERS, KIESEL, PARADIS, and TUFARO participated in a telephone call. [redacted] surreptitiously recorded a part of the conversation and later provided the recording and a draft transcript to the government.[32] The recording contains the following relevant portions:

> PETERS: Okay. **Here's what I would like to do though, at Mike's request. He said to me, "What are the very, very worst documents out there that we've created that would most likely lead to embarrassment** or serve as a basis for somebody's… or Jamie Court's allegations that there was, that there was some conflict… anything from the pinnacle or standpoint of ethics." . . .
>
> Now, I said to him "Ya know, Mike, I don't really know," and he kinda chided me for not knowing and that's a fair criticism from where I stand. **I said, "although it's not teed up yet, there's a probably greater than 50 percent likelihood that eventually it will be revealed that we drafted for Landskroner a draft complaint." Now, at first, there was a great gnashing of teeth.**
>
> . . .
>
> PETERS: But this is, **Mike is aware that this could get ugly for a while**. But he wants to let us get in there and tear off the band-aids because once you get beneath the smoke, you know, you'll see that there really is ultimately, no ethical fire.
>
> . . .

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

PETERS: And all of the story is going to be told through these emails? Right, Paul?

PARADIS: Yes. Yes.

KIESEL: Yes. And by the way, **there are emails with the City of L.A., discussing -- knowing we were doing this and encouraging us to do this quickly.**

PETERS: **Okay.**

. . .

KIESEL: And then, Tommy, the only other piece, at least on the emails I saw, was Michael Libman, who was gonna to be filing the Jones versus DWP complaint reached out to me. He was in trial, and he said, "Paul, I need the money to file the Jones action." And I said, maybe something like, "We'll take care of it." And Paul Paradis was copied on it. And Paul wrote back and said, “no Landskroner is picking up all costs, all expenses. It’s on Landskroner.” And Landskroner obviously paid for the filing of the complaint.

PETERS: **I will want to read that one** because that one, **because optically, someone is going to optically scratch their head on**. So, I'll know about that one. Yeah, so if you could **send those things to me so I can get through 'em before Wednesday morning**, that would make me more comfortable. **It's just what’s the universe of shit that’s going to happen. I can give a heads up to Mike.**

. . .

KIESEL: Well, let me just add that I am feeling a whole lot better after this conversation than I had been for the last 48 hours. This has been a difficult situation.

PETERS: What were you expecting? What were you figuring that Mike was gonna ask us to do?

KIESEL: **I was figuring that Mike was not gonna release the documents at all** but Mike wanted to take a writ on the objections and we were just gonna make this thing so much worse than it is, in the end. So, I’m thrilled that we’re getting transparency. Light is what will disinfect the situation, nothing more.

PETERS: Yep.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

101. Based on the context of the messages and my knowledge of the investigation, I believe the parties' references to "Mike" throughout the January 27 conversation refer to FEUER. I further believe that the reference to "Jamie Court" refers to the president of an organization called Consumer Watchdog, which has, according to open-source media reports and other information revealed during the investigation, raised public allegations of corruption and ethical violations by City Attorney's Office and LADWP regarding the billing system litigation.

102. PETERS proffered that he participated in a phone call with KIESEL and PARADIS on January 27, 2019, and provided the following information relevant to that call:

a. PETERS told KIESEL and PARADIS that he wanted to see the documents.

b. KIESEL asked whether FEUER would allow them to produce the documents, and PETERS stated that "I will take a look."

c. KIESEL "seemed resigned" to the fact that the documents would be produced. By contract, PARADIS was more reluctant and concerned about the possibility of production.

103. PETERS proffered that, at some point during this time period, he conveyed to KIESEL and PARADIS that FEUER was "not interested in producing these documents."[33]

[33] I recognize that this information is inconsistent with other evidence described herein and, if true, would appear to represent a change in direction from the discussion reflected in the aforementioned partially recorded call on January 27, 2019.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

104. On the morning of Monday, January 28, 2019, at 9:08 a.m., BRAJEVICH (using **BRAJEVICH's ACCOUNT**) left a voicemail for PETERS. BRAJEVICH stated that he was calling to touch base with PETERS before "the 9:30 call," which BRAJEVICH planned to take from the road.[34]

105. PETERS proffered that over the weekend of January 26-27, 2019, as directed by FEUER, PETERS drafted a written script to read in court at the January 30 *Jones* hearing

106. PETERS further proffered that the following took place at and between a series of meetings with FEUER and KAPUR early in the week of January 28, 2019:

a. In preparation for the January 30, 2019 hearing in the *Jones* case, PETERS and FEUER worked together to hone the written script that PETERS was instructed to read aloud in court.

b. To the best of PETERS' recollection, PETERS drafted his statement by hand on a yellow pad and delivered it orally to FEUER at FEUER's direction. FEUER then critiqued PETERS's performance and directed him to make various changes. According to PETERS, FEUER's changes were of the "micromanagerial" variety and included instructing PETERS to refrain from using a definitive article.

---

[34] As noted above, I believe that this referenced 9:30 a.m. conference call was a scheduled call that KIESEL had invited PETERS, BRAJEVICH, PARADIS, TUFARO, and [redacted] (via an electronic calendar invitation that I have seen) to join at that time. A further email from KIESEL at 9:24 a.m. on January 28, 2019, indicates that this call was cancelled a few minutes before it was to take place.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

c. FEUER had never required PETERS to do anything like this before. PETERS was embarrassed about being required, as a division chief, to deliver a mock presentation to the City Attorney.

d. In addition to FEUER and KAPUR, PETERS recalled that Wilcox was present for at least one of the mock presentations. PETERS further believed (but was uncertain) that BRAJEVICH may have been present.

107. An electronic calendar entry sent by Google calendar on behalf of FEUER at **FEUER's EMAIL** to PETERS and KAPUR at **KAPUR's EMAIL** indicates a scheduled meeting between FEUER, KAPUR, and PETERS on Monday, January 28, 2019, from 2:30 p.m. to 3:30 p.m (two days before the scheduled hearing on the documents).

108. On the evening of Monday, January 28, 2019, BRAJEVICH left a voicemail for PETERS. BRAJEVICH reported that he had a good meeting with Maribeth [Annaguey], and noted that he and PETERS were "on for 11:00 tomorrow." BRAJEVICH said that he told "them" that if there were "any particular buzz words" that PETERS should say when PETERS was "down there on Wednesday" [January 30, 2019], to give them to PETERS tomorrow.

a. I believe that BRAJEVICH's reference to buzz words that PETERS was supposed to say on January 30, 2019, indicates BRAJEVICH's awareness that PETERS was receiving direction from others about what to say at the January 30 hearing.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

109. FEUER's daily schedule, which was emailed to PETERS, indicates a scheduled meeting on Tuesday, January 29, 2019 (one day before the hearing), from 10:30 a.m. to 11:00 a.m., between FEUER, KAPUR, and PETERS.

110. I have reviewed a January 29, 2019 email from PARADIS to PETERS and TUFARO attaching a .pdf file. The attached .pdf files contained email correspondence reflecting PARADIS's and KIESEL's coordination with LANDSKRONER in drafting and filing the *Jones v. City* complaint.[35] In an email on January 30, 2019, PETERS replied to confirm receipt.

111. Both KIESEL and [redacted] advised the government that early in the week of January 28, 2019, KIESEL asked [redacted] to gather emails responsive to PwC's document request related to the City's PMQ deposition, that [redacted] worked with KIESEL's technical staff to do so, and that on January 30, 2019, [redacted] sent an email to PETERS and PARADIS with a Dropbox link to a .pst[36] file containing the emails from KIESEL's system that [redacted] found to be responsive.

---

[35] To my knowledge, these files from PARADIS, which I have reviewed, have not been revealed or produced by the City. I do not know whether they were recovered in the City's forensic examination of PETERS's computer (described below) or why they were not included in the City's below-described April 2019 filing revealing the KIESEL Emails.

[36] In computing, a Personal Storage Table (".pst") is an open proprietary file format used to store copies of messages, calendar events, and other items within Microsoft software such as Microsoft Exchange Client, Windows Messaging, and Microsoft Outlook.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. I have reviewed this email from [redacted] to PETERS and PARADIS dated January 30, 2019, with a Dropbox link to a .pst file labeled "Emails Responsive to PMQ."

112. PETERS proffered as follows:

a. PETERS received the documents from both PARADIS and KIESEL on approximately January 29, 2019.

b. Believing that FEUER did not want the documents to come to light, PETERS did not tell FEUER that he had received these documents from PARADIS and KIESEL.

c. FEUER did not ask about the documents after the late-January meeting wherein PETERS told FEUER what he expected the documents to show, and PETERS understood that FEUER did not want him to produce the emails.

d. During this time period, on a date that he did not recall, PETERS informed KIESEL and PARADIS that "Mike has decided not to produce the documents," which PETERS believed to be FEUER's implicit directive to PETERS.

113. On the morning of January 30, 2019, PETERS appeared in court at the *Jones* hearing, as directed by FEUER. At the hearing, PETERS made the following statement (related in pertinent part), which was in substance the statement that FEUER had "flyspecked" and instructed him to make:

> My name is Tom Peters, and I'm appearing personally in this matter for the first time based on the court's request in the related case that the City Attorney be asked to review the status of these matters. That is being done, but I do want to make sure that you understand our commitment to assuring the court that . . . . This court needs to feel completely comfortable and at ease that its confidence in this settlement in justified. There are a few things I think we can do

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to advance that goal. Look, from the summer of 2014, if not earlier, the Department of Water and Power knew there was a huge problem with the Customer Care and Billing System. We still have a dispute, as to this day, as to whether it was PwC's fault or DWP's. That's the related litigation.

Look, fundamentally, with respect to this lawsuit, the Jones, et al., ratepayer class actions, there was a shared objective between the Department and the ratepayers from the get-go to give them 100 percent on the dollar refund of every dollar that had been overbilled, not 99 percent or 98 percent, but, Your Honor, also we couldn't pay 101 or 102 percent. That's a gift of public funds. **So through arm's length negotiations, that goal was ultimately achieved** as was the interrelated goal of getting a meaningful, durable, thorough process underway to make sure that the Customer Care and Billing System was repaired such that there was not a repeat, and we're obviously still grappling with that problem to this day. **But to the extent that anybody continues to be concerned at a lack of arm's length negotiation, I have some proposals**, and I think hopefully everybody will think are good ideas. One is the City suggested that we have a deposition of retired federal judge Dikran Tevrizian who presided over the multiple mediation sessions we had because he's the one person who, better than anyone else, would know the nature of the negotiations. The City certainly doesn't object to that.

To the extent that people are concerned about how the remediation or the refund is going, the City would certainly not object to deposition of Mr. Bender or Ms. Barbara Berkovich I think is her name, who is the special master who knows about the appellate process. The court has asked that she give her report at the end of this. If anybody's curious on how things stand today, then they should do it. I should also report to the court that in the related case, the City is not going to take any sort of a writ related to the recent litigation related to the PMQ depo notices.[37]

---

[37] From review of the transcripts and related materials, I understand this as a reference to the court's order that the City submit a PMQ witness for a deposition and produce related documents, which was issued over the City's objection. I also understand that the documents discussed between PETERS and FEUER, sent to PETERS by KIESEL and PARADIS, and withheld by PETERS at FEUER's implied direction were arguably responsive to this PMQ notice.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

> **As the court will recall, there were documents that were requested of the City through that PMQ deposition notice. We will be producing those documents.** We will be producing, also, the Chief Deputy of the office, Jim Clark, coincidentally a partner until about six years ago of the Gibson firm which is defending PwC. He will respond, I think, to all of the categories of inquiry set forth in that notice.

a. Following this statement by PETERS, the court commented as follows:

> I think that matter [of the discovery issues raised in the *PwC* case], it seems to be viewed seriously, which I think is important, and **I hear your words about cooperation with the discovery that will be coming along.**

b. PETERS replied as follows:

> Yeah. **We should all be assured that the City Attorney's commitment to always practicing with the highest ethical standards in mind has indeed been advanced, and I think that once the totality is understood, everyone will conclude that that is precisely what has happened here**.

c. Based on my knowledge of the investigation, I believe that by directing PETERS to make this prepared statement, FEUER intended for the court, the parties, and PwC to believe that the City would no longer fight production of all materials responsive to PwC's PMQ notice, and that it would comply with the order to produce that discovery.

114. On January 30, 2019, at 11:28 a.m., PETERS sent an email to FEUER at **FEUER's EMAIL** and KAPUR at **KAPUR's EMAIL** with the subject line "Things went well in court this morning." In the three-paragraph email, PETERS summarized that morning's hearing in the *Jones* case, including the following:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. PETERS opined that he had expressed his thoughts well with a "non-apologetic" tone, and that the judge had responded well.

b. PETERS stated that the court indicated that the propriety of the settlement was not being questioned, and that the only issue was whether there was a conflict.

c. PETERS stated, "Because we believe that our team's ethics will be vindicated once all of the facts concerning the interaction with Jones/Landskroner are revealed and understood, I am anxious to get those facts out as soon as possible and have yet again expressed such to the Pauls [KIESEL and PARADIS], who agree."

d. "[O]ur purpose for the day appears to have been fulfilled. Now on to the implementation of our plan, where I will be working carefully to see that things go as smoothly as possible."

e. PETERS asked FEUER to advise whether PETERS should come to FEUER's office to discuss further.

115. Seventeen minutes later, using **FEUER's EMAIL**, FEUER replied to all, "Thank you so much, Thom. Deeply appreciated. I would be grateful for a few more minutes with you today on this point, but no emergency. Mike."

116. At 12:56 p.m. on January 30, KAPUR (using **KAPUR's ACCOUNT**) replied to just PETERS as follows: "Thom – glad to hear it went well – I know a big relief to you (and Mike) as it sounds that you were successful of starting to turn the course of the ship –- not an easy thing to do!"

117. PETERS proffered that soon after the January 30 hearing, and after PETERS sent the aforementioned email to FEUER and KAPUR reporting that the hearing had gone well, FEUER came down to PETERS's office, which was on a different floor, and the following events took place:

a. FEUER and PETERS did not have a meeting scheduled; rather, FEUER was dropping by unannounced.

b. FEUER left his security detail outside PETERS's office and shut the door.

c. FEUER expressed that he was very thankful that things had gone well at the hearing, and that PETERS had stuck to the script and delivered their message to FEUER's satisfaction.

d. FEUER stated that he was pleased that Maribeth Annaguey, the City's outside counsel, had given PETERS's performance a positive review.

e. FEUER was very effusive in his praise of PETERS and in expressing his gratitude.

f. FEUER apologized if he had offended PETERS for "treating him like a first-year associate" and requiring him to deliver mock performances in FEUER's office.

g. FEUER came around to PETERS's side of the desk and stood behind PETERS. FEUER "laid hands on" PETERS by placing both hands on PETERS's shoulders in a friendly and intimate gesture.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

h. During the conversation, FEUER stated words to the effect that, "I've got your back," and "I've always taken care of you."

i. During this interaction, PETERS told FEUER words to the effect that, "By the way, you don't need to worry about those documents." FEUER replied with words to the effect that this was "great, wonderful. I appreciate it."

j. FEUER did not ask what documents PETERS was talking about, nor did he ask what PETERS meant. At no time did FEUER ever ask to see the documents, or ask whether PETERS had seen them or what they had revealed.

k. FEUER's unannounced visit to PETERS's office lasted approximately 10-15 minutes.

l. The interaction was unusual, and it was very significant to PETERS. PETERS interpreted it as confirmation that he had done the right thing in withholding the documents, because he had correctly intuited that FEUER did not want him to do so.

103. PETERS proffered that during this time period, BRAJEVICH was involved in discussions relating to the City's strategy for shielding from production the documents sought by PWC in its PMQ discovery demand.

104. I believe the evidence, including the above-described proffer information, voicemails, emails, and meeting invitations to or from BRAJEVICH, combined with BRAJEVICH's engaged role in this high-profile lawsuit involving LADWP, provides probable cause to believe that BRAJEVICH was involved in substantive

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Case 2:24-cv-01650-SB Document 28 Filed 06/07/24 Page 1103 of 1425 Page ID #:2309

Case 2:24-cv-01650-SB Document 28 Filed 06/07/24 Page 1104 of 1425 Page ID #:2310

ii. In a reply to a question as to why one of the existing class counsel was not recommended to Jones, CLARK testified as follows: "My understanding, and this is mostly from outside counsel, the Liner [law firm] people, who have been trying to deal with [the plaintiffs' lawyers for the existing class actions], that they were just intransigent, couldn't —— they wouldn't —— didn't want to negotiate or propose things that were not —— were not acceptable. And I don't know if they were willing to do what DWP wanted, which was basically —— there would have been overcharge repaid and have the —— and have oversight of the system to correct it." The City's errata changed CLARK's answer to, "I don't know what Mr. Paradis recommended to Mr. Jones."

iii. At his deposition, CLARK was asked the following question: "No one brought Mr. Landskroner into the case because he was viewed as someone who would be the most zealous advocate available for Mr. Jones to pursue claims; correct?" CLARK replied, "That's —— that's right." In his errata, the City changed CLARK's reply to, "I don't know why Mr. Paradis recommended him to Mr. Jones."

d. On or about March 6, 2019, shortly after LANDSKRONER invoked the Fifth Amendment in court in response to questions by the judge about whether any of his attorney's fees had been paid to PARADIS and the Special Counsels' representation of Jones was revealed in court, the City Attorney's Office announced that both PARADIS and KIESEL had stepped down or been terminated.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

e. On or about March 22, 2019, the City Attorney's Office announced that PETERS had resigned in the wake of media requests for information about PETERS' receipt of outside counsel referral fees unrelated to the LADWP billing litigation.

3. The City's April 26, 2019 filing and press release claiming that the KIESEL Emails had just been discovered

106. On April 26, 2019, under FEUER's name and at his direction, the City filed a "Notice Re: Documents" in the *City v. PwC* case. The Notice stated that "[o]n April 24, 2019, at approximately 5:30 p.m., counsel for the City learned that a .pst file labeled "Emails Responsive to PMQ(1).pst existed on a forensically imaged hard drive."[40] The Notice went on to describe certain emails between and among PARADIS, KIESEL, LANDSKRONER, and LIBMAN indicating that PARADIS and KIESEL had prepared and filed the *Jones v. City* complaint on behalf of LANDSKRONER and LIBMAN, along with other coordination. The Notice specifically noted that "No City employee or officer sent or received any of these emails." The Notice attached some of the emails and indicated that the emails had been produced to PwC after they were discovered.[41]

[40] According to multiple sources, including FEUER, the hard drive in question had been used by PETERS and, after PETERS's resignation, was forensically imaged by an outside vendor at the direction of the Browne George law firm representing the City after PETERS resigned in late March 2019.

[41] The omnibus affidavit articulated my understanding at that time that the .pst file —— which the City's April 26, 2019 filing described as containing 131 records but attached only a fraction (approximately 29) of that number —— contained at least some of the emails among City personnel that later emerged during the *PwC* litigation notwithstanding the City's stringent efforts to shield those emails from production. This

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

107. Contemporaneous with the City's Notice, the City issued a press release that included the following statement by Rob Wilcox, spokesperson for the City Attorney's Office:

> **The emails we've just discovered reveal a reprehensible breach of ethics** by outside lawyers in whom our office placed trust. **The conduct of outside counsel now coming to light** was outrageous and inexcusable.

108. I believe that the City's filing and public statement were intended to convey that no City official or employee, to include FEUER, knew about Special Counsel's coordination with LANDSKRONER and LIBMAN in advance of the *Jones v. City* complaint until the KIESEL Emails were discovered in a forensic review of PETERS' hard drive on April 24, 2019.

---

understanding was informed in part by information provided by KIESEL, and in part by my review of the complex and dynamic factual landscape of the *Jones* and *PwC* litigation.

The prosecution team's review of the contents of the .pst file was hindered by privilege protections and technical difficulties. Only after those issues were successfully mitigated was I finally able to review the contents of the file. This was after the omnibus affidavit was filed and when I learned that it contained 145 items. Several of these, in a folder marked "Deleted Items," were email chains and attachments that reflected communications between and among City employees and officials related to the LADWP billing litigation. The file did not contain other emails to and from City personnel that the City sought to shield and that later emerged.

I do not know how the City arrived at the count of 131 records itemized in its April 2019 notice, or whether the hard drive that the FBI obtained (from the City's vendor with assistance from the City) after execution of the search warrant was in the same condition as when it was earlier reviewed by the City's outside counsel. Nor is it clear whether the City's counsel, upon reviewing the .pst file and making the representation that none of the emails were sent to or from City employees or officials, viewed the items in the folder marked "Deleted Items." The FBI continues to investigate these and other questions related to the .pst file and the hard drive, both through forensic examination and through witness interviews and other investigative means.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

4. FEUER's initial interview with the prosecution team

109. On July 22, 2019, while agents were executing the July 2019 search warrants, including at the City Attorney's Office, FEUER met with the prosecution team and requested to be interviewed immediately. The interview was recorded, and I have reviewed the transcript.

110. During that interview, FEUER advised the government as follows:

Q: Are you aware of whether anybody in your office, including special counsel or anybody else, forwarded or provided internal privy information to the Jones litigators in order to help it achieve that hierarchy?

A: I would have been horrified, and had I been cognizant of that activity, whoever provided it would not have been engaged with the City, on the staff, or outside counsel then or ever again.

Q: Why is that?

A: Because I would not have considered that ethical behavior.

Q: Have you since learned that any of that occurred?

A: What I have since learned is that, because **I've seen email traffic that emerged fairly recently, in April** that —— especially Mr. Kiesel, and it appeared, from the email traffic, Mr. Paradis, had been assisting in the filing of the Jones and DWP litigation with Plaintiff's counsel.

And to anticipate a question, **around mid to late April, something in that time frame, three months ago or so, I received a phone call** from our counsel indicating that they had found, I think, a thumb drive or something on the computer that had not been opened. There had been attempts made to open it a couple times, and they had found a way to open it. And that that drive contained emails that I just referred to. And they described the content of those emails to me at that point. Maybe early April something like that. And we agreed on that conversation —— I remember the conversation. I was

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

> on my way to an event that night. **And we agreed that information had to be immediately disclosed to the Court and to opposing counsel.**

111. In the interview, FEUER further advised the government as follows as part of a lengthy statement about KIESEL's deposition testimony that the City directed his actions on behalf of the *Jones* plaintiff who sued the City:[42]

> A: "When the —— **in April when I learned about the email exchange** and subsequent to that when there was testimony by Mr. Kiesel in deposition that our office was cognizant of that activity, it really made little sense to me."

112. During the interview, FEUER further stated as follows:

> A: **When the emails in mid to late April emerged**, I actually asked Mr. George to inquire as to whether [CLARK] knew anything about that.
>
> Q: To inquire of Mr. Clark?
>
> A: Yes. I don't remember for sure, but I believe that during that period his deposition was still forthcoming, and I wanted really to just create enough distance that Mr. Clark felt he could say whatever he thought the truth was about any of these issues.
>
> But Mr. George reported to me that he did ask Mr. Clark. He said Mr. Clark was infuriated by the **revelation of those emails**. And Mr. Clark . . . referred in passing to Mr. Kiesel has having perjured himself in his testimony with regard to whether our office was cognizant of any of these.
>
> **I asked Mr. George to ask Mr. Clark on or about April 20-something if he had any possible awareness of anything close to what was being memorialized in those emails.** To which Mr. George said Mr. Clark responded by becoming infuriated, said absolutely not, that's completely unethical, no one should ever do that. But was very – I was told was very exercised that someone he'd been working with had engaged in that behavior.
>
> . . .

[42] As FEUER's statement was not directly relevant to a pending question, no question is indicated here.

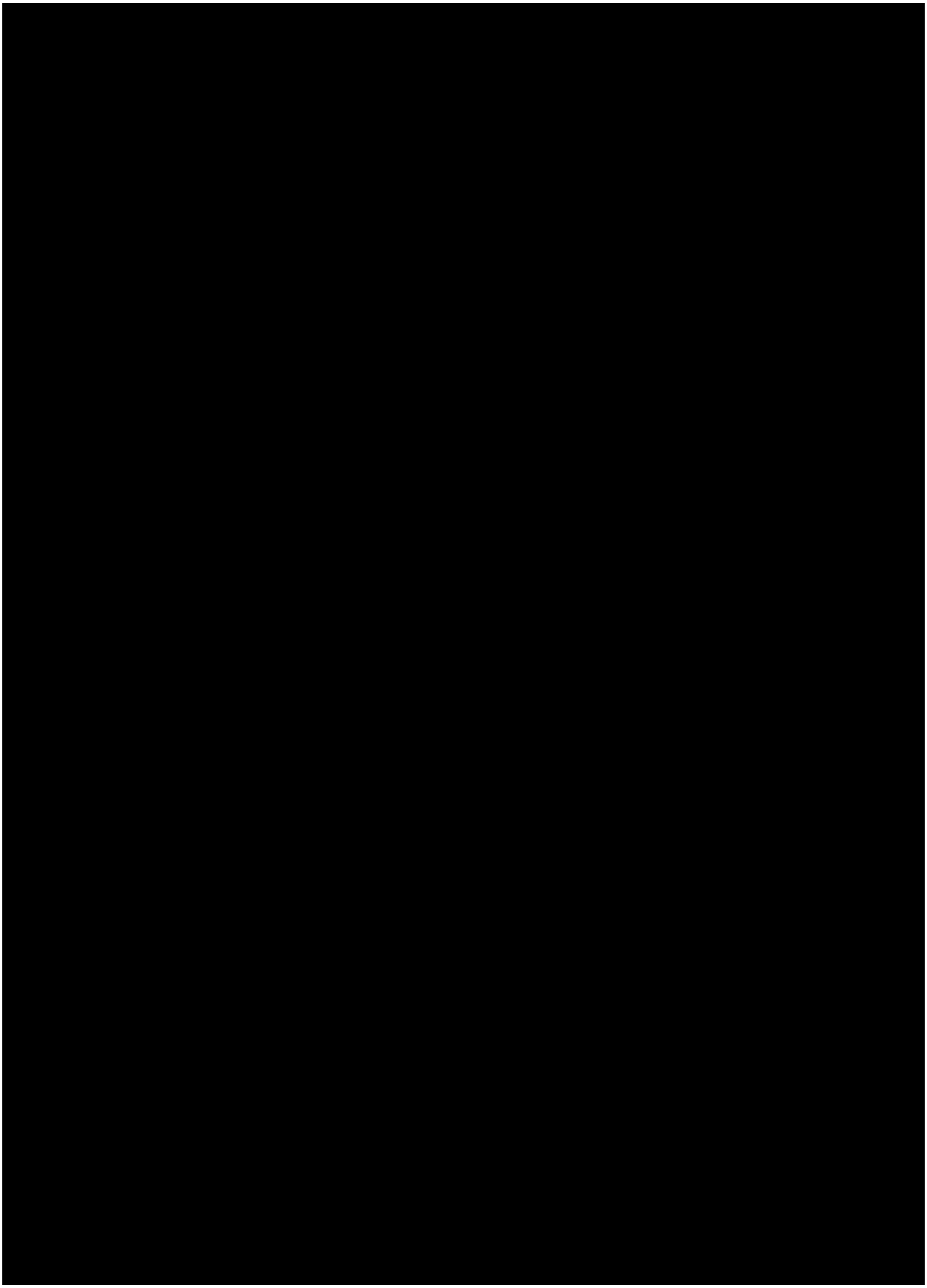
Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

> And I needed – **facts kept emerging of which I was unaware. The fact of the email, for example**, you know, what I thought we were at a stage where I thought I had a handle on what transpired, which – at that stage, with the exception of Mr. Landskroner invoking the Fifth Amendment [and] Mr. Paradis doing the same - **I thought I had a handle on exactly what had taken place here.**
>
> **And now this email exchange comes to light**.

113. I believe that in these statements, FEUER intended to convey to the government that – consistent with the City's April 26, 2019 Notice and accompanying press release - FEUER had no awareness of Special Counsel's coordination with LANDSKRONER and LIBMAN in advance of the *Jones v. City* complaint until the KIESEL Emails were discovered in a forensic review of PETERS' hard drive on April 24, 2019. I further believe that these official statements by FEUER were material and misleading, based on the below-described evidence indicating that PETERS apprised FEUER in late January 2019 of both the existence of the KIESEL Emails and the damaging information that they likely contained, after which FEUER directed PETERS to take care of the KIESEL Emails, FEUER did not follow up to find out what was in the KIESEL Emails, and FEUER did not disclose the KIESEL emails to the Court or PwC. I believe that FEUER was motivated to provide such misleading statements in order to distance himself as far as possible from the, at minimum, unethical conduct engaged in by attorneys in his office and working on behalf of his office because of the resulting political damage to his reputation and that of the City Attorney's Office.

5. [redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB



Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

[redacted]

[redacted]

116. On August 13, 2019, FEUER testified in a deposition in the *PwC* case.[44] The deposition transcript reflects that FEUER testified as follows:

> **Q: On April 26, when this filing was made, did you authorize this filing?**
>
> **A. I directed it.**
>
> Q. Mr. Wilcox also made a statement on that day to The Los Angeles Times; is that correct?
>
> A. Correct.

[44] The information in this paragraph is derived from the deposition transcript, which I have reviewed.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Q. It accused Mr. Kiesel and Mr. Paradis of a egregious breach of ethics or a reprehensible breach of ethics, if I remember correctly; is that right?

A. Yes.

Q. Nothing was said about Mr. Peters; is that correct?

A. Correct.

. . .

Q: Did you have any understanding as to why Mr. Peters did not produce "Emails Responsive to PMQ" that had been provided to him by Mr. Kiesel's office?

A: At what time?

Q: On April 26, 2019.

A: My understanding was that the —— that analysis had been done that revealed that there had not been —— that the document had not successfully been opened.

Q: Did you understand that Mr. Kiesel's office had provided an email to Mr. Peters which provided him with instructions on how to open it and indicated that the name of the file was "Emails Responsive to PMQ"?

A: No.

Q: Do you have any understanding as to how —— as to why it is that Mr. Peters says he didn't open a file called "Emails Responsive to PMQ" in preparation for a PMQ deposition that he was defending after a court order requiring the production of responsive documents?

A: No.

. . .

Q: **At the time that you learned about the documents, April 26**, did you have any concern about the fact that those documents had been identified as being responsive to the PMQ notice, that the second PMQ deposition had taken place after these documents were provided to Mr. Peters, and that Mr. Peters never produced them to PwC?

A: I wanted to know whether Mr. Peters was cognizant of the content of those documents at the time that they were transmitted to him.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

117. I believe that by this sworn testimony, FEUER intended to convey that he had no awareness of the facts that were ultimately revealed in the KIESEL Emails prior to learning about those emails shortly after his counsel discovered them on approximately April 24, 2019. I further believe that this sworn testimony was intended to convey that upon learning of the KIESEL Emails in late April 2019, FEUER immediately directed that the emails be filed with the court and produced to the defendant, and simultaneously authorized a statement condemning the conduct revealed by the emails as a "reprehensible breach of ethics." I believe that this testimony was misleading, given the evidence described herein. While false or misleading sworn testimony at a civil deposition in a state case would not, standing alone, violate federal law, it is consistent with what I perceive as FEUER's misleading or false narrative in an interview with the federal government [redacted] intended to convey that he was unaware of the KIESEL Emails until April 2019, when he immediately directed their disclosure.

6. Contacts regarding CLARK's and PETERS's depositions

118. On April 9 and April 29, 2019, CLARK provided additional testimony at his court-ordered PMQ deposition in the *PwC* case. CLARK prefaced his testimony with a prepared statement blaming poor preparation by his attorneys for what he described as his inaccurate testimony during his February 26, 2019 deposition. As noted above, I believe that his February 26

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

testimony was largely accurate, and that his subsequent errata purporting to correct critical parts of that testimony was largely inaccurate. CLARK's testimony on April 9 and April 29, 2019, was generally inconsistent with his February 26 testimony and consistent with his errata, and for the aforementioned reasons, I believe that CLARK's April 9 and April 26 testimony contained material false statements related to the collusive litigation described herein.

119. On May 1 and May 2, 2019, following his aforementioned March 2019 resignation from the City Attorney's Office, PETERS provided testimony at a court-ordered deposition in the *PwC* case. A review of PETERS' phone indicates no text messages between **CLARK's ACCOUNT** and PETERS after PETERS's March resignation until Monday, May 6, 2019. On May 6, 2019, one business day after PETERS' deposition testimony, CLARK texted PETERS from **CLARK's ACCOUNT** and asked PETERS to call him. After a series of text exchanges, the two men made an appointment for CLARK to call PETERS the following Friday afternoon using either **CLARK's ACCOUNT** or CLARK's home phone.

7. Contacts regarding KIESEL's deposition

120. On April 29, 2019, counsel for PwC contacted KIESEL and offered him an opportunity to sit for a deposition in which KIESEL could address what PwC viewed as the City's "Ro[gue] Special Counsel theory of the case, which is inconsistent with [PwC's] view of the evidence." KIESEL agreed. Before the end of May, KIESEL had agreed to be deposed in the *PwC* case.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

121. On April 30, 2019, PwC's counsel advised outside counsel for the City that PwC intended to take KIESEL's deposition in early May 2019. The City objected to that timing and invoked mediation, work-product, and attorney-client privilege objections to KIESEL's documents and testimony. After some scheduling discussions, a late May 2019 date was selected for KIESEL's deposition.

122. The City was by that time on notice that KIESEL would provide a narrative that was contrary to the City's, because by April 30, 2019 —— responding to the City's press release accusing KIESEL of a "reprehensible breach of ethics" based on what was revealed by the KIESEL Emails —— KIESEL provided the following media statement for an article published on the morning of April 30, 2019:

> I have always conducted myself with the highest level of ethics. Neither I nor my firm played any role in drafting the complaint. **This was done at the request of the city of Los Angeles.** The only thing reprehensible is the disingenuous spin coming out of the city attorney's office. **To be clear, I was completely open, direct and candid with everyone at all levels of the city attorney's office.**

123. On Friday, May 24, 2019, the business day before KIESEL was set to testify at his Tuesday, May 28, 2019 deposition,[45] CLARK called PETERS from **CLARK's ACCOUNT** and left a voicemail wherein CLARK stated that although they hadn't spoken in a few weeks, he was calling to discuss two issues, including the following: "I understand we're going to see each other on Tuesday [May 28], which I'd like to talk about."

[45] Monday, May 27, 2019, was the Memorial Day holiday.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. Based on the context and my knowledge of the investigation, and specifically the below-described information about CLARK and PETERS appearing collaboratively with the City at KIESEL's deposition the following Tuesday, I believe that CLARK was calling to discuss KIESEL's deposition and their plans for how it would be handled.

124. Later on May 24, 2019, CLARK left a subsequent voicemail for PETERS using **CLARK's ACCOUNT**. CLARK stated as follows:

> Hey Thom, it's Jim. We got cut off at a crucial point. Um. "The big question is, because" —— and then I stopped hearing you. . . . We can talk about it on Tuesday.

a. I believe this message to mean that CLARK and PETERS had been speaking on the phone, and that after PETERS said, "The big question is, because," the call was cut off.

b. Based on the timing of these two messages and my knowledge of the investigation, I believe that the conversation that got cut off at a "crucial" point, but which could be continued on Tuesday, involved KIESEL's upcoming deposition the following Tuesday.

125. In a pair of subsequent text messages between **CLARK's ACCOUNT** and PETERS's phone on May 24, 2019, CLARK and PETERS agreed to continue their discussion "on Tuesday" due to PETERS's poor cell reception.

126. On May 28, 29, and 30, 2019, KIESEL testified at a deposition in the *PwC* case. KIESEL testified to facts that were contrary to the City's narrative about the *Jones* litigation,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

including that by February 2015, members of the City Attorney's Office authorized the plan to have Jones sue the City in order to obtain a favorable settlement of all of the existing class actions. KIESEL further testified that by early March 2015, both CLARK and PETERS were aware of the plan to file the *Jones v. City* complaint, and that both CLARK and PETERS were present when the decision was made for LIBMAN to serve as local counsel to LANDSKRONER, who had already been "recruited" to take over the representation of Jones.

127. KIESEL advised the government as follows with respect to his May 2019 deposition:

a. CLARK and PETERS attended KIESEL's deposition.

b. Despite the fact that PETERS had already abruptly resigned from the City Attorney's Office by that time, PETERS did not appear adverse to the City.

c. During breaks, CLARK and PETERS would huddle together with the City's outside counsel and look at KIESEL. CLARK's face was red, and "it looked like [CLARK] was going to have a stroke." KIESEL perceived these actions as an "intimidation tactic."

128. Based on the above information and my knowledge of the investigation, I believe that CLARK used **CLARK's ACCOUNT** to contact PETERS on May 24, 2019, to discuss KIESEL's upcoming deposition testimony, which the City had reason to know would be adverse to the City and contrary to the City's false or misleading narrative regarding the collusive litigation described herein.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

129. Again, I believe all of the foregoing narrative of apparent obfuscation, false and misleading statements, and omissions are part of FEUER's campaign to distance himself as far as possible from the, at minimum, unethical conduct engaged in by attorneys in his office and working on behalf of his office because of the resulting political damage to his reputation and that of the City Attorney's Office.

C. General Proffer Information about FEUER, KAPUR, BRAJEVICH, and CLARK

60. PETERS proffered that FEUER and KAPUR were very close, and that KAPUR usually attended PETERS' meetings with FEUER. PETERS opined that KAPUR had "extraordinary loyalty" toward FEUER, and that she was "very effective in enacting FEUER's directives." PETERS recalled that FEUER's schedule required him to be out of the office a lot, and that KAPUR did not generally travel with FEUER. However, PETERS believed that FEUER and KAPUR kept in close touch throughout the day and after hours on matters important to FEUER.

61. PETERS proffered that FEUER had hired BRAJEVICH for his current position as LADWP General Counsel, and that BRAJEVICH was "very well connected" in the City Attorney's Office and in political circles in the City more generally. PETERS believed that BRAJEVICH was somewhat close to FEUER. PETERS noted that on the *PwC* case, BRAJEVICH reported directly to FEUER, in light of CLARK's recusal from that matter.

62. PARADIS proffered to the government the following relevant information regarding BRAJEVICH:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

m. At one point, PETERS told PARADIS that he had told BRAJEVICH about Salgueiro's threats, and that BRAJEVICH was upset that the mediation of her demands had taken place at LADWP. PARADIS was unsure when this conversation with BRAJEVICH took place, other than it was during November or December 2017.

n. PARADIS did not recall specifically what PETERS said he had told BRAJEVICH. PARADIS had the sense that BRAJEVICH knew everything that FEUER knew about cases involving LADWP, but he could not provide a factual basis for that understanding.

o. PARADIS observed that BRAJEVICH was obsequious toward FEUER. PARADIS further proffered that although he did not witness many interactions between BRAJEVICH and FEUER and thus could not speak to the closeness of their relationship, he observed on multiple occasions BRAJEVICH "kissing up" to KAPUR, whom PARADIS understood to be FEUER's "gatekeeper."

118. PARADIS advised that he and BRAJEVICH "tolerated each other" but did not really like each other. PARADIS further informed the government that PARADIS and FEUER "hated" each other.

a. BRAJEVICH did not like to use email and frequently asked PARADIS not to discuss sensitive things with him by email but to instead contact him by phone or text.[46]

[46] WRIGHT proffered that BRAJEVICH was very careful about using both email and text messages, because of general concerns about discoverability. WRIGHT further noted that he was not aware of any nefarious reason for BRAJEVICH's caution about written communications.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

119. DAVID WRIGHT (former LADWP General Manager) proffered that BRAJEVICH —— as an Assistant City Attorney assigned as General Counsel for LADWP —— reported to FEUER. According to WRIGHT, the role of an LADWP General Counsel was to protect the City, and as such, BRAJEVICH's loyalties lay with the City Attorney's Office rather than with LADWP in instances where their respective interests diverged.

120. CLARK proffered that he and FEUER used to be very close, with a relationship of mutual trust and respect. However, after the FBI executed a search warrant at the City Attorney's Office, and specifically in CLARK's office, CLARK perceived that FEUER kept him at a distance.

D. Summary of Probable Cause for the TARGET ACCOUNTS

130. Based on my knowledge of the investigation and the information herein, I believe there is probable cause to believe that evidence of the Target Offenses and criminal schemes may be located in the **TARGET ACCOUNTS**. In particular, BRAJEVICH's use of **BRAJEVICH'S ACCOUNT** and **BRAJEVICH's EMAIL** to contact PETERS to discuss the KIESEL Emails and issues relating to disclosure in late January 2019, as well as other matters relating to the City's strategy in responding to allegations about the collusive litigation, indicates that **BRAJEVICH's ACCOUNT** and **BRAJEVICH's EMAIL** may contain evidence of the Target Offenses and criminal schemes.[47] Moreover, BRAJEVICH's reported caution in using email

[47] On or about December 6, 2019, I served on Microsoft an order pursuant to 18 U.S.C. § 2703(d) for **BRAJEVICH's EMAIL**. Microsoft advised that the only responsive information they had

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

and preference for telephonic communications further supports the probable cause to believe that **BRAJEVICH's ACCOUNT** will contain evidence of the Target Offenses and criminal schemes.

131. I believe that FEUER's use of **FEUER's EMAIL** and KAPUR's use of **KAPUR's EMAIL** to communicate with PETERS and each other about the City's strategy for responding to allegations of unethical conduct and a court order to reveal documents that were perceived as damaging to the City constitute probable cause to believe that evidence of the Target Offenses and criminal schemes will be found on **FEUER's EMAIL** and **KAPUR's EMAIL**.

132. I believe that CLARK's above-detailed use of **CLARK's ACCOUNT** to contact PETERS about matters related to the LADWP billing litigation, including KIESEL's anticipated deposition testimony that contradicted the City's false and misleading narrative about the collusive litigation, constitutes probable cause to believe that evidence of the Target Offenses and criminal schemes will be found in **CLARK's ACCOUNT**.

133. FEUER used **FEUER's ACCOUNT** to text PETERS, including in messages related to the collusive litigation. Specifically:

---

for **BRAJEVICH's EMAIL** was profile data confirming that the account was assigned to BRAJEVICH. In follow-up conversations, Microsoft informed me that the lack of other responsive information indicated to Microsoft that other responsive data (access logs and header information) indicated that it had been deleted. Microsoft was unable to determine when or by whom the data had been deleted, nor could they advise whether there was additional content available that would be potentially responsive to a search warrant. I believe that even if Microsoft has no content for **BRAJEVICH's EMAIL**, that fact may also constitute evidence of the Target Offenses and criminal schemes, including obstruction of justice.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. On July 18, 2015, during the period in which City was mediating the allegedly preordained settlement in the *Jones* case to resolve all of the class actions on terms favorable to the City, PETERS sent FEUER a text message on **FEUER's ACCOUNT** advising FEUER of KIESEL's cell phone number (which I assume, based on context and my knowledge of the investigation, FEUER had requested from PETERS). Later that day, FEUER acknowledged the information with a text from **FEUER's ACCOUNT** reading, "Thank you."

b. On March 12, 2019, within days of KIESEL's and PARADIS's withdrawal as Special Counsel, PETERS texted FEUER on **FEUER's ACCOUNT** to advise as follows relevant to the collusive litigation and the City's correlated public-relations problems:

> "Hello. Eric George [of the Browne George law firm] has agreed to take the case and has what is, in my view, a very solid approach to [Judge] Berle's and the press's concerns. I think you will benefit from learning the particulars. Eric also has a couple of tactical thoughts which you should hear and deci[redacted] to approve. When able, please call him. [redacted]. Thank you."

i. As detailed above and in the omnibus affidavit, the Browne George law firm was involved in the City's media and public-relations strategy following the public revelation in March 2019 that PARADIS and KIESEL had represented Jones, and also in crafting FEUER's and the City's response to the discovery of the KIESEL Emails on PETERS's hard drive in April 2019. I believe that the use of **FEUER's ACCOUNT** to discuss the ongoing public-relations crisis —— which FEUER was very concerned about and which I believe, as stated above,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

caused FEUER to make the false and/or misleading statements described herein —— constitutes probable cause to believe that evidence of the Target Offenses and criminal schemes will be found on **FEUER's ACCOUNT**.

134. Moreover, the evidence shows that FEUER relied on members of his trusted inner circle —— including CLARK, KAPUR, and possibly BRAJEVICH —— and therefore, it is more likely that FEUER would have communicated with others, including **BRAJEVICH's ACCOUNT** and **CLARK's ACCOUNT,** about the facts underlying the Target Offenses and criminal schemes.

135. I believe that this evidence, coupled with other evidence -- including that articulated in the omnibus affidavit -- gives rise to probable cause to believe that the **TARGET ACCOUNTS** will contain evidence of violations of the Target Offenses and criminal schemes.

IX. BACKGROUND ON E-MAIL AND THE PROVIDERS

136. In my training and experience, I have learned that providers of e-mail and/or social media services offer a variety of online services to the public. Providers, like the PROVIDER, allow subscribers to obtain accounts like the **TARGET ACCOUNTS**. Subscribers obtain an account by registering with the provider. During the registration process, providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail or social media account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of

payment (including any credit or bank account number). Some providers also maintain a record of changes that are made to the information provided in subscriber records, such as to any other e-mail addresses or phone numbers supplied in subscriber records. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of an account.

137. Therefore, the computers of a PROVIDER are likely to contain stored electronic communications and information concerning subscribers and their use of the PROVIDER's services, such as account access information, e-mail or message transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of a SUBJECT ACCOUNT.

138. A subscriber of a PROVIDER can also store with the PROVIDER files in addition to e-mails or other messages, such as address books, contact or buddy lists, calendar data, pictures or videos (other than ones attached to e-mails), notes, and other files, on servers maintained and/or owned by the PROVIDER. In my training and experience, evidence of who was using an account may be found in such information.

139. In my training and experience, e-mail and social media providers typically retain certain transactional information about the creation and use of each account on their systems.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail and social media providers often have records of the Internet Protocol ("IP") address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a **TARGET ACCOUNT**.

140. In my training and experience, e-mail and social media account users will sometimes communicate directly with the service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers of e-mails and social media services typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of a **TARGET ACCOUNT**.

141. I know from my training and experience that the complete contents of an account may be important to establishing the actual user who has dominion and control of that account at a given time. Accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. Given the ease with which accounts may be created under aliases, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of an account, investigators often have to rely on circumstantial evidence to show that an individual was the actual user of a particular account. Only by piecing together information contained in the contents of an account may an investigator establish who the actual user of an account was. Often those pieces will come from a time period before the account was used in the criminal activity. Limiting the scope of the search would, in some instances, prevent the government from identifying the true user of the account and, in other instances, may not provide a defendant with sufficient information to identify other users of the account. Therefore, the contents of a given account, including the e-mail addresses or account identifiers and messages sent to that account, often provides important evidence regarding the actual user's dominion and control of that account. For the purpose of searching for content demonstrating the actual user(s) of a **TARGET ACCOUNT**, I am requesting a warrant requiring the PROVIDER to turn over all information

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

associated with a **TARGET ACCOUNT** with the date restriction included in Attachment B for review by the search team.

142. Relatedly, the government must be allowed to determine whether other individuals had access to a **TARGET ACCOUNT**. If the government were constrained to review only a small subsection of an account, that small subsection might give the misleading impression that only a single user had access to the account.

143. I also know based on my training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as “lol” to express “laugh out loud”), or codewords (which require entire strings or series of conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of a message or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and parenthesis :) to convey a smile or agreement) to discuss matters. “Keyword searches” would not account for any of these possibilities, so actual review of the contents of an account by law enforcement personnel with information regarding the identified criminal activity, subject to the search procedures set forth in Attachment B, is necessary to find all relevant evidence within the account.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

144. This application seeks a warrant to search all responsive records and information under the control of the PROVIDER, which is subject to the jurisdiction of this court, regardless of where the PROVIDER has chosen to store such information.

145. As set forth in Attachment B, I am requesting a warrant that permits the search team to keep the original production from the PROVIDER, under seal, until the investigation is completed and, if a case is brought, that case is completed through disposition, trial, appeal, or collateral proceeding.

a. I make that request because I believe it might be impossible for a provider to authenticate information taken from a **TARGET ACCOUNT** as its business record without the original production to examine. Even if the provider kept an original copy at the time of production (against which it could compare against the results of the search at the time of trial), the government cannot compel the provider to keep a copy for the entire pendency of the investigation and/or case. If the original production is destroyed, it may be impossible for the provider to examine a particular document found by the search team and confirm that it was a business record of the provider taken from a **TARGET ACCOUNT**.

b. I also know from my training and experience that many accounts are purged as part of the ordinary course of business by providers. For example, if an account is not accessed within a specified time period, it -- and its contents

-- may be deleted. As a consequence, there is a risk that the only record of the contents of an account might be the production that a provider makes to the government, for example, if a defendant is incarcerated and does not (perhaps cannot) access his or her account. Preserving evidence, therefore, would ensure that the government can satisfy its Brady obligations and give the defendant access to evidence that might be used in his or her defense.

X. REQUEST FOR NON-DISCLOSURE

134. Pursuant to 18 U.S.C. § 2705(b), I request that the Court enter an order commanding the PROVIDER not to notify any person, including the subscribers of the **TARGET ACCOUNTS**, of the existence of the warrant until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date the requested warrant is signed by the magistrate judge, or such later date as may be set by the Court upon application for an extension by the United States. There is reason to believe that such notification will result in: (1) flight from prosecution; (2) destruction of or tampering with evidence; (3) intimidation of potential witnesses; (4) otherwise seriously jeopardizing the investigation; or (5) exposing the identities of confidential sources who have cooperated with the government and in some cases may continue to actively and covertly cooperate.

XI. CONCLUSION

135. Based on the foregoing, I request that the Court issue the requested search warrants.

ANDREW CIVETTI, Special Agent
Federal Bureau of
Investigation

Subscribed to and sworn before
me on January 31, 2020.

HONORABLE PATRICK J. WALSH
UNITED STATES MAGISTRATE JUDGE

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

EXHIBIT 2

From: Leela Kapur <leela.kapur@lacity.org>
Received(Date): Mon, 25 Mar 2019 00:28:55 +0100
Subject: Jim's Deposition
To: Mike Feuer <mike.feuer@lacity.org>

Mike: The following are some excerpts from Jim's depo. I am paraphrasing but you will get the gist. O: indicates his original response and R: his revised. A: answers that weren't amended. Statements in quotation marks are statements Jim made (again sometimes paraphrased) but without the question attached. While I suspect much of this can be explained as the questions were less than precise, etc., I wanted you to get a feeling for the breadth of the confusing responses — many of which are not objectively clarified through documentation.

Did Mr. Tom tell you he was aware that P had an atty/client relationship with Jones?
O: I think so
R: He did not

Did P brief any (of our DWP attorneys) on nature of his representation of Jones?
O: I don't know
R: They say he did not.

Was Maribeth provided a copy of draft complaint?
O: Yes
R: No apparently not.

In talking about the Liner memo cautioning against P dual representation of City and Jones v. PWC — Did Liner provide memo to City Attorney's office?
O: I don't know.
R: Yes
O: We don't have a copy now
R: We do

"I discarded my notes last Friday. I don't need them (4-5 pages). Doesn't know and didn't ask if a retention order in place."

Inconsistent testimony as to whether he knew of the draft complaint before Thom requested it be prepared.

"I understand there were 2 draft complaints. One was sent to Jones — no City person saw it. Just learned of it but I was screened so someone else may have known of it."

Was Feuer part of decision to not file Jones v. PWC complaint?
O: I don't remember Mike taking part in that discussion. I am sure I reported it to him but don't think he was involved decision.
R: I don' think he was involved in the recommendation.

When did he (Feuer) first learn of the existence of the complaint?
A: I have no idea.

Did you apprise him (Feuer) of the fact?

A: I'm sure I did. We met twice a week. I advised him of what's going on. I have no specific recollection of advising him.

At any time did City Attorney or DWP voice concerns about propriety of P serving as counsel for Jones and City?
O: Not that I recall.
R: Yes, Richard Tom passed on outside counsel advice that shouldn't represent both against PWC.

"I am sure I heard Landskroner's (LK) name before 4/1/15." But then "learn of LK when complaint came out." But then "heard of him before that by a few days." And "When it became clear to P that PWC suit by Jones not going forward, P contacted LK, with whom he had a prior relationship based on another case and Cleveland system issues."

Did you understand at that time Jones had determined to sue LA?
A: I think we were told that.

Your understanding that before 3/26, Jones had instructed P to file against the City?
A: I don't know. P told me the he told Jones that couldn't represent him because Jones wanted to sue City not PWC.

Did P tell you he told Jones that P represented the City?
A: Sure Jones was aware. Because there two suits were contemplated. One by DWP and one by Jones.

Your understanding that 4/1/15 complaint against DWP was originally drafted by P?
A: I think he had — not sure— he had some role
A: Based on P, he prepared the earlier complaint and gave to LK.
A: (after lunch break) Clarified that he meant that P had given other class complaints to LK. No reason to believe P and role in actual drafting of the complaint against DWP. Don't know one way or the other.

Do you know if ever a time in their relationship that Jones was NOT considering potential suits against DWP?
A: I don't. P may have told me that LK would be filing against DWP.

Did any one in City Attorney's office authorize P to bring in LK for purpose of suing City?
O: I think the City was informed that once P concluded to have a conflict. I assume somebody authorized it but not me.
R: Struck last sentence.

At point P recommending LK, you personally understood reason was for LK to sue City?
O: Correct
R: Correct as to PWC, not City.

Why not refer Jones to Blood or other class plaintiff counsel?
A: They were unreasonable. Refused to toll claims. LK more reasonable, based on P.
O: Understnding from Liner that Blood et al were intransigent. Didn't want to negotiate. Were not acceptable. Didn't have same goals as DWP.

R: I don't know why P recommended to Jones.

No one brought LK into case because viewed as someone who would be most zealous advocate for Jones?
O: That's right
R: Don't know why P recommended him.

"Sure we knew before 4/1/15 that Jones would be filing against City."

Did you know there would be an immediate settlement request?
A: We were trying to settle. I think I knew.

Some questions about a meeting or phone call between Feuer, Blood and Clark. Jim doesn't remember it.

"P provided LK other complaints for purpose of making easier for LK to draft complaint covering all causes of action."

When asked about City's knowledge of LK's actual hours worked, Jim stated we agreed to the fees without seeing hours claimed.

How much earlier than 4/1/15 did you know the settlement demand would be forthcoming at some point and you would be settling with Jones?
O: Sometime letter half to end of March.
R: I didn't

P was involved in remediation before filing of Jones complaint?
O: I think that is right
R: No

He was asked why P participated in Jim's due diligence interviews as he was prepping for PMK depo (e.g., interviews with our CA staff and DWP staff). Jim didn't really answer the question.

Sent from my iPad

--
**********Confidentiality Notice **********
This
electronic message transmission contains information
from the Office of the
Los Angeles City Attorney, which may be confidential or protected by the attorney-client privilege and/or the work product doctrine. If you are not the intended recipient, be aware that any disclosure, copying, distribution
or use of the content of this information is prohibited. If you have received this communication in error, please notify us immediately by e-mail and delete the original message and any attachments without reading or saving in any manner.

****

TRACY L. WILKISON
Attorney for the United States,
Acting Under Authority Conferred By 28 U.S.C. § 515
SCOTT GARRINGER
Assistant United States Attorney
Deputy Chief, Criminal Division
MELISSA MILLS (Cal. Bar No. 248529)
FRANCES LEWIS (Cal. Bar No. 291055)
Assistant United States Attorneys
Public Corruption and Civil Rights Section
DIANA KWOK (Cal. Bar No. 246366)
Assistant United States Attorney
Environmental and Community Safety Crimes Section
1500 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-0627
Facsimile: (213) 894-2927
E-mail: Melissa.Mills@usdoj.gov

Attorneys for Applicant
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

IN RE: CELLULAR TELEPHONES	No. 2:20-MJ-3828 WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS **(UNDER SEAL)**

Upon application by the United States of America, supported by the law enforcement agent's affidavit, for a warrant relating to the following cellular telephones:

a. [redacted] a cellular telephone issued by Verizon ("Carrier 1"), subscribed to by MICHAEL FEUER and believed to be used by MICHAEL FEUER ("**Subject Telephone 1**");

b. [redacted] a cellular telephone issued by Carrier 1, subscribed to by [redacted] and believed to be used by LEELA KAPUR ("**Subject Telephone 2**"); and

c. [redacted] a cellular telephone issued by AT&T ("Carrier 2" and, together with Carrier #1, collectively referred to as the "Carriers"), subscribed to by an as-yet-unidentified person and believed to be used by JOSEPH BRAJEVICH ("**Subject Telephone 3**" and, together with **Subject Telephones 1 and 2**, collectively referred to as the "**Subject Telephones**").

THIS COURT FINDS THAT there is probable cause to believe that prospective cell-site information and GPS information likely to be received concerning the approximate location of the **Subject Telephones**, currently within, or being monitored or investigated within, the Central District of California, will constitute or yield evidence of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding) (the "Target Offenses"), being committed by MICHAEL FEUER, PAUL PARADIS, JACK LANDSKRONER, and others known and unknown (the "Target Subjects").

THIS COURT FURTHER FINDS THAT, pursuant to 18 U.S.C. § 3123, the attorney for the government has certified that the information likely to be obtained is relevant to an ongoing criminal investigation of the Target Subjects being conducted by the Federal Bureau of Investigation (the "Investigating Agency") for violations of the Target Offenses.

THIS COURT FURTHER FINDS reasonable cause exists to believe that providing immediate notification of this warrant to the user of the **Subject Telephones** may have an adverse result.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

GOOD CAUSE HAVING BEEN SHOWN, THIS COURT HEREBY ISSUES THIS WARRANT AND ORDERS THAT:

1. The Carrier shall disclose, at such intervals and times as directed by the Investigating Agency, information concerning the location (physical address) of the cell-site at call origination (for outbound calling), call termination (for incoming calls), and, if reasonably available, during the progress of a call, for the **Subject Telephones**, as well as such other information, apart from the content of any communication, that is reasonably available to the Carrier and that is requested by the Investigating Agency or any law enforcement agency working with the Investigating Agency, concerning the cell-sites/sectors receiving and transmitting signals to and from the **Subject Telephones** whether or not a call is in progress.

2. The Carrier shall disclose at such intervals and times as directed by the Investigating Agency the approximate physical location of the **Subject Telephones**, to include E-911 Phase II data and latitude and longitude data gathered for the **Subject Telephones**, including Global Positioning Satellite ("GPS") and/or network timing information, including Sprint's Per Call Measurement Data, Verizon's Real Time Tool, AT&T's Network Event Location System and T-Mobile's True Call data, and including information from such programs as Nextel Mobile Locator, Boost Mobile Loopt, Sprint/Nextel Findum Wireless, or a similar program, which will establish the approximate location of the **Subject Telephones**, and which information is acquired in the first instance by the Carrier, which will establish the approximate location of the **Subject Telephones** (referred to herein as "GPS information"), and shall furnish all information,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

facilities, and technical assistance necessary to accomplish said disclosure unobtrusively.

3. As part of the receipt of the requested GPS information, the Investigating Agency is prohibited from seizing any tangible property pursuant to this warrant, or any other prohibited wire or electronic information as stated in 18 U.S.C. § 3103a(b)(2). This warrant does not address whether the Investigating Agency may seize such property or information in relation to any other investigation authorized by law.

4. The Investigating Agency is permitted to delay service of this warrant to the subscriber(s) of the **Subject Telephones** for a period of 30 days from the date that the disclosure ends. Any requests for a continuance of this delay should be filed with this Court, unless directed to the duty United States Magistrate Judge by this Court.

5. The Investigating Agency shall make a return of this warrant to the United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office within ten calendar days after the disclosure of information ceases. With respect to prospective cell-site and other location information, the return shall state the date and time the telephone company began providing information pursuant to this warrant, and the period during which information was provided, including pursuant to any orders permitting continued disclosure.

6. The disclosure of the requested information by the Carrier shall begin during the daytime on the earlier of the day on which law enforcement officers first begin to receive information pursuant to this warrant or ten days after the date of this warrant, and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001140
Page 1140 of 1425

continue for up to 45 days from the date of this warrant unless additional orders are made continuing the period of the disclosure.

7. The disclosure of the requested information shall occur whether the **Subject Telephones** are located within this District, outside of the District, or both, and, for good cause shown, shall extend to any time of the day or night as required.

8. The disclosure of the requested information shall not only be with respect to the **Subject Telephones**, but also with respect to any additional changed telephone number(s) and/or unique identifying number, whether the changes occur consecutively or simultaneously, listed to the same wireless telephone account number as the **Subject Telephones** within the period of disclosure authorized by the warrant.

9. The Carrier shall execute the Court's warrant as soon as practicable after it is signed. If a copy of the warrant is given to the Carrier, the copy may be redacted by law enforcement to exclude the Target Subjects and any description of the offenses under investigation.

10. The Investigating Agency shall reimburse the Carrier for their reasonable expenses directly incurred by the Carrier in providing the requested information and any related technical assistance.

11. To avoid prejudice to this criminal investigation, the Carrier and its agents and employees shall not disclose to or cause a disclosure of this Court's warrant and orders, or the request for information by the Investigating Agency or other law enforcement agencies involved in the investigation, or the existence of this investigation, except as necessary to accomplish the assistance

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

hereby ordered, until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date the Carrier complies with this warrant or such later date as may be set by the Court upon application for an extension by the United States. In particular, the Carrier and its agents and employees are ordered not to make any disclosure to the lessees of the telephone or telephone subscribers. Upon expiration of this order, at least ten business days prior to disclosing the existence of the warrant, the Carrier shall notify the agent identified below of its intent to so notify:

Special Agent Andrew Civetti
Federal Bureau of Investigation
11000 Wilshire Blvd., Los Angeles, CA
310-294-0386
Acivetti@FBI.gov

12. The application, this warrant, and the return to the warrant shall remain under seal until otherwise ordered by the Court. Law enforcement is permitted to provide a copy of the warrant to the Carrier.

Patrick J. Walsh

UNITED STATES MAGISTRATE JUDGE
Hon. Patrick J. Walsh

DATE/TIME OF ISSUE: 8/14/2020 4:00 p.m.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Case 2:24-cv-01650-SB Document 28 Filed 06/03/24 Page 1143 of 1425 Page ID #:2349
Case 2:20-mj-03799-DUTY *SEALED* Filed 08/14/20 Page 1 of 164 Page ID #:199

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of:

MICHAEL "MIKE" FEUER, date of birth [redacted] 1958

Case No. 2:20-MJ-3799

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A-1

located in the Central District of California, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 371; 666; 1001; 1341; 1343; 1346; 1505; 1510; 1951; 1956; and 1621	Conspiracy; Bribery and Kickbacks Concerning Federal Funds; False Statements; Mail Fraud; Wire Fraud; Deprivation of Honest Services; Obstructing Federal Proceeding; Obstruction of Justice; Extortion; Money Laundering; and Perjury in a Federal Proceeding

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/

Applicant's signature

Andrew Civetti- FBI Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 8/14/2020

Judge's signature

City and state: Los Angeles, CA

Hon. Patrick J. Walsh, United States Magistrate Judge

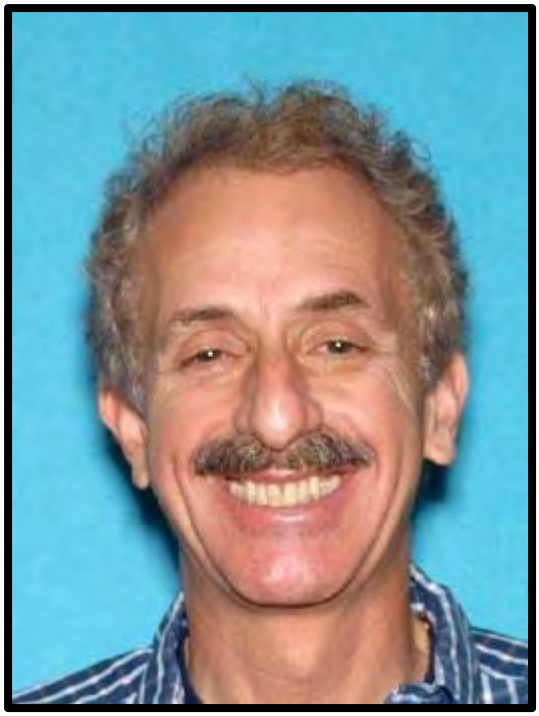
Printed name and title

AUSA: Melissa Mills

ATTACHMENT A-1

PROPERTY TO BE SEARCHED

The person to be searched is **MICHAEL "MIKE" FEUER**, date of birth [redacted] 1958, as pictured below:



Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

ATTACHMENT B

I. CELL PHONE ITEMS TO BE SEIZED

1. Law enforcement personnel are authorized to seize the cellular telephones with telephone numbers [redacted] ("**FEUER'S PHONE**"), [redacted] ("**KAPUR'S PHONE**"), and [redacted] ("**BRAJEVICH'S PHONE**") (collectively, the "**TARGET PHONES**" or the "digital devices").

2. During the execution of this search warrant, law enforcement is permitted to: (1) depress the thumb and/or fingers of **MIKE FEUER**, **LEELA KAPUR**, or **JOSEPH BRAJEVICH** onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of **FEUER, KAPUR,** or **BRAJEVICH** with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

3. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations, between November 1, 2017, and the present, of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False

Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding) (collectively, the "Subject Offenses"), namely:

a. Information as to who accessed or used the **TARGET PHONES**, including records about their identities.

b. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Retention of PAUL PARADIS and PAUL KIESEL, or entities related thereto, to represent the City of Los Angeles, and the ensuing representation;

ii. Communications involving or about any party to, or to counsel for any party to, *Jones v. City of Los Angeles* (the "*Jones* matter") or *City of Los Angeles v. PricewaterhouseCoopers* (the "*PwC* matter"), including communications regarding these matters with or referencing the persons identified in paragraphs 10-22 of Exhibit 1 to the affidavit supporting this warrant, and other counsel for and parties to these matters;

iii. The litigation of the *Jones* matter and the *PwC* matter, including discovery disputes, the deposition of the City's "person most qualified," and emails and other materials arguably or allegedly responsive to discovery demands or court orders;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

iv. Efforts to conceal the litigation practices of the City Attorney's Office's or members or representatives thereof in the litigation involving the LADWP billing system;

v. Efforts to conceal actions by the City Attorney's Office or members or representatives thereof in the litigation involving the LADWP billing system, including shielding documents from production, filing false or misleading documents with the court, and offering false or misleading testimony;

vi. The City's actions, strategy, or tactics in responding to revelations or allegations of fraud, discovery violations, and unethical conduct in the litigation involving the LADWP billing system, including media outreach and contacts, litigation decisions, and notification or lack of notification to the court of relevant developments;

vii. Negotiations or agreements to conceal business practices used in the LADWP billing litigation by the City Attorney's Office or members thereof, and communications involving or referencing the same;

viii. Destruction or concealment of evidence relevant to the LADWP billing litigation.

c. Any **TARGET PHONE** which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

d. With respect to any **TARGET PHONE** containing evidence falling within the scope of the foregoing categories of items to be seized:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

5. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

6. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

review only digital device data which has been released by the Privilege Review Team.

7. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

8. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

9. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001150
Page 1150 of 1425

by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

10. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

11. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

12. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

13. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

14. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

15. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

16. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

17. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

18. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

19. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AFFIDAVIT

I, Andrew Civetti, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since September 2015. I am currently assigned to a Public Corruption Squad, where I specialize in the investigation of corrupt public officials, including bribery, fraud against the government, extortion, money laundering, false statements, and obstruction of justice. In addition, I have received training in the investigation of public corruption and other white collar crimes.

2. The FBI and United States Attorney's Office ("USAO") are investigating alleged corrupt activities at the Los Angeles Department of Water and Power ("LADWP") and the Los Angeles City Attorney's Office ("City Attorney's Office"), ("the Federal Investigation").

3. I am aware that the City receives in excess of $10,000 annually in federal funds through various programs.

II. PURPOSE OF AFFIDAVIT

4. I make this affidavit in support of applications to seize and search the following cellular telephones:

a. Telephone number [redacted] located at the following office address, residence address, or alternatively on the person of **MICHAEL "MIKE" FEUER** ("**FEUER's PHONE**"):

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

i. **MICHAEL FEUER**, described in more detail in Attachment A-1;

ii. Los Angeles City Hall East, 200 N. Main Street, 8th Floor, Los Angeles, CA, Office of the City Attorney, identified and pictured in Attachment A-2 ("**FEUER's OFFICE**");

iii. [redacted], Los Angeles, California, identified and pictured in Attachment A-3 ("**FEUER's RESIDENCE**");

b. Telephone number [redacted] located at the following office address, residence address, or alternatively on the person of **LEELA KAPUR** ("**KAPUR's PHONE**"):

i. **LEELA KAPUR**, described in more detail in Attachment A-4;

ii. Los Angeles City Hall East, 200 N. Main Street, 8th Floor, Los Angeles, CA, Office of the Chief of Staff to the City Attorney, identified and pictured in Attachment A-5 ("**KAPUR's OFFICE**");

iii. [redacted], Toluca Lake, California, identified and pictured in Attachment A-6 ("**KAPUR's RESIDENCE**");

c. Telephone number [redacted] located at the following office address, residence address, or alternatively on the person of **JOSEPH BRAJEVICH** ("**BRAJEVICH's PHONE**"):

i. **JOSEPH BRAJEVICH**, described in more detail in Attachment A-7;

ii. Los Angeles Department of Water and Power, 221 N. Figueroa Street, 10th Floor, Los Angeles, CA, Office of

the General Counsel ("**BRAJEVICH'S OFFICE**"), identified and pictured in Attachment A-8;

iii. [redacted], Los Angeles, California, identified and pictured in Attachment A-9 ("**BRAJEVICH's RESIDENCE**").

5. In connection with the investigation into this matter, the requested search warrants seek authorization to search the respective offices, residences,[1] and persons of FEUER, KAPUR, and BRAJEVICH, described in more detail in Attachments A-1 through A-9, **FEUER's PHONE**, **KAPUR's PHONE**, and **BRAJEVICH's PHONE** (collectively, the **TARGET PHONES**, described in Attachment B), and seize any data on a **TARGET PHONE** that constitutes evidence of the criminal schemes identified herein and evidence or fruits of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding) (collectively, the "Subject Offenses"), and any **TARGET PHONE** that is itself an instrumentality of the criminal schemes and Subject Offenses, as also set forth in Attachment B. Attachments A-1 through A-9 and Attachment B are incorporated herein by reference.

[1] Based on my review of open source databases, California Department of Motor Vehicle records, and/or subscriber information for the **TARGET PHONES**, I believe the identified residences are the residences of FEUER, KAPUR, and BRAJEVICH respectively.

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, information obtained from other agents and witnesses [redacted]), consensually recorded conversations, and information obtained from the prior related search warrants, as detailed further below. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

7. On January 28, 2020, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized search warrants for the seizure of information associated with iCloud accounts belonging to FEUER and BRAJEVICH (20-MJ-396), as well as Google accounts belonging to FEUER and KAPUR (20-MJ-397) (collectively, the "January 2020 search warrants"). On September 12, 2019, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized two search warrants (19-MJ-3813 and 19-MJ-3814) for PETERS's residence and person to seize PETERS's cell phone (collectively, the "September 2019 search warrants"). On July 18, 2019, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized two search warrants (19-MJ-2915 and 19-MJ-2923) for the seizure of information associated with nineteen e-mail accounts from two Internet Service Providers, and six search warrants (19-MJ-2913, 19-MJ-2914, 19-MJ-2917, 19-MJ-2919, 19-MJ-2920, and 19-MJ-2922) for the premises of sixteen

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

locations (collectively, the "July 2019 search warrants"). All of the July 2019 search warrants were supported by my single omnibus affidavit (the "omnibus affidavit"). The January 2020, September 2019, and July 2019 search warrants and my supporting affidavits are incorporated herein by reference. A copy of my supporting affidavit to the January 2020 search warrants is attached hereto as **Exhibit 1**. Copies of the affidavits supporting the September 2019 and July 2019 search warrants can be made available for the Court upon request.

III. RELEVANT BACKGROUND ON SUBJECTS

8. **MICHAEL FEUER** is the City Attorney for the City of Los Angeles. On July 22, 2019, during the execution of a search warrant at the City Attorney's Office, FEUER provided a voluntary recorded interview, portions of which are detailed herein.[2] Thereafter, FEUER provided certain additional information to the prosecution team via telephone or in person, either directly or via his Chief of Staff, LEELA KAPUR. [redacted] FEUER has indicated to the government on multiple occasions that he had plans to run for Mayor of Los Angeles in 2022 and he believed he would be among the favorites.[4]

[2] I was not present for this interview, but I have reviewed the FBI report and corresponding transcript.

[redacted]

[4] I was present for some, but not all, of such communications. Where I was not, I learned of FEUER's statements from other government personnel who were present.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. Based on my review of Apple ID subscriber information which registered **FEUER's PHONE** ([redacted] to an Apple ID account [redacted]) utilized by FEUER, my review of subscriber records for [redacted], and FEUER's use of [redacted] as recently as July 2020 to contact the prosecution team relating to the investigation, among other evidence, I believe that FEUER uses **FEUER's PHONE**.

b. Based on my review of an iCloud back-up produced by Apple, Inc., in response to the January 2020 search warrants, I believe that while **FEUER's PHONE** was used to register the Apple ID [redacted] as described in the affidavit supporting the January 2020 warrants, FEUER did not utilize that specific Apple ID to back up **FEUER's PHONE** to the iCloud, resulting in a lack of any iCloud data for that phone.[5]

9. **LEELA KAPUR** is FEUER's Chief of Staff, a position she has held since 2013. Based on my review of a contact card in FEUER's [redacted] iCloud back-up, as well as my review of KAPUR's emails, among other evidence, I believe that KAPUR uses **KAPUR's PHONE**.

10. **JOSEPH BRAJEVICH** is an Assistant City Attorney and the General Counsel for LADWP. Based on my review of subscriber records for **BRAJEVICH's PHONE**, iCloud records produced by Apple, Inc., in response to the January 2020 search warrants, and BRAJEVICH's use of **BRAJEVICH's PHONE** to contact the prosecution

[5] The Apple ID [redacted] as used to back-up (at least in part) another phone [redacted]) utilized by FEUER and subscribed to FEUER's wif[redacted].

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

team, among other evidence, I believe that BRAJEVICH uses **BRAJEVICH'S PHONE**.

17. Other than what has been described herein to my knowledge, the United States has not attempted to obtain the contents of the **TARGET PHONES** by other means.

IV. STATEMENT OF PROBABLE CAUSE

25. As further detailed in the affidavits referenced above and incorporated herein, the FBI and USAO are conducting an ongoing investigation into the City Attorney's Office and LADWP, including a suspected bribery-fueled collusive litigation settlement that allegedly defrauded LADWP ratepayers out of many millions of dollars, an $800,000 hush-money payment made in order to conceal those collusive litigation practices, and obstruction of justice and perjury relating to this investigation.

26. As described in the attached January 2020 search warrants, there is probable cause to believe that FEUER made false or misleading statements to the investigation team, [redacted] wherein he denied knowledge of any hush money payment to conceal his office's litigation practices as well as knowledge of specific other details about the collusive litigation. As further detailed in that affidavit, the evidence supporting probable cause included text messages between BRAJEVICH, THOMAS PETERS (FEUER's then-Chief of Civil Litigation), and others; calendar entries for FEUER, KAPUR, BRAJEVICH, and PETERS; a surreptitious

audio recording of PETERS' contemporaneous statements detailing **FEUER's** knowledge; and corroborating proffer statements[6] by PETERS, among other evidence. The affidavit additionally set forth probable cause to believe that evidence of the Subject Offenses and criminal schemes identified above would be located in, among other places, the iCloud back-ups then believed to be linked to **FEUER'S PHONE** and **BRAJEVICH'S PHONE**, and in the City email accounts of FEUER, KAPUR, and BRAJEVICH.

27. Upon receiving the filtered data from FEUER's Apple ID [redacted] and the associated iCloud back-up pursuant to the January 2020 search warrants, the FBI learned that the data produced by Apple associated with FEUER's Apple ID [redacted] was from another phone that FEUER appeared to use primarily for personal purposes, but not from **FEUER's PHONE**, although **FEUER's PHONE** was the phone number used to register this Apple ID ([redacted] Based on my training and experience, I understand this to mean that **FEUER** utilized the Apple ID [redacted] for the other phone and backed up data from the other phone to this iCloud account, but did not back up data from **FEUER's PHONE** to this iCloud account. The FBI is not aware whether FEUER utilized a different Apple ID for **FEUER's PHONE** and if so, is currently unable to identify such an account. In the event that an Apple ID was identified for **FEUER's PHONE**, it is unknown whether

[6] Proffer statements provide use immunity for statements by a person in return for the information they provide. The written agreement, however, allows the government to use such information derivatively, including in search warrant applications.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

FEUER's PHONE utilized an iCloud back-up, what data/content, if any, existed in the back-up, and how much data/content was available based on how often back-ups occurred for the relevant time period. Based on my training and experience, individuals who utilize iCloud can select what content is and is not backed up. In addition, some applications and content is not backed up and therefore the only way to obtain the information would be from the phone itself. As such, the best way to obtain data is directly from **FEUER's PHONE**.

28. The filtered data from BRAJEVICH's iCloud account pursuant to the January 2020 search warrants indicated that while data from **BRAJEVICH's PHONE** was periodically backed up to BRAJEVICH's iCloud account, iMessages, text messages, SMS messages, and chats were not available or present in the records produced by Apple. As such, the only way to obtain that data from **BRAJEVICH's PHONE** would be from the phone itself.

29. Pursuant to the January 2020 search warrants, the FBI obtained from Google a substantial volume of data from the City email accounts of FEUER and KAPUR.[7] The review of that data is ongoing, and has been complicated and slowed by the government's protocols of filtering all data through a team of attorneys and the required ingestion and processing of voluminous data into a document-management database at multiple stages. Some of the relevant evidence reviewed to date is detailed below.

[7] The January 2020 search warrants also directed Microsoft to produce data from BRAJEVICH's email account. However, following service of the warrant, Microsoft advised that the contents of that account were not hosted by Microsoft and were likely stored on a server on LADWP premises.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

A. FEUER's Potentially False or Misleading Statements [redacted] That He Was Not Apprised of Key Portions of CLARK's Deposition Testimony

30. Filtered evidence from mike.feuer@lacity.org ("FEUER's CITY EMAIL") indicates that he may have provided misleading or false information to investigators [redacted] on at least one other topic beyond the two areas of apparent misleading or false statements described in the affidavit supporting the January 2020 search warrants and summarized briefly above. Specifically, FEUER [redacted] stated in his July 22, 2019 interview that he was not aware of the substance of the February 2019 deposition testimony of his Chief Deputy, JAMES CLARK, with the exception of one exchange that FEUER had inadvertently learned about from a reporter.[8] The single exchange about which FEUER [redacted] stated that he was aware centered around CLARK's testimony that he was sure that he had advised FEUER of the existence of the draft *Jones* complaint. According to FEUER, after learning of

[8] As noted in the prior affidavits referenced and incorporated herein, CLARK was selected to represent the City in a Person Most Qualified, or "PMQ," deposition in February 2019. During that deposition, CLARK gave significant testimony that was contrary to the City's official position and highly advantageous to the litigation position of the City's opponent, PwC. For example, CLARK testified that he was aware of the class action complaint against the City before it was filed, and that the City deliberately selected an opposing counsel because of his willingness to settle on terms favorable to the City. Following his PMQ testimony, CLARK met with counsel for the City and subsequently issued an errata purporting to change or reverse approximately 55 answers, many of them in a substantive manner that more closely adhered to the City's narrative. Following CLARK's first day of testimony on February 26, 2019, his PMQ deposition subsequently continued on April 9, 2019, and April 29, 2019.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

this exchange from the reporter, he told CLARK, "I don't recall such a conversation. We never had that conversation."

31. As detailed below, apart from that one exchange, FEUER was emphatic that he was otherwise not apprised of the substance of CLARK's testimony. [redacted] FEUER expounded on why it was important that he not be involved in or apprised of CLARK's ongoing PMQ deposition testimony before it was concluded (in late April 2019), because FEUER felt that CLARK needed to tell "his version of the truth without any influence from me." FEUER repeatedly stated that he was only aware of the one aforementioned exchange that he inadvertently learned about from a reporter.

32. In an interview with the investigation team on July 22, 2019, FEUER's statements about CLARK's deposition testimony included the following colloquy:

> Q. What about Mr. Clark's testimony? I understand that he testified in February of 2019. Did you read his transcripts?
>
> A. **I have not read the transcript, no.**
>
> Q. Did you speak with him in the wake of that deposition testimony?

33. FEUER apparently interpreted the above question as an inquiry about an instance in the deposition wherein a media outlet reported that CLARK testified about speaking with FEUER on a particular issue. FEUER stated that after CLARK's statement was brought to FEUER's attention via the media, FEUER spoke with CLARK about it. Specifically, according to FEUER:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

A: I said to Mr. Clark at that point, "I don't recall such a conversation. We never had that conversation." And he did not recall even saying it in the deposition. So that was that. So we responded to the Daily Journal. Mr. Clark was -- I was told -- going to be correcting his deposition.

Q. Did you have conversations with him about that before it happened?

A. No. What I wanted to say to you is I did not want in any manner to have any conversation with Mr. Clark that would have any effect on his testimony, either the corrections or if he was then redeposed. So, obviously, I have views about these issues because I did not have such conversations. But I said to my staff, I want there to be no conversations and no inference that he could even draw about anything I think about this until his depositions are done.

34. FEUER further stated that although he was aware that his staff would be working with CLARK to correct any inaccuracies to the portion of his PMQ deposition that had already taken place, he directed his staff that, "I do not want Mr. Clark to draw or to have any sense of my views of his testimony." FEUER further stated that notwithstanding the brief conversation he initiated with CLARK about the above-referenced portion of testimony that FEUER had learned from the media, "I was very sensitive to the fact that Mr. Clark needed to be able to tell his version of the truth without any influence from me since my name was associated with his quote . . . . I did not want for a second for him to infer one way or the other my views on the topic until his testimony was finished."

35. In further describing his role with respect to CLARK's deposition and the many measures he purportedly took to remain distanced from it, FEUER stated as follows: "**I was never**

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

involved in, very purposely, with Mr. Clark's deposition testimony. I did not prepare him for the testimony. I did not accompany him to the deposition. **I was not apprised of his testimony after it was conducted**."

[redacted]

[redacted][9] repeated explanations to the prosecution team [redacted] about the single instance of CLARK's PMQ deposition testimony that he was apprised of is consistent with his testimony in his own civil deposition in the *City v. PwC* case. When asked whether he was aware of a portion of CLARK's testimony, FEUER replied, "**I am not aware of the content of Mr.**

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

[redacted]

37. The review to date of FEUER's CITY EMAILS, which is ongoing, indicates that FEUER was in fact "aware of the content of Mr. Clark's deposition" because he was apprised by his staff in details as to numerous aspects of CLARK's PMQ deposition, [redacted]

38. On March 24, 2019, after CLARK's errata was issued but before his deposition testimony continued in April, KAPUR sent FEUER, via iPad, a lengthy email, partially provided below and in full (**Exhibit 2**), entitled, "Jim's Deposition," relaying excerpts from CLARK's first day of PMQ deposition and the subsequent corrections to his testimony as follows:

Clark's deposition, with one exception." He elaborated by detailing the above-referenced occasion on which he was contacted by a reporter with a question about CLARK's testimony, and then again confirmed that he had not read CLARK's testimony or the errata thereto. While false or misleading sworn testimony at a civil deposition in a state case would not, standing alone, violate federal law, it is consistent with what I perceive as FEUER's misleading or false narrative in an interview with the federal government [redacted] intended to convey that FEUER had not been apprised of any portion of CLARK's deposition testimony, apart from that one clearly delineated exception.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

> [Email from KAPUR to FEUER] Mike: **The following are some excerpts from Jim's depo.** I am paraphrasing but you will get the gist. O: indicates his original response and R: his revised. A: answers that weren't amended. Statements in quotation marks are statements Jim made (again sometimes paraphrased) but without the question attached. While I suspect much of this can be explained as the questions were less than precise, etc., I wanted you to get a feeling for the breadth of the confusing responses – many of which are not objectively clarified through documentation.
>
> Did Mr. Tom tell you he was aware that P[10] [PARADIS] had an atty/client relationship with Jones?
>
> O: I think so
>
> R: He did not
>
> Did P brief any (of our DWP attorneys) on nature of his representation of Jones?
>
> O: I don't know
>
> R: They say he did not.

39. Between one and eight hours[11] after KAPUR's March 24, 2019 email summarizing CLARK's deposition testimony and the corrections thereto was sent, FEUER forwarded it to his same City email address. It does not appear that any other address

[10] Based on my knowledge of the investigation, I believe all references to "P" are PAUL PARADIS, former special counsel for the City.

[11] The timestamp on KAPUR's email is 11:28 p.m. on March 24. The timestamp on FEUER's forward of the email is 12:31 a.m. on March 25; however; his email indicates the timestamp of KAPUR's original email as 4:28 p.m on March 24. In my review of FEUER'S and KAPUR'S CITY EMAILS, I have noted other instances of a time lag of seven hours between the timestamp on an email and the timestamp of the same email as indicated in a reply. Based on this review, I believe that the time lag is due to a computer reversion to Greenwich Mean Time (+0 hours) versus Pacific Standard Time (+7 hours).

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

was blind-copied, and I do not know why FEUER forwarded this email to himself.

40. Additionally, on two occasions, KAPUR emailed CLARK's deposition transcript to FEUER's secretary.[12] On March 12, 2019, KAPUR sent CLARK's rough deposition transcript without any text in her email. On March 18, 2019, KAPUR emailed CLARK's deposition transcript with "corrections interlineated," (which appeared to indicate that the changes that the City intended for CLARK to make in his errata were written into the transcript for each segment of purportedly erroneous testimony) and asked that it be printed, cautioning that it was "sensitive."

B. FEUER's Potentially False or Misleading Statement That He Was Not Aware of CLARK's Deposition Notes That CLARK Later Destroyed

41. In a recorded interview with the investigation team on July 22, 2019, FEUER was asked whether he was aware that CLARK testified that he had taken notes to prepare for his PMQ deposition. FEUER replied that he was not aware of that. When asked whether he would be concerned if CLARK had taken notes and had then destroyed or discarded them, FEUER described, at length, the circumstances in which CLARK's hypothetical destruction of notes would or would not have concerned FEUER, had he known about it. The interview contained the following colloquy:

[12] Based on my review of FEUER's and KAPUR's CITY EMAILS, while KAPUR was apparently assigned to a different secretary, KAPUR did occasionally send tasks or requests to FEUER's secretary, indicating that FEUER's secretary may have occasionally filled in for KAPUR's.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Q. **Are you familiar with that, during his own -- during some preparation for the deposition Mr. Clark was taking notes to prepare himself for the deposition?**

A. **No.** Again, I wasn't involved with the preparation.

Q. **And just -- if you grant that indulgence -- that, say, Mr. Clark had prepared notes or taken notes as part of his own preparation for his deposition, that he had done that, would you have any concerns about him destroying those notes prior to the deposition?** And destroyed, just thrown them away, shredded them up so they weren't available. Would that concerned you?

A. **You know, I'd have to -- the answer is I don't know.** I'd have to go back and look to see – I don't recall rules around preservation around -- certainly if we're in the middle of litigation and they were a document and we were required to preserve it, the destruction of that document as evidence would be wrong to do. Notes that he was taking in the course of that, I'd have to go back and look. I don't know what the rules are about that.

Q. **And then if during that deposition he referenced the fact that he didn't remember things that he had taken notes on that were then thrown away, would that concern you as just in terms of his own preparation for a deposition?** Where, if your employees take notes for a deposition, throws them away, and then at the deposition says they can't answer certain questions because he threw away his notes? It just strikes us as a little weird, a little odd for a preparation for a deposition.

A. **You know, I don't know.** Again, I think in retrospect, simple things are true. Hindsight is easy. But in retrospect, Mr. Clark had just returned from a couple-month medical leave. In retrospect, Mr. Paradis, if I had my druthers, would not have been preparing him for this deposition.

42. As noted above, in the aforementioned March 24, 2019 email summary of CLARK's PMQ deposition, KAPUR advised FEUER that CLARK had substantively testified as follows:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

"I discarded my notes last Friday. I don't need them (4-5 pages).

Doesn't know and didn't ask if a retention order in place."

43. Based on my training, experience, and knowledge of the investigation, I am aware that the emails of City officials and employees are subject to broad public disclosure obligations, including pursuant to the California Public Records Act, and that City officials and employees are often careful to refrain from including sensitive details in emails for that reason. From the ongoing review of FEUER's and KAPUR's CITY EMAILS obtained pursuant to the January 2020 search warrants, I am further aware that FEUER and KAPUR are cognizant of those disclosure obligations. As such, I believe that FEUER and KAPUR are likely more cautious in discussing sensitive matters, which would include issues related to the Subject Offenses and criminal schemes, via email, and more likely to discuss such matters by other means, including using the **TARGET PHONES**.

44. In reviewing FEUER's CITY EMAILS, I learned that he habitually created for himself draft emails (which were apparently not sent to anyone) with notes to himself about certain meetings, conversations, or other events, including several relating to the fallout from the DWP billing litigation. I believe that FEUER's practice of using email to memorialize his strategies, state of mind, and plans relating to the DWP billing litigation problems suggests a possible use of the Notes, Reminders, Pages, or other note-taking functions or applications on **FEUER's PHONE** to capture similar writings.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Examples of such draft emails that appear to relate to the Subject Offenses and criminal schemes include the following:

a. January 28, 2019 draft email:

From: 'Mike Feuer' <mike.feuer@lacity.org>
To:
Sent: 1/28/2019 9:51:14 PM
Subject:

any chance revealing could expose us to more than otherwise?
should we roll out last 2 piece first?
review 5 aspects:

- no obj
- jim
- mediation priv
- depo of indep monitor

how confer with jim? wasn't most of what berle did in dwp, not pwc case?

- mediation priv waiver
- depo of indep monitor
- jim as pmq

retain new counsel?

Based on my knowledge of the investigation, as further detailed in the attached affidavit, I believe that FEUER's statement in this January 28, 2019 draft email on the PwC matter asking himself, "any chance revealing could expose us to more than otherwise?" is likely a reference to his then-ongoing deliberations over whether to reveal information about PARADIS's and KIESEL's work on behalf of the plaintiff in the *Jones v. City* case, which — according to PETERS — PETERS discussed at length with FEUER and KAPUR in several conversations between January 25, 2019, and January 30, 2019. As further described in the attached affidavit, PETERS's proffer statements to that effect are corroborated by 1) a phone call, surreptitiously recorded by a third party, wherein PETERS related such a

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

conversation with FEUER; 2) calendar entries reflecting ongoing meetings between FEUER, KAPUR, and PETERS, on those dates (including January 28, 2019); and 3) voicemails from BRAJEVICH to PETERS.

b. March 8, 2019 and March 11, 2019 draft emails: Two draft unsent emails dated March 8, 2019 (entitled "Theory of the case"), and March 11, 2019 (no subject header), contained FEUER's articulated bullet-form narratives about his office's laudable achievement on behalf of the ratepayers in the *Jones* settlement, his adherence to the highest ethical standards, his plan for hiring an outside ethics expert, and his intent to hold PwC accountable for DWP's billing problems. This narrative was mirrored in FEUER's multiple public statements on the matter, [redacted] interview statements to the investigation team, and deposition testimony.

c. March 23, 2019 draft email: Another draft unsent email dated March 23, 2019, about his strategy for containing the fallout contains bullet points including the following: "depos —— DWP lawyer revelations," "email review —— no surprises/worst of worst," "criminal investigation," and "recs for my action —— th and j (implication)." The context and significance of these and other references is not entirely clear, but because the instant investigation was not public (and indeed was in its infancy) by that date, I believe the reference to "criminal investigation" may reflect FEUER's consideration of instigating a criminal investigation from his office, or his awareness of the possibility that other entities might commence

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a criminal investigation. I further believe that FEUER's reference to recommendations for his action as to "th and j" likely means ["THOM"] PETERS and ["JIM"] CLARK may relate to FEUER's consideration of whether to take employment or other measures relating to PETERS and CLARK for their role in the billing litigation and its fallout.

d. August 9, 2019 draft email: In another unsent draft email dated August 9, 2019, FEUER listed what appeared to be his talking points for a meeting with an individual appointed by City Council to oversee the City Attorney's Office's handling of the Jones/DWP/PwC situation. These talking points reflected FEUER's strategy for handling the various investigations and cases then pending. Additionally, FEUER set forth his bulleted arguments against the notion that FEUER should be recused from ongoing litigation in the matter.

e. August 29, 2019 draft email: In a draft unsent email dated August 29, 2019, FEUER itemized his vision for the optimal way forward in the DWP billing litigation morass, including the text of a statement that he hoped to obtain from the U.S. Attorney's Office asserting that neither he nor anyone from his office was a target or subject of this investigation.

45. Similarly, the limited data available from BRAJEVICH's iCloud account included three Notes, one of which appeared to briefly reflect a meeting at the mayor's office on March 27, 2019, relating to the DWP billing litigation. As described further in Exhibit 1 and in my other affidavits incorporated herein, multiple developments unfurled in the DWP billing

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

litigation during March 2019 that were detrimental to the City, including the resignation of the City's Special Counsel in the PwC litigation, a finding by the judge overseeing that litigation that there was evidence sufficient to establish a prima facie case of fraud by the City, and invocation of the Fifth Amendment by the plaintiff's attorney who had been recruited by the City's Special Counsel, among other events. As such, I believe that a meeting at the mayor's office on March 27, 2019, would likely have discussed facts relevant to the Subject Offenses and criminal schemes. I believe that this evidence suggests that BRAJEVICH may also have additional Notes or similar writings stored on his phone relevant to the Subject Offenses and criminal schemes.

C. Additional Evidence

a. I have reviewed Verizon toll records from **KAPUR's PHONE** for the calendar year 2019, which reflect 12 calls, on seven different dates, between **KAPUR's PHONE** and **FEUER's PHONE** from that year.[13] Based on my review of FEUER's and KAPUR's CITY EMAILS, most of these 12 calls appear to be temporally proximate to events reflected in those emails related to the collusive

[13] Based on information learned in the investigation as to the importance of the Chief of Staff position and FEUER's and KAPUR's close professional relationship, as detailed in the attached prior affidavit, I believe that FEUER and KAPUR would likely have engaged in calls on more than seven dates during 2019, which suggests that they may have been using other technology, such as FaceTime or another telephone application, to do so. Based on my training and experience, the Verizon phone tolls that I reviewed would only reflect direct cell-to-cell and would not indicate iMessages, FaceTime calls, or messages or calls using other secure applications. However, evidence of such messages or calls would potentially be stored on **FEUER's PHONE** and **KAPUR's PHONE**.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

litigation and the City's attempts to cast itself in a positive light following public revelation of details thereof. Moreover, all but one of these 12 calls are temporally proximate to email exchanges involving outside counsel for the DWP cases, suggesting that the substance of those calls likely included discussion of the DWP cases, possibly with outside counsel joining the calls.

46. Based on my training and experience and knowledge of this investigation, including information that I have received about the role of KAPUR as Chief of Staff to FEUER, I believe that the above-described evidence may suggest that FEUER and KAPUR primarily engaged in cell-to-cell communications when outside counsel was involved, and that they may have used other channels, such as FaceTime or another secure telephone application, for one-on-one verbal communications. I am aware from my training and experience that any such communications would not be reflected in the toll records for either subscriber, but that evidence of any such communications might be contained in their respective phones.

47. One call with **FEUER's PHONE** during 2019 reflected on KAPUR's toll records —— specifically at 2:02 a.m. on February 9, 2109 —— took place before the City's outside counsel was brought into the case (and thus would not have involved a call on FEUER's PHONE with them). I reviewed an email from that date wherein FEUER asked KAPUR, at 1:31 a.m., to call him, and he could explain when they spoke. In a follow-up email at 1:32 a.m., FEUER stated, "Shoulda said to use cell: [redacted]

[**FEUER's PHONE**]." I believe that FEUER's clarifying email asking KAPUR to call him on **FEUER's PHONE** and providing the number to her —— his longtime Chief of Staff —— may further suggest that their one-on-one verbal communications usually took place via some channel other than cell-to-cell calls.

D. Disclosure of Information Unrelated to Probable Cause

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

X. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[14]

51. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents,

[14] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

52. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

53. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress FEUER's, KAPUR's, or BRAJEVICH's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of FEUER's, KAPUR's, or BRAJEVICH's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

54. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

XI. CONCLUSION

55. Based on the foregoing, I request that the Court issue the requested search warrants.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 14th day of August, 2020.

HONORABLE PATRICK J. WALSH
UNITED STATES MAGISTRATE JUDGE

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

EXHIBIT 1

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of: Information associated with accounts identified as [redacted] joseph.brajevich@ladwp.com; and associated with the phone number [redacted] that is within the possession, custody, or control of Apple Inc.	Case No. 2:20-MJ-00396

APPLICATION FOR WARRANT PURSUANT TO 18 U.S.C. § 2703

I, a federal law enforcement officer, request a warrant pursuant to Title 18, United States Code, Section 2703, and state under penalty of perjury that I have reason to believe that within the following data:

See Attachment A-1

There are now concealed or contained the items described below:

See Attachment B

The basis for the search is:

☑ Evidence of a crime;
☑ Contraband, fruits of crime, or other items illegally possessed;
☐ Property designed for use, intended for use, or used in committing a crime.

The search is related to a violation of:

Code section(s)	*Offense Description*
18 U.S.C. §§ 371; 666; 1001; 1341; 1343; 1346; 1505; 1510; 1951; 1956; and 1621	Conspiracy; Bribery and Kickbacks Concerning Federal Funds; False Statements; Mail Fraud; Wire Fraud; Deprivation of Honest Services; Obstructing Federal Proceeding; Obstruction of Justice; Extortion; Money Laundering; and Perjury in a Federal Proceeding (collectively, the "Target Offenses").

The application is based on these facts:

See attached Affidavit, which is incorporated herein by reference.

Applicant's signature
Andrew Civetti, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: _____

Judge's signature

City and State: _____

Patrick J. Walsh, U.S. Magistrate Judge
Printed name and title

AUSA: Melissa Mills- Ext. 0627

ATTACHMENT A-1

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the Apple accounts associated with the below, and specifically including associated iCloud and iTunes accounts, that is within the possession, custody, or control of Apple Inc., a company that accepts service of legal process at 1 Infinite Loop, M/S 36-SU, Cupertino, California, 95014, regardless of where such information is stored, held, or maintained.

a. The Apple iCloud account, [redacted] associated with the phone number [redacted] and the name MIKE FEUER (**"FEUER's ACCOUNT"**);

b. The Apple iCloud account, [redacted] and Apple iCloud account, joseph.brajevich@ladwp.com, associated with the phone number [redacted] and the name JOSEPH BRAJEVICH (**"BRAJEVICH's ACCOUNT"**);

c. The Apple iCloud account associated with the phone number [redacted] and the name JAMES CLARK (**"CLARK's ACCOUNT"**).

ATTACHMENT B

I. SEARCH PROCEDURES INCLUDING PRIVILEGE REVIEW PROCEDURE

1. The warrant will be presented to personnel of Apple, Inc. (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below in Section IV.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.15.a. below), law enforcement agents and/or other individuals assisting law enforcement agents who are not participating in the investigation of the case and who are assigned as the "Privilege Review Team" will review the content records, according to the procedures set forth herein, to determine whether or not any of the content records appears to contain or refer to communications between an attorney, or to contain the work product of an attorney, or between a spouse and any person ("potentially privileged information"). The "Search Team" (law enforcement personnel conducting the investigation

and search and other individuals assisting law enforcement personnel in the search) will review only content records which have been released by the Privilege Review Team. With respect to the non-content information produced by the PROVIDER (see Section II.15.b. below), no privilege review need be performed and the Search Team may review immediately.

5. With respect to content records, the Search Team will provide the Privilege Review Team and/or appropriate litigation support personnel[1] with an initial list of "scope key words" to search for on the content records, to include words relating to the items to be seized as detailed below. The Privilege Review Team will conduct an initial review of the content records using the scope key words, and by using search protocols specifically chosen to identify content records that appear to be within the scope of the warrant. Content records that are identified by this initial review, after quality check, as not within the scope of the warrant will be maintained under seal and not further reviewed absent subsequent authorization or in response to the quality check as described below.

6. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for among the content records that are identified by the initial review and quality check described above as appearing to fall within the

[1] Litigation support personnel and computer forensics agents or personnel, including IRS Computer Investigative Specialists, are authorized to assist both the Privilege Review Team and the Investigation Team in processing, filtering, and transferring documents and data seized during the execution of the warrant.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

scope of the warrant, to include specific words like names of any identified attorneys or law firms and names of any identified spouses] or their email addresses, and generic words such as "privileged" and "work product". The Privilege Review Team will conduct an initial review of these content records by using the privilege key words, and by using search protocols specifically chosen to identify content records containing potentially privileged information. Content records that are not identified by this initial review as potentially privileged may be given to the Search Team.

7. Content records that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Content records determined by this review not to be potentially privileged may be given to the Search Team. Content records determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a Privilege Review Team Assistant United States Attorney ("PRTAUSA"). Content records identified by the PRTAUSA after review as not potentially privileged may be given to the Search Team. If, after review, the PRTAUSA determines it to be appropriate, the PRTAUSA may apply to the court for a finding with respect to particular content records that no privilege, or an exception to the privilege, applies. Content records that are the subject of such a finding may be given to the Search Team. Content records identified by the PRTAUSA after review as privileged will be maintained under seal by the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

investigating agency without further review absent subsequent authorization.

8. The Search Team will search only the content records that the Privilege Review Team provides to the Search Team at any step listed above in order to locate, extract and seize content records that are within the scope of the search warrant (see Section III below). The Search Team does not have to wait until the entire privilege review is concluded to begin its review for content records within the scope of the search warrant. The Search Team and the Privilege Review Team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

9. During its review, the Search Team may provide the Privilege Review Team and/or appropriate litigation support personnel with a list of additional "scope key words" or search parameters to capture the items to be seized as detailed below; any additional content records identified through this quality check must first be reviewed by the Privilege Review Team subject to the terms set forth herein before being released to the Search Team. This quality check is intended only to ensure that the initial scope key word review successfully eliminated only data outside the scope of the search warrant from seizure.

10. If, while reviewing content records or non-content information, either the Privilege Review Team or the Search Team encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

shall immediately discontinue its search pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

11. The Privilege Review Team and the Search Team will complete the search of non-content information and both stages of the search of the content records discussed herein as soon as is practicable but not to exceed 180 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the records beyond this 180-day period without first obtaining an extension of time order from the Court.

12. Once the Privilege Review Team and the Search Team have completed their review of the non-content information and the content records and the Search Team has created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the Search Team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, neither the Privilege Review Team nor the Search Team will access the data from the sealed original production which fell outside the scope of the items to be seized or was determined to be privileged absent further order of the Court.

13. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

14. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDER

15. To the extent that the information described in Attachment A is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each **TARGET ACCOUNT** listed in Attachment A:

a. All contents of all wire and electronic communications associated with the **TARGET ACCOUNT**, limited to that which occurred on or after December 1, 2014,[2] including:

i. All e-mails, communications, or messages of any kind associated with the **TARGET ACCOUNT**, including stored or preserved copies of messages sent to and from the account, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information

[2] To the extent it is not reasonably feasible for the PROVIDER to restrict any categories of records based on this date restriction (for example, because a date filter is not available for such data), the PROVIDER shall disclose those records in its possession at the time the warrant is served upon it.

associated with each e-mail or message, and any related documents or attachments.

ii. All records or other information stored by subscriber(s) of the **TARGET ACCOUNT**, including address books, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files.

iii. All records pertaining to communications between the PROVIDER and any person regarding the **TARGET ACCOUNT**, including contacts with support services and records of actions taken.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), any alternate names, other account names or e-mail addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, **and including any changes made to any subscriber information** or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

services used, and including the dates on which such changes occurred, for the following accounts:

(I) the **TARGET ACCOUNT**.

ii. All user connection logs and transactional information of all activity relating to the **TARGET ACCOUNT** described above in Section II.15.a., including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations, and including specifically the specific product name or service to which the connection was made.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

16. For each **TARGET ACCOUNT** listed in Attachment A, the search team may seize all information between December 1, 2014, and the present described above in Section II.15.a. that constitutes evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding), namely:

a. Information relating to who created, accessed, or used the **TARGET ACCOUNT**, including records about their identities and whereabouts.

b. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Retention of PAUL PARADIS and PAUL KIESEL, or entities related thereto, to represent the City of Los Angeles;

ii. Communications involving or relating to any party to, or to counsel for any party to, *Jones v. City of Los Angeles* (the "*Jones* matter") or *City of Los Angeles v. PricewaterhouseCoopers* (the "*PwC* matter"), including communications with or referencing MICHAEL FEUER, JAMES CLARK, THOMAS PETERS, PAUL PARADIS, PAUL KIESEL, GINA TUFARO, LEELA KAPUR, JOSEPH BRAJEVICH, Julissa Salgueiro, and other counsel and parties;

iii. Any lawsuit where the City was a party to the lawsuit and appears to have had a legal, representational, and/or financial interest in both sides of the lawsuit, including the *Jones* matter;

iv. The litigation of the *Jones* matter and the *PwC* matter, including discovery disputes, the deposition of the City's "person most qualified," and emails and other materials arguably or allegedly responsive to discovery demands or court orders;

v. Efforts to conceal the litigation practices of the City Attorney's Office's or members or representatives thereof in the litigation related to the LADWP billing system, including knowledge or direction of payments made or benefits

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

given to individuals or entities in an effort to discourage their revelation of those practices;

vi. Efforts to conceal actions by the City Attorney's Office or members or representatives thereof in the litigation related to the LADWP billing system, including shielding documents from production, filing false or misleading documents with the court, and offering false or misleading testimony;

vii. The City's actions, strategy, or tactics in responding to revelations or allegations of fraud, discovery violations, and unethical conduct in the litigation related to the LADWP billing system, including media outreach and contacts, litigation decisions, notification or lack of notification to the court of relevant developments, authorization of payment of hush money, and other actions;

viii. Negotiations or agreements relating to hush money payments offered to or solicited by any individual or entity to conceal business practices related to the LADWP billing litigation by the City Attorney's Office or members thereof, and communications relating thereto;

ix. Obstruction of justice, perjury, or false official statements related to the LADWP billing litigation;

x. Destruction or concealment of evidence related to the LADWP billing litigation.

c. Calendar or date book entries and notes, including calendars or date books stored on digital devices;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

d. All records and information described above in Section II.15.b.

IV. PROVIDER PROCEDURES

17. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. The PROVIDER shall send such information to:

[redacted]

18. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

19. IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 2705(b), that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A, of the existence of the warrant, until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date this warrant is signed by the magistrate judge or such later date as may be set by the Court upon application for an extension by the United States. Upon expiration of this order, at least ten business days prior to disclosing the existence of the warrant, the PROVIDER shall notify the filter attorney identified above of its intent to so notify.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

AFFIDAVIT

I, Andrew Civetti, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since September 2015. I am currently assigned to a Public Corruption Squad, where I specialize in the investigation of corrupt public officials, including bribery, fraud against the government, extortion, money laundering, false statements, and obstruction of justice. In addition, I have received training in the investigation of public corruption and other white collar crimes.

2. I am currently one of the agents assigned to an investigation of alleged corrupt activities at the Los Angeles Department of Water and Power ("LADWP") and the Los Angeles City Attorney's Office ("City Attorney's Office"). As discussed in more detail herein, these activities include the following criminal schemes, among others:

a. Collusive litigation practices related to lawsuits involving the City Attorney's Office and LADWP, which were fueled in at least one instance by a $2.175 million kickback from plaintiff's attorney JACK LANDSKRONER to attorney PAUL PARADIS, a Special Counsel retained by the City Attorney's Office.

b. The concealment of an $800,000 hush-money payment to a prospective whistleblower by Special Counsels PARADIS and

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

PAUL KIESEL in exchange for silence as to collusive and potentially fraudulent litigation practices involving PARADIS, KIESEL, and THOMAS PETERS, then the Chief of Civil Litigation at the City Attorney's Office, among others.

3. I am aware that the City receives in excess of $10,000 annually in federal funds through various programs.

II. PURPOSE OF AFFIDAVIT

4. I make this affidavit in support of applications for search warrants to Apple, Inc., Google, Inc., and Microsoft Corporation for the seizure of information associated with the following accounts (collectively, the "**TARGET ACCOUNTS**"):

Apple, Inc. Accounts

a. The Apple iCloud account,[1] [redacted] associated with the phone number [redacted] and the name MIKE FEUER (**"FEUER's ACCOUNT"**);

b. The Apple iCloud account, [redacted] and Apple iCloud account, joseph.brajevich@ladwp.com, associated with the phone number [redacted] and the name JOSEPH BRAJEVICH (**"BRAJEVICH's ACCOUNT"**);

[1] According to Apple's website, "iCloud stores your content securely and keeps your apps up to date across all your devices. That means all your stuff—photos, files, notes, and more—is safe and available wherever you are. iCloud comes with 5 GB of free storage and you can add more storage at any time." Based on my review of Apple's website and my review of Apple subscriber information, I understand that phone numbers are linked to iCloud Accounts to secure and retrieve data. Specifically, the use of iCloud with an Apple device and associated phone number may have content capturing an individual's utilization of that device.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

c. The Apple iCloud account associated with the phone number [redacted] and the name JAMES CLARK (**"CLARK's ACCOUNT"**);

Google, Inc. Accounts

d. Mike.Feuer@lacity.org (**"FEUER's EMAIL"**);

e. Leela.Kapur@lacity.org (**"KAPUR's EMAIL"**);

Microsoft Corporation Account

f. Joseph.Brajevich@ladwp.com (**"BRAJEVICH's EMAIL"**).

5. Apple Inc. ("PROVIDER #1") is a provider of electronic communication and remote computing services, headquartered at Cupertino, California. Google, Inc. ("PROVIDER #2") is a provider of electronic communication and remote computing services, headquartered at Mountain View, California. Microsoft Corporation ("PROVIDER #3") is a provider of electronic communication and remote computing services, headquartered at Redmond, Washington (collectively, the "PROVIDERS").[2]

[2] Because this Court has jurisdiction over the offenses being investigated, it may issue the warrant to compel the PROVIDERS pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). See 18 U.S.C. §§ 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction") and 2711 ("the term 'court of competent jurisdiction' includes -- (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that -- (i) has jurisdiction over the offense being investigated; (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title").

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

6. The information to be searched is described in Attachments A-1 through A-3. This affidavit is made in support of applications for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A) and 2703(d)[3] to require the PROVIDERS to disclose to the government copies of the information (including the content of communications) described in Section II of Attachment B. Upon receipt of the information described in Section II of Attachment B, law enforcement agents and/or individuals assisting law enforcement and acting at their direction will review that information to locate the items described in Section III of Attachment B subject to the search protocol and potential privilege review procedures outlined in Attachment B. Attachments A-1 through A-3 and Attachment B are incorporated herein by reference.

7. As described more fully below, I respectfully submit there is probable cause to believe that the information associated with the **TARGET ACCOUNTS** constitutes evidence, contraband, fruits, or instrumentalities of criminal violations

[3] The government is seeking non-content records pursuant to 18 U.S.C. § 2703(d). To obtain the basic subscriber information, which do not contain content, the government needs only a subpoena. See 18 U.S.C. § 2703(c)(1), (c)(2). To obtain additional records and other information--but not content--pertaining to subscribers of an electronic communications service or remote computing service, the government must comply with the dictates of section 2703(c)(1)(B), which requires the government to supply specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation in order to obtain an order pursuant to 18 U.S.C. § 2703(d). The requested warrant calls for both records containing content as well as subscriber records and other records and information that do not contain content (see Attachment B).

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding) (collectively, the "Target Offenses").

8. The facts set forth in this affidavit are based upon my personal observations, my training and experience, information obtained from other agents and witnesses [redacted] consensually recorded conversations, and information obtained from the prior related search warrants, as detailed further below. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

9. On September 12, 2019, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized two search warrants (19-MJ-3813 and 19-MJ-3814) for PETERS's residence and person to seize PETERS's cell phone (collectively, the "September 2019 search warrants"). On July 18, 2019, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized two search warrants (19-MJ-2915 and 19-MJ-2923) for the seizure of information associated with nineteen e-mail accounts from two Internet Service Providers, and six search warrants (19-MJ-2913,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

19-MJ-2914, 19-MJ-2917, 19-MJ-2919, 19-MJ-2920, and 19-MJ-2922) for the premises of sixteen locations (collectively, the "July 2019 search warrants"). All of the July 2019 search warrants were supported by a single omnibus affidavit (the "omnibus affidavit"). The September 2019 and July 2019 search warrants and their supporting omnibus affidavit are incorporated herein by reference, and copies can be made available for the Court.[4]

III. BACKGROUND ON SUBJECTS

10. MICHAEL FEUER is the City Attorney for the City of Los Angeles. On July 22, 2019, during the execution of a search warrant at the City Attorney's Office, FEUER provided a voluntary interview, portions of which are detailed herein.[5] Thereafter, FEUER provided certain additional information to the prosecution team via telephone or in person, either directly or

[4] In addition, on April 18, 2019, the Honorable Jacqueline Chooljian, United States Magistrate Judge, authorized search warrants relating to the Los Angeles Department of Water and Power's then General Manager, DAVID WRIGHT. Specifically, these warrants authorized search warrants for WRIGHT's phone, WRIGHT's laptop, two of WRIGHT's email addresses, and two of WRIGHT's Apple iCloud accounts (collectively, the "April 2019 search warrants"). On June 4, 2019, the Honorable Patrick J. Walsh, United States Magistrate Judge, authorized search warrants for two of WRIGHT's residences, WRIGHT's office, WRIGHT's cellular phone, and a burner cellular phone that the FBI had surreptitiously provided to WRIGHT, as well as for an e-mail account used by Deputy Los Angeles City Attorney JAMES CLARK; on June 18, 2019, Judge Walsh authorized a subsequent search warrant for WRIGHT's Riverside residence (collectively, the "June 2019 search warrants"). The April 2019 and June 2019 search warrants and their supporting affidavits are also incorporated herein by reference, and copies can be made available for the Court.

[5] For all interviews and proffer sessions detailed herein, I either attended the interview myself or received information from another FBI agent who attended.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

via his Chief of Staff, LEELA KAPUR. [redacted] FEUER has indicated to the government that he had plans to run for Mayor of Los Angeles in 2022 and he believed he would be among the favorites.

a. Based on my review of Apple iCloud subscriber information which registered **FEUER's ACCOUNT** to FEUER's phone number [redacted]), my review of PETERS's phone, including messages with FEUER at [redacted] my review of subscriber records for [redacted] and FEUER's use of [redacted] to contact the prosecution team relating to the investigation, I believe that FEUER uses **FEUER's ACCOUNT**.

b. Based on my review of e-mail records, I believe FEUER uses **FEUER's EMAIL**.

11. LEELA KAPUR is the Chief of Staff to FEUER.

a. Based on my review of PETERS's phone, I believe KAPUR uses the telephone number [redacted] Based on my review of e-mail records, I believe KAPUR uses **KAPUR's EMAIL**.

12. JOSEPH BRAJEVICH is an Assistant City Attorney and the General Counsel for LADWP.

a. Based on my review of Apple iCloud subscriber information which registered **BRAJEVICH's ACCOUNT** to BRAJEVICH's phone number ([redacted] my review of PETERS's phone, including messages with BRAJEVICH at [redacted] and

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

BRAJEVICH's use of [redacted] to contact the prosecution team about the investigation, I believe that BRAJEVICH uses **BRAJEVICH's ACCOUNT.**

b. Based on my review of e-mail records, I believe BRAJEVICH uses **BRAJEVICH's EMAIL**.

13. JAMES CLARK is the Deputy Chief for the Los Angeles City Attorney and a retired partner with Gibson, Dunn & Crutcher, LLP ("Gibson Dunn"). On November 7, 2019, CLARK submitted to a voluntary interview with the prosecution team in the presence of his attorneys and pursuant to a written proffer agreement.[7]

14. Based on my review of PETERS's phone, including messages with CLARK at [redacted] I believe that CLARK uses **CLARK's ACCOUNT**.

15. THOMAS PETERS was the Chief of Civil Litigation at the City Attorney's Office. On or about March 22, 2019, PETERS resigned from that position. PETERS has requested immunity from the government pursuant to 18 U.S.C. § 6001 et seq., as well as other protections and/or recommendations with respect to prospective investigations or actions by other authorities. The government continues to consider those requests and has neither acted on them nor made representations as to whether or not they will be granted. On January 28, 2019, the government

[7] Under the terms of the proffer sessions discussed herein, the government is allowed to make derivative use of the information provided to it. The government agrees only not to use the information against the provider of the information in the government's case-in-chief against that person, provided the person is entirely truthful in proffer sessions.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

interviewed PETERS in the presence of his attorneys and pursuant to a proffer agreement.

15. PAUL PARADIS is an attorney and partner at Paradis Law Group, PLLC, operating in New York and Los Angeles. At relevant times between 2015 and March 2019, PARADIS acted as Special Counsel for the City in a civil lawsuit against PricewaterhouseCoopers ("PwC") regarding an alleged faulty billing system, (Superior Court of California, captioned *City of Los Angeles v. PricewaterhouseCoopers*, Case No. BC574690 ("*PwC* case")).

a. I have interviewed PARADIS on numerous occasions regarding his involvement in the criminal schemes and Target Offenses detailed herein in the presence of his attorneys and pursuant to a proffer agreement. Much of the information provided by PARADIS has been substantially corroborated by other evidence, and other than the details provided in footnote 9 below, I do not have a reason to believe that PARADIS has provided untruthful information.

b. PARADIS has no criminal record and has agreed to assist the government in exchange for favorable consideration in a potential future prosecution of him related to his conduct in this matter.

c. PARADIS has provided the government access to his email account, cell phone, bank accounts, and many other documents relevant to the investigation. PARADIS has also made numerous consensual recordings at the request of the government, some of which are detailed in the omnibus affidavit.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

16. GINA TUFARO was at relevant times a New York attorney and the law partner of PARADIS.

a. On June 19, 2019, I interviewed TUFARO in the presence of her attorney [redacted]

b. [redacted]

17. PAUL KIESEL, a Los Angeles-based attorney, was at relevant times a Special Counsel for the City Attorney's Office on litigation relating to the LADWP billing system.

a. The government has conducted voluntary interviews with KIESEL in the presence of his attorney, as detailed in pertinent part below. To date and to my knowledge, information proffered by KIESEL has largely been consistent with other evidence, with the possible exception of the information provided in footnote 9.[9]

[redacted]

[9] In the first part of January 2020, KIESEL informed me that he intended to contact PARADIS about litigation strategy for a federal civil lawsuit (related to the events detailed herein) in which KIESEL and PARADIS were named as defendants. PARADIS contacted me to inform me that KIESEL had contacted him before PARADIS returned the contact. At my direction, PARADIS did not record the contact. Both KIESEL and PARADIS also reported back to me on the contact. Their accounts varied slightly in the following respect:

PARADIS reported that during the course of the discussion about the federal civil lawsuit, KIESEL asked whether they had a

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. KIESEL has also voluntarily provided certain documentary information, including text messages, emails, and a handwritten entry from his diary.

18. JULISSA SALGUEIRO was previously employed as a paralegal by KIESEL until approximately July 2017. Salgueiro submitted to a voluntary interview with the prosecution team [redacted]

19. [redacted] is an attorney affiliated with KIESEL's law firm. On December 5, 2019, [redacted] submitted to a voluntary interview with the prosecution team.

20. [redacted] is a law partner of KIESEL's firm. On January 14, 2020, [redacted] submitted to a voluntary interview with the prosecution team.

21. DAVID WRIGHT was the General Manager of LADWP until his resignation or dismissal on or about July 23, 2019.

a. I have interviewed WRIGHT on several occasions, including one voluntary interview without counsel during the execution of a search warrant at his home in June 2019, and several additional voluntary interviews in the presence of his

---

conversation with PETERS in late January 2019 about documents requested by *PwC* (a situation described in further detail below). PARADIS told me that he did not provide a substantive answer to KIESEL, but that he attempted to jog KIESEL's memory by reminding him about a location significant to the conversation that PARADIS recalled. KIESEL reported that PARADIS answered his substantive question and told KIESEL that they did in fact have such a conversation with PETERS. I do not know whether this discrepancy is attributable to a misunderstanding between KIESEL or PARADIS, a lapse of memory by one of them, or an intentional misstatement by one of them. Based on my history of interactions with both and the lack of any apparent reason for either to lie about this issue, I suspect that it was either a misunderstanding or a memory lapse.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

counsel and pursuant to a proffer agreement. At various points, I believe that WRIGHT provided untruthful information in response to my questions.

22. ROBERT WILCOX is a press spokesman for the City Attorney's Office.

VI. PRESERVATION REQUESTS & SEARCH WARRANTS

23. On or about December 4, 2019, the government sent Google, Inc. a preservation letter for **FEUER** and **KAPUR EMAILS** and Microsoft Corporation a preservation letter for **BRAJEVICH's EMAIL**.

24. On or about December 6, 2019, the government obtained orders pursuant to 18 U.S.C. § 2703(d) for information associated with the **FEUER, BRAJEVICH**, and **KAPUR EMAILS**.

25. On or about January 8 and 9, 2020, the government sent Apple Inc. subpoenas, nondisclosure orders, and preservation letters for subscriber information associated with the **FEUER, BRAJEVICH,** and **CLARK ACCOUNTS**.

26. Other than what has been described herein to my knowledge, the United States has not attempted to obtain the contents of the **TARGET ACCOUNTS** by other means.

IV. SUMMARY OF PROBABLE CAUSE

A. FEUER's Knowledge of Hush Money, [redacted]

[redacted]

[redacted] the evidence provides probable cause to believe that at FEUER's implied direction, PETERS ordered KIESEL to confidentially settle Salgueiro's demands or face termination of his Special Counsel contract. Specifically, as detailed further below, PETERS informed the government that he advised FEUER of Salgueiro's threats and demands, ordered KIESEL to buy Salgueiro's silence in accordance with FEUER's perceived direction, and apprised FEUER after the hush-money settlement that the matter had been taken care of. This information is corroborated in part by information proffered by PARADIS and KIESEL, as well as by documentary evidence.

B. FEUER's Knowledge of Special Counsel's Collaboration with Opposing Counsel and Collusive Litigation January 2019, Contrary to His Later Statements [redacted]

28. Multiple sources of evidence provide probable cause to believe that FEUER obstructed justice, made materially misleading statements to the FBI, [redacted] relating to the timing of FEUER's knowledge that his Special Counsel (PARADIS and KIESEL) had collaborated with opposing counsel in a collusive lawsuit that allowed the City to settle multiple class actions on the City's preferred terms. Specifically, FEUER made official statements to the government [redacted] that I believe were intended to misleadingly indicate that

FEUER first learned about emails showing collaboration between Special Counsel and the City's opposing counsel on April 24, 2019, and that he immediately disclosed that information to the court, the City's litigation opponent, and the media. Based on my training, experience, and knowledge of the investigation, by misleadingly portraying FEUER's knowledge in this way, it appears FEUER was attempting to personally distance himself from this scandal likely for political gain (or to avoid political fallout).

29. However, the evidence indicates that PETERS apprised FEUER in as early as late January 2019 of the existence of those emails and the facts that they revealed. Specifically, as further detailed below, PETERS proffered that he told FEUER in late January 2019 about the emails and what they would show, that FEUER was very upset, that PETERS withheld them from discovery in the *PwC* matter at what he perceived to be FEUER's direction in order to conceal it from the court and the public, and that PETERS subsequently advised FEUER that FEUER no longer needed to worry about the documents being made public. This information is corroborated in part by a surreptitiously recorded phone call from January 27, 2019, wherein PETERS relayed to PARADIS, KIESEL, and TUFARO the substance of his initial contemporaneous conversation with FEUER. PETERS's proffer information is also partially corroborated by emails and calendar entries showing meetings between FEUER and PETERS related to the LADWP matters during the last week of January 2019, as well as with other evidence.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

V. STATEMENT OF PROBABLE CAUSE

25. The FBI is conducting an ongoing investigation into the City Attorney's Office and LADWP, including a suspected bribery-fueled collusive litigation settlement that allegedly defrauded LADWP ratepayers out of many millions of dollars, an $800,000 hush-money payment made in order to conceal those collusive litigation practices, and obstruction of justice and perjury relating to this investigation. Background facts relating to these and other facets of the investigation are further detailed in the omnibus affidavit referenced above and incorporated herein. The case numbers associated with the search warrants supported by my omnibus affidavit are outlined above.

A. [redacted]

1. Salgueiro's Initial Threats to Reveal Information Related to the Collusive Litigation and Demands for Hush Money

26. As further detailed below, the evidence indicates that Salgueiro obtained certain documents from KIESEL's law firm, including but not limited to documents reflecting coordination between the City's Special Counsel and the plaintiff's counsel in the *Jones* lawsuit, and threatened to reveal the documents if KIESEL did not pay her a large amount of money.

27. KIESEL advised the government of the following information:[10]

[10] As noted below, some of this information is corroborated by a contemporaneous diary entry provided by KIESEL; which I have reviewed.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. Around August or September 2017, KIESEL was approached by Salgueiro, an employee that his law firm terminated in or around July 2017.

b. Salgueiro told KIESEL that she had taken certain documents from the firm, including some that showed the City's entanglement in the representation of an adverse party that had sued the City in the LADWP billing system litigation.

c. Salgueiro initially demanded $1,500,000 from KIESEL, or she would take the materials public.

d. KIESEL was not initially concerned about Salgueiro taking the materials public, because although they might be "embarrassing" to the City, he did not believe that they reflected any wrongdoing.

28. Salgueiro advised the government [redacted]:

a. Before leaving KIESEL's employ, Salgueiro took certain documents from KIESEL's firm that she believed would show that the firm and the City conspired to represent both sides of the litigation in the *Jones v. City of Los Angeles* matter and in other matters, including unrelated cases and employment-related matters (collectively, the "Salgueiro documents").[11]

[11] [redacted]ro provided to the government, [redacted] electronic files that she described as the documents that she took from KIESEL's firm and threatened to review. These documents were submitted directly to the government's privilege-review team, and I have since reviewed a redacted version. They comprise several folders in different case names, with the documents relevant to the *Jones* matter

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. After Salgueiro was fired by KIESEL in or around July 2017, she demanded a large sum of money, around $900,000, from KIESEL in order to return the Salgueiro documents, refrain from taking the Salgueiro documents public, and resolve certain employment discrimination and harassment complaints.

c. KIESEL countered Salgueiro's demand with a lower five-figure offer, using former Special Counsel PAUL PARADIS as a mediator.

29. PARADIS proffered to the government as follows:

a. Salgueiro took the Salgueiro documents when she left KIESEL's firm and threatened to reveal them if KIESEL did not pay her a large sum of money.

---

marked "Jones." The documents from the "Jones" folder include the following relevant representative items:

- An April 16, 2015 email from KIESEL directing Salgueiro to prepare a notice of related case in the *Jones* matter "as though it was coming from Michael Libman, counsel for Jones, and NOT coming from us."
- Screenshots of apparent metadata indicating Salgueiro's preparation of various pleadings for both LANDSKRONER and the City
- Documents showing that Salgueiro and the KIESEL law firm filed documents for LANDSKRONER and LIBMAN on behalf of plaintiff Jones (including the first amended complaint), paid associated filing fees, and otherwise coordinated plaintiff's counsel's work
- Timesheets showing that Salgueiro billed time for her work preparing, finalizing, and filing documents on behalf of plaintiff Jones

The remainder of the documents (the ones not in the "Jones" folder) as provided to the prosecution team after filtering are heavily redacted, and any relevance they may have to this investigation is not presently clear to me based on the current evidence.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. PARADIS believed that some of the documents related to the *Jones* matter, and others related to another matter wherein the City played both sides of litigation.

2. Awareness by FEUER, KAPUR, BRAJEVICH, CLARK, and PETERS of Salgueiro's Threats and Demands

30. Information from multiple sources, as detailed below, provides probable cause to believe that PETERS, acting at FEUER's implied direction, instructed KIESEL to pay the hush money that Salgueiro demanded to keep her from going public with her information, including information about secret collaboration between the City and plaintiff's counsel in the *Jones* case. The below information also constitutes probable cause to believe that BRAJEVICH and KAPUR were aware of the Salgueiro threats and demands and their context. The evidence further provides probable cause to believe that CLARK had some awareness of Salgueiro's threats to reveal sensitive documents relating to the *Jones* matter, although he may not have had a full understanding of the details.

a. KIESEL'S and PARADIS'S October 2017 negotiations with Salgueiro

31. On October 10, 2017, Salgueiro sent a text message, which I have reviewed, to PARADIS stating in pertinent part, "Hi Mr. P, I left a written message with Clark's asst. on Fri. re set up of mtg n didn't hear bk. 1. Okay 2 drop off set of docs w/note saying if w/like 2 discuss 2 call me?"

32. [redacted] in October 2017, she went to the City Attorney's Office to try to speak with CLARK, but he

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

was not there. According to Salgueiro, she left with CLARK's assistant a large envelope containing a copy of the Salgueiro documents, along with a message. [redacted]

33. As described below, the evidence indicates that KIESEL engaged in multiple initial attempts to negotiate with Salgueiro, which were unsuccessful due to KIESEL's unwillingness to pay an amount that Salgueiro was willing to accept.

34. KIESEL advised the government as follows:

a. KIESEL met with Salgueiro on October 30 or 31, 2017, in a meeting at LADWP headquarters coordinated by PARADIS, who was serving as a "mediator" between Salgueiro and KIESEL. An individual known as Rosa or "Mama Rosa" (later identified as Rosa Rivas) accompanied Salgueiro. At that time, Salgueiro demanded $900,000, in an offer that she said would remain open for 24 hours. KIESEL agreed to think about it and then countered with an offer of $60,000.

b. KIESEL then received a text message from Salgueiro that she would see him in CCW[12] on December 4, 2017, which KIESEL interpreted as a threat to publicize her information at the next-scheduled hearing in *City of Los Angeles v. PwC*, which was scheduled for that date in the Central Civil West courthouse.

35. PARADIS proffered the following relevant information:

[12] Central Civil West was at the time a Superior Court courthouse in Los Angeles, where the judge presiding over the *City of Los Angeles v. PwC* litigation was located.

a. On October 30, 2017, PARADIS and KIESEL met with Salgueiro and "Mama Rosa" at the LADWP cafeteria in an attempt to "mediate" Salgueiro's demands. At the conclusion of the mediation session, KIESEL informed PARADIS that he was willing to pay Salgueiro $120,000 to prevent her from publicizing the Salgueiro documents. Through PARADIS, Salgueiro countered that offer with a demand for $900,000 that would be open for 24 hours. On October 31, 2017, KIESEL told PARADIS that he rejected Salgueiro's $900,000 demand and would now offer $60,000 instead. PARADIS texted this new offer to Salgueiro, who texted both PARADIS and KIESEL that she would "c u both Dec. 4 at 2pm at CCW."

36. I have reviewed text messages between KIESEL, PARADIS, and Salgueiro which are substantively consistent with the above-referenced information.

b. November meetings with PETERS about Salgueiro

37. PETERS proffered the following information:

a. PETERS learned about Salgueiro's threats and demands from PARADIS during an in-person meeting with PARADIS and likely TUFARO on approximately November 16, 2017, after the first failed mediation with Salgueiro at LADWP headquarters.

b. At that initial meeting, the following took place:

i. PARADIS informed PETERS about the details of Salgueiro's demands, including that Salgueiro had threatened to reveal 1) certain attorney work-product documents that she had

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

taken from KIESEL's office, which included the *Jones v. PwC* draft complaint that the City was actively seeking to shield from production; 2) emails showing the transmittal of documents showing cooperation and coordination between the City and Jones' counsel (LANDSKRONER); 3) information that Salgueiro herself had filed the *Jones* lawsuit against the City (on behalf of KIESEL); and 4) other unidentified documents implicating cases involving the City.

ii. PETERS learned that KIESEL had engaged in a failed attempt to mediate Salgueiro's demands, and that this "mediation" had taken place at LADWP headquarters. PETERS felt that it was improper for the mediation to take place on City property.

iii. PETERS was "livid" to learn about the situation. He was particularly upset that KIESEL had not told him about Salgueiro's threats and demands, which PETERS felt that he had a need and a right to know.

iv. PETERS, PARADIS, and TUFARO agreed that they needed to have a discussion with KIESEL to talk about Salgueiro's threats and demands.

v. PETERS wanted to "impress on KIESEL the gravity of the situation."

vi. PARADIS told PETERS that KIESEL was not taking the situation seriously. PARADIS urged PETERS to be blunt in discussing the situation with KIESEL.

vii. PARADIS told PETERS that he "felt like a narc" for "ratting KIESEL out" and sharing this information with

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

PETERS without KIESEL's knowledge. PARADIS asked PETERS to "cloak" the fact that PARADIS was the source of the information. PETERS agreed to do so.

c. On November 17, 2017, PETERS sent KIESEL a series of text messages demanding that KIESEL come to his office immediately. KIESEL and PARADIS came to PETERS's office that day. At that November 17, 2017 meeting, the following occurred:

i. PETERS "read the riot act" to both KIESEL and PARADIS about the Salgueiro situation. PETERS included PARADIS to "cloak" the fact that he had learned the information from PARADIS, pursuant to PARADIS's request.

ii. PETERS asked KIESEL how KIESEL could not have shared the information with PETERS earlier. PETERS said that both PETERS and FEUER had a need and a right to know about Salgueiro's threats and demands, because this was an issue that could result in negative press coverage for the City Attorney's Office.

iii. PETERS, KIESEL, and PARADIS discussed the merits of Salgueiro's threats and demands, including the fact that Salgueiro was threatening to reveal documents relating to the *Jones* matter and other City litigation if KIESEL did not pay her money. PETERS recalled learning that Salgueiro was seeking "millions of dollars" from KIESEL.

iv. KIESEL was resistant to the idea of paying Salgueiro what she was asking. KIESEL told PETERS that he planned to hire a crisis-management person, an action that

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

PETERS considered ancillary to the City's more pressing concerns.

v. PETERS strenuously imparted to KIESEL that it was in his best interest to pay Salgueiro what she was asking to ensure that she did not make her information public.

vi. PETERS told KIESEL that if he did not take care of the situation, KIESEL would not be able to continue representing the City.

d. PETERS understood that Salgueiro had certain employment-related claims that she would agree not to pursue if KIESEL paid her to get the documents back. From PETERS's experience and his knowledge of Salgueiro, specifically her age, gender, ethnicity, termination after a medical leave for an allegedly work-related injury, and length of employment, PETERS believed that Salgueiro's employment claims might present a litigation risk for KIESEL.[13]

---

[13] Based on information provided by PETERS, KIESEL, PARADIS, and Salgueiro, I understand that Salgueiro was prepared to allege employment claims that included: 1) her termination after a lengthy medical leave; 2) unfulfilled promises that she believed KIESEL had made, including to pay for her to attend law school; and 3) KIESEL's general harsh or demanding treatment of her throughout her employment.

Based on that information and other information described herein, it is my belief that Salgueiro's threat to bring an employment lawsuit against KIESEL might have conferred a credible litigation risk to KIESEL and his firm. However, I further believe that such a lawsuit would not have been substantially damaging to the City. I also believe that the City's primary or sole concern in seeking to convince KIESEL —— who was reluctant to pay and willing to risk public revelation of all the information —— to pay to resolve Salgueiro's claims, was a desire to conceal the documents concerning the City's collaboration with Jones.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

e. PETERS viewed Salgueiro's demands as creating a "crisis situation" for himself and for the City Attorney's Office. PETERS believed that if the Salgueiro information were revealed, it would not only be embarrassing for the City Attorney's Office, but it would also implicate the candor of the process by which the *Jones* settlement had been approved. PETERS believed that the revelation of previously undisclosed cooperation between PARADIS/KIESEL and LANDSKRONER in the preparation of a complaint to sue the City could imperil the *Jones* settlement, including by providing objectors to the settlement with a foundation to reopen the objections that they had already unsuccessfully raised.

38. During CLARK's proffer, he advised the government that he was not familiar with any threats to reveal documents or information relating to the collusive litigation or demands for hush money, and that he did not recall ever receiving any such documents, information, or contacts. CLARK further advised that such events would have been significant and memorable in his opinion, and that he believed he would have recalled them if he observed them.[14]

---

[14] Multiple witnesses, including FEUER and CLARK, have advised that CLARK suffered from an [redacted] during a period that included 2017 and 2018, which affected CLARK's functionality at work and culminated with a medical [redacted] nd early 2019 [redacted]. CLARK advised the government that his [redacted] problem was resolved by February 2019, when he recommenced work. However, during the July 22, 2019 court-[redacted]ce, the FBI found approximately [redacted] hidden throughout CLARK's small office space. The government immediately advised FEUER of

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

39. Based on the foregoing and my knowledge of the investigation, I believe that CLARK, at some point, had some awareness of Salgueiro's threats, but may not have had a full understanding of the scope of the information that Salgueiro was threatening to reveal. I further believe that CLARK delegated handling of this situation to PETERS with an express directive that it be taken care of.

40. KIESEL advised the government as follows:

a. On November 17, 2017, KIESEL received a series of text messages from PETERS demanding that KIESEL come to see him immediately.[15]

b. KIESEL left a court proceeding in Orange County to drive to PETERS's office at City Hall East in Los Angeles, where he and PARADIS met with PETERS.

c. During that meeting, PETERS was visibly angry and told KIESEL to make the problem go away or KIESEL and PARADIS would be fired. PETERS told KIESEL and PARADIS that Salgueiro

that discovery. [redacted]

[15] I have reviewed text messages between PETERS and KIESEL on that date that corroborate this information.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

had called the City Attorney's Office asking to speak with FEUER, that FEUER had not taken the call, and that the call was routed to CLARK, who re-routed the call to PETERS and directed him to handle it. KIESEL further advised that his sense was that CLARK did not have a full awareness of the situation, and that KIESEL did not recall any in depth conversations with CLARK about Salgueiro.

d. During the meeting, PETERS told KIESEL to do "whatever it takes" and "whatever it costs," which KIESEL understood as a directive to pay whatever Salgueiro was asking to buy her silence.

e. KIESEL believed that Salgueiro had a "legitimate severance demand" based on her employment with him. However, KIESEL did not see any issues with the prospect of the Salgueiro documents being publicly revealed, because the City was fully aware of what those documents contained, and KIESEL did not think they would make the City look bad.

f. KIESEL was reluctant to pay what Salgueiro was asking, but he did not want to be fired from the Special Counsel role, particularly after investing substantial time and resources into the case of *City of Los Angeles v. PwC* over approximately three years without any compensation (because the Special Counsel contract provided for compensation for KIESEL and PARADIS only on a contingency-fee basis). KIESEL had by that time spent approximately a quarter million dollars of his own money on costs associated with the case, which contributed to his desire to remain on the case to recoup that investment.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

g. KIESEL could not recall whether PETERS told him that FEUER was aware of Salgueiro's threats and demands, but he believed that PETERS and CLARK would have told FEUER. Based on the circumstances and relationships that KIESEL observed, he "could not imagine" that CLARK and PETERS would not have told FEUER about this situation, because they were "good soldiers" to FEUER.

41. KIESEL further advised the government that after the aforementioned meeting wherein PETERS threatened to fire him, he subsequently met with PETERS again, and that PETERS had calmed down. At that time, PETERS indicated that he would not terminate the contract, and that they would see what happened.

42. KIESEL advised the government that since approximately 1980, he has regularly kept a handwritten diary on noteworthy events in his life. KIESEL showed the government (and provided a copy of) an entry in his diary that was dated December 1, 2017, that appears to recount KIESEL's recollection of the above-described November 2017 meeting in which PETERS called KIESEL up from Orange County to discuss Salgueiro's threat. According to the entry, which described PETERS as "spitting MAD" (emphasis in original), PETERS told KIESEL, "How could you not tell me about this threat, Paul??" The entry further reports, "Thom [PETERS] said you have 2 choices. Either settle with J [Salgueiro] or your FIRED!" (emphasis in original).

43. The above-described diary entry provided by KIESEL dated December 1, 2017, further related KIESEL's efforts to address and resolve Salgueiro's demands following his meeting

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

with PETERS. It then stated as follows: "Last Wed [November 29, 2017], I met, again, with Thom [PETERS] + laid all of this out and thankfully he understood + indicated he would not terminate us + we'll see how things develop."

44. I believe that the contemporaneous information from KIESEL's handwritten diary related herein is consistent with the information provided herein and other evidence described herein as to events surrounding Salgueiro's threat.

45. PARADIS proffered the following relevant information:

a. After Salgueiro's warning that she would see them at the *PwC* hearing, PARADIS grew concerned that the situation with Salgueiro was "rapidly escalating out of control" and that PETERS needed to be apprised of the details.

b. On November 6, 2017, PARADIS left a voicemail for PETERS advising that there were a couple of matters they needed to discuss and asking to meet.[16]

c. On November 16, 2017, PARADIS and TUFARO met with PETERS in PETERS's office and informed PETERS of the status of the Salgueiro situation, including that she was threatening to reveal documents relating to her employment-related claims as well as documents showing potential conflicts in the *Jones* case and other cases. PARADIS related the following relevant information about that meeting:

i. PETERS described CLARK's involvement in the Salgueiro matter, as detailed above.

[16] PETERS's phone does not reflect such a voicemail on that date; rather, it reflects a text message from PARADIS asking for a meeting with PETERS.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

ii. PETERS discussed the merits of Salgueiro's employment claims and noted that he had witnessed first-hand KIESEL's treatment of Salgueiro when PETERS worked at KIESEL's firm.

iii. PETERS stated that KIESEL had been primarily responsible for PETERS's wife being appointed as a Superior Court judge, because KIESEL had exerted his influence in the selection process. PETERS further shared his goal to also be appointed as a judge after leaving the City Attorney's Office, and he stated that he was aware of KIESEL's influence over that process as a member of the Governor's Committee that recommended candidates for judgeships, which was a factor in PETERS wanting the matter resolved promptly without becoming public.

iv. PETERS and PARADIS discussed a variety of approaches and then agreed that PETERS should text KIESEL the following morning to tell KIESEL that PETERS urgently wanted to see him in his office. They further agreed that KIESEL should not be informed that PETERS and PARADIS had met on November 16, 2017. At PARADIS's urging, they also agreed that PETERS should "take a very stern approach" with KIESEL, demand that he resolve the situation with Salgueiro, and threaten KIESEL with termination as Special Counsel if he did not do so. They did not discuss invoking FEUER's name as part of such an approach.

d. After their meeting on November 16, 2017, PETERS called PARADIS that evening to further discuss the planned conversation with KIESEL.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

e. On the morning of November 17, 2017, PARADIS left a voicemail for PETERS and subsequently received a call back from PETERS. PETERS stated that he was going to text KIESEL and PARADIS as they had previously discussed.[17]

f. Later that day, PARADIS and KIESEL met with PETERS in PETERS's office. During that November 17, 2017 meeting, the following took place:

i. PETERS did not disclose to KIESEL that he had met with PARADIS and TUFARO the day before about the Salgueiro matter.

ii. According to PETERS, he had learned from CLARK that CLARK had received from Salgueiro a package and two phone calls requesting a meeting. PETERS relayed that CLARK had advised him as follows: [18]

(I) CLARK was "fucking pissed" about the fact that Salgueiro had brought this to CLARK's attention, and CLARK had not responded because he did not intend to meet with Salgueiro.

(II) CLARK told PETERS that he wanted KIESEL's situation with Salgueiro resolved so that it did not become public.

---

[17] According to the phone records, PETERS had already begun texting KIESEL by the time PARADIS said that he had this conversation with PETERS.

[18] PETERS proffered that he could not remember discussing the Salgueiro matter with CLARK before the settlement was paid, but did specifically remember a conversation with CLARK about it after the matter was resolved.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

(III) CLARK asked PETERS what Salgueiro was complaining about specifically, and PETERS explained to CLARK that Salgueiro was complaining about KIESEL "having been on both sides of several cases" related to the approximately six cases reflected in the documents that Salgueiro had provided in her package to CLARK.

(IV) PETERS stated his understanding that at least two of the cases on which Salgueiro was threatening to reveal information were litigation with the City, and that one was the *Jones v. City* case.

iii. PETERS advised that he had already informed FEUER about this situation. PETERS stated that FEUER was extremely unhappy about it, and that if it was not immediately cleaned up, KIESEL's firm, and probably PARADIS's firm too, would be terminated as Special Counsel to the City in the *PwC* case.

iv. KIESEL was resistant and stated that Salgueiro was unreasonable, that he was not prepared to pay her $900,000, and that he viewed her threats as extortion.

v. PETERS stated that while he understood Salgueiro was demanding a large amount of money, PETERS, FEUER, and CLARK had no choice but to demand that KIESEL work out a deal with Salgueiro to pay her because the City Attorney's Office could not tolerate this situation becoming public.

vi. PETERS ended the meeting by firmly directing KIESEL to work out a deal with Salgueiro to buy her silence and ensure that her information did not become public. PETERS also

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

again made clear that if KIESEL did not comply quickly, he, and likely PARADIS also, would be terminated.

46. PARADIS proffered that after the November 17, 2017 meeting, KIESEL left, and PETERS stopped PARADIS on the way out to instruct PARADIS to reiterate to KIESEL what was going to happen if KIESEL did not agree to pay Salgueiro off. PARADIS indicated that he would do so.

47. PARADIS proffered that at the time of the November 17, 2017 meeting, PARADIS was unsure as to whether PETERS had truly informed FEUER about Salgueiro's threats, or whether that was simply a tactic that PETERS was using to try to convince KIESEL to comply. However, PARADIS did not think that PETERS would take the actions he did without apprising FEUER, because PETERS was afraid of FEUER and would have wanted to "cover his ass."[19]

c. PETERS's November discussions with FEUER and BRAJEVICH about Salgueiro's threats and demands

48. PETERS proffered that at some point after the aforementioned November 17, 2017 meeting and before December 1, 2017, PETERS spoke with FEUER as another meeting was breaking up. PETERS provided the following relevant information as to that conversation:

a. PETERS did not specifically recall whether anyone else was present during this conversation, but he believed that

[19] As noted below, PARADIS proffered that PETERS later confirmed to him that he in had in fact informed FEUER about Salgueiro's threats and demands.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

KAPUR was probably present, and that Robert Wilcox (FEUER's media spokesman) might have been there as well.

b. During this conversation, PETERS told FEUER that a disgruntled former employee of KIESEL's was threatening to reveal documents including the draft *Jones v. PwC* complaint, which FEUER was then aware was the subject of a contested motion to compel in the *PwC* case, as well as other documents showing cooperation and coordination between PARADIS and Jones' counsel (JACK LANDSKRONER) before the *Jones* complaint was filed that had not previously been disclosed to PwC or the court. According to PETERS, FEUER was already aware that there had been some cooperation between PARADIS and the plaintiff's counsel.

c. PETERS advised FEUER that the former employee seemed irrational, was being guided by a "guru," and was "holding the City hostage" by threatening to reveal these documents, which PETERS characterized as the City's attorney work product.

d. PETERS provided this information as a "heads up" to FEUER, as PETERS knew that FEUER always wanted to be made aware of matters that might be reported in the press.

e. FEUER was upset by this information and questioned how KIESEL could have let this happen.

f. It was apparent to PETERS that FEUER, whom PETERS characterized as "a very smart man," immediately saw the risk to the City inherent this situation.

g. PETERS assured FEUER that PETERS was monitoring the situation.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

49. PETERS proffered that on November 30, 2017, PETERS received a call from BRAJEVICH, and they spoke on the phone.[20] PETERS had not told BRAJEVICH about the Salgueiro situation, but BRAJEVICH already had some awareness of it, including the fact that KIESEL and PARADIS had attempted to mediate the dispute with Salgueiro at LADWP headquarters. PETERS proffered the following with respect to that conversation:

a. BRAJEVICH asked PETERS how much PETERS knew about the Salgueiro situation, and PETERS gave BRAJEVICH some details about her threats and demands.

b. PETERS told BRAJEVICH that he was scheduled to discuss the issue with FEUER the following day (Friday, December 1, 2017), and he invited BRAJEVICH to join that discussion.

c. PETERS believed that BRAJEVICH needed to be involved in the discussions about Salgueiro's threats and demands, for two reasons. First, BRAJEVICH was effectively supervising KIESEL's and PARADIS's work on the matter to which Salgueiro's threats related. Second, LADWP headquarters, where the failed "mediation" had taken place, was BRAJEVICH's "domain" (as LADWP General Counsel).

d. The December 1, 2017 meeting with FEUER, KAPUR, BRAJEVICH, and PETERS about Salgueiro

[20] I have reviewed an email from this date to PETERS from his secretary requesting that PETERS call BRAJEVICH. As described below, a subsequent meeting invitation indicates that BRAJEVICH was scheduled to telephonically join a previously scheduled December 1, 2017 meeting with FEUER, KAPUR, and PETERS on the *PwC* case.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

50. PETERS proffered that on Friday, December 1, 2017, PETERS participated in a scheduled meeting with FEUER, KAPUR, and BRAJEVICH (called in) to provide an update on the Salgueiro situation.[21] PETERS proffered the following information about this December 1 meeting:

a. The Salgueiro situation —— which PETERS described as "the issue du jour" at that time, in light of Salgueiro's looming threat to appear at the Monday, December 4 hearing —— was the primary or sole focus of that planned meeting.

b. The meeting took place at the end of the day in FEUER's office.

c. BRAJEVICH was not present in person but instead called in to the meeting to participate by telephone.

d. PETERS provided an "update on the state of play" of the Salgueiro situation, including that Salgueiro still had the documents showing cooperation between the City and Jones, and that Salgueiro had threatened to appear at the hearing set for Monday, December 4, 2017.

e. The participants discussed the likelihood that if Salgueiro appeared at the hearing, she would try to file or give the documents.

---

[21] As noted herein and detailed below, I have reviewed a calendar entry for FEUER and a meeting invitation reflecting this meeting from 4:45 p.m. to 5:00 p.m. PETERS proffered that he could not recall whether anyone else attended this meeting. He opined that FEUER's press spokesman, Rob Wilcox, [redacted] ave here" if available. PETERS also stated that [redacted], FEUER's Chief of Intergovernmental Relations, might also have attended. As noted herein, documents reflecting the scheduling of this meeting do not indicate that either Wilcox or [redacted] was invited.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

f. The participants discussed the possibility that Salgueiro would invite the press to attend the hearing in order to publicize the information to the media.

g. FEUER and BRAJEVICH expressed frustration that KIESEL had not been able to take care of the problem and reach an "accommodation" with Salgueiro.

h. FEUER stated that KIESEL needed to do whatever needed to be done to take care of the situation.

i. Accordingly to PETERS, it was "absolutely clear" and understood by all participants at this meeting that Salgueiro was demanding money from KIESEL in exchange for the return of the documents.

j. PETERS told FEUER that he would personally attend the Monday hearing, in light of Salgueiro's threat to show up. FEUER did not ask PETERS to attend the hearing, but PETERS preemptively offered because he knew from his prior experience with FEUER that this was what FEUER would want.

k. FEUER conveyed that he was confident that PETERS could handle the situation.

l. Both FEUER and BRAJEVICH expressed the view that it was outrageous that the "mediation" had happened on City property.

51. According to an electronic calendar entry, there was a scheduled meeting regarding the *PwC* case between FEUER, KAPUR, PETERS, and BRAJEVICH on December 1, 2017, from 4:45 p.m. to 5:00 p.m. The meeting notice specified that BRAJEVICH would be participating by phone.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

52. In a text message on December 1, 2017, at 5:07 p.m., using **BRAJEVICH's ACCOUNT**, BRAJEVICH said to PETERS, "Thom- when you have a chance **I want to follow on the fact that the mediation took place at DWP**. Not urgent and can wait until Monday. Thanks and have a great weekend." Metadata from PETERS' phone indicates that PETERS opened this message at 9:19:10 p.m on that same date.

a. PETERS proffered that he understood this to refer to KIESEL's attempted "mediation" with Salgueiro on LADWP property, which he and BRAJEVICH and others had discussed in the aforementioned meeting that afternoon.

53. In a text message on December 1, 2017, at 9:18:57 p.m., PETERS told PARADIS, **"Mike is not firing anyone at this point. But he is far from happy about the prospect of a sideshow. Also, mediating Paul's matter at DWP, not a popular move.** We can speak over the weekend. Thanks."[22]

a. PETERS has informed the government that this message meant to convey that FEUER had considered and then rejected the idea of firing PARADIS and KIESEL, but that FEUER considered the threatened release of documents by SALGUEIRO to be a prospective "sideshow" that would impair both the litigation and the reputation of FEUER's office. The "sideshow" was a reference to media attention.

[22] Based on my general knowledge of text messaging services, I am aware that a user receiving a text message can often see a banner containing part or all of a message without opening the message. Based on the sequence of events and timing of these messages, I believe PETERS may have viewed BRAJEVICH's message via such a banner, sent the related message to PARADIS, and then opened BRAJEVICH's message in order to reply to it.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

54. Based on my knowledge of the investigation and the above-described information and timeline, I believe that the "mediation at DWP" discussed in the BRAJEVICH-PETERS and PETERS-PARADIS texts, both from December 1, 2017, referenced KIESEL's unsuccessful attempts to negotiate Salgueiro's demands for hush money, as directed by PETERS at FEUER's implied direction.

55. I further believe that BRAJEVICH's message to PETERS — — which BRAJEVICH sent seven minutes after his meeting with FEUER, KAPUR, and PETERS about the *PwC* matter was scheduled to end, and which asked to "follow on the fact that the mediation took place at DWP" —— suggests that this topic of KIESEL's dispute with Salgueiro and its bearing on the City's interest in the *PwC* case was likely discussed at that meeting. This belief is supported by the language selected by BRAJEVICH. In particular, I believe that BRAJEVICH's request indicated his intent to "follow on" an existing discussion. Moreover, BRAJEVICH's lack of any explanation or background as to what "mediation" he meant suggests to me that BRAJEVICH and PETERS had recently discussed this topic. Finally, I note the fact that his text message identifies two separate but related issues, likely from the meeting: (1) the "sideshow" and (2) "also" the location of the "mediation."

56. PETERS proffered that in one of his multiple conversations with FEUER about the Salgueiro situation, FEUER questioned whether KIESEL should be fired for allowing this to happen, but FEUER ultimately did not decide to terminate KIESEL or PARADIS.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

57. PETERS proffered that in one of his multiple conversations with FEUER about the Salgueiro situation before the settlement, PETERS believed that he conveyed to FEUER that Salgueiro was "looking for seven figures," meaning that Salgueiro was demanding a million dollars or more.

e. *Settlement of Salgueiro's demands on December 4, 2017*

58. Information from multiple witnesses and documents indicate that on December 4, 2017, Salgueiro made good on her above-described threat to appear at a court hearing in the PwC matter and attempted to provide copies of the Salgueiro documents both to the court and to the counsel for PwC. The evidence provides probable cause to believe that after Salgueiro showed up in court and attempted to provide her documents to the court and PwC's counsel in the presence of PETERS, PETERS directed KIESEL to settle with Salgueiro and was later informed that KIESEL had done so by paying $800,000 in hush money.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

[redacted]

62. PETERS, KIESEL, and PARADIS each (separately) advised the government substantively as follows:

a. PETERS, KIESEL, and PARADIS all attended the aforementioned *PwC* hearing in the LADWP billing litigation.[24]

b. At or after the hearing, Salgueiro approached [redacted], which PETERS, KIESEL, and PARADIS interpreted as a signal that Salgueiro was prepared to carry out her threat to reveal her information.

---

[23] [redacted] confirmed to the government that the described incident took place (he was not certain of the hearing date but believed it to be in that general time frame).

[24] PARADIS proffered that PETERS told him that he was attending the hearing at the express direction of FEUER. PETERS proffered that he told FEUER that he would attend the hearing, because he knew that FEUER would have wanted him to do so, and would have asked him to do so had he not preemptively volunteered.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

c. PETERS, KIESEL, and PARADIS reconvened in PETERS's office after the hearing, and they agreed that KIESEL would met with Salgueiro for the purpose of doing whatever he needed to do to resolve the situation and ensure that she did not reveal her information.

d. KIESEL met with Salgueiro later that day and agreed to pay her $800,000 in exchange for the return of her information and her assent to a confidentiality agreement.

63. Text messages between PETERS and KIESEL reflect the following exchange from December 4, 2017, with times indicated in brackets:

> KIESEL: I am parked on the north west corner of 1st and Los Angeles Street. [12:13 p.m.]
>
> PETERS: I'm with Paradis. Can u come to my office now to meet? [3:06 p.m.]
>
> KIESEL. Yes. [redacted] is at the elevator engaging J [Salgueiro] so [redacted] and I are stuck. Will come down as soon as we can. [3:07 p.m.]
>
> PETERS: She gave [redacted] her card. [3:09 p.m.]
>
> KIESEL: You waiting for me or going back with Paul [3:09 p.m.]
>
> PETERS: Tried to file a bunch of docs. I'm with Paradis. [3:11 p.m.]
>
> KIESEL: Going back to City Hall? I will meet you there if you go with Paul. [3:12 p.m.]
>
> PETERS: Yes. My office please. I will get you parking. [3:14 p.m.]
>
> KIESEL: Thanks. [3:14 p.m.]
>
> PETERS: **Settle the case if you can! I need you to take care of this.** We are in my office. [3:40 p.m.]

> KIESEL: On my way up now will be there in three minutes. [3:59 p.m.]
>
> KIESEL: I am meeting Julissa tonight at 7:30 PM. With [redacted] **Will get this done**. [6:09 p.m.]
>
> KIESEL: **Deal with J at 800. 450 within 7 days. Have 150 in sixty days balance by May 1.** She will work with attorney [redacted] as her counsel. **Will return all documents when completed. Oyyy** [9:15 p.m.]
>
> PETERS: **Good job. Be sure there is a confidentiality agreement of a sort that would make Marty Singer envious.** [11:43 p.m.]

64. PETERS and KIESEL both (separately) advised the government that these texts corroborate the above-described information that PETERS attended this hearing in the LADWP billing litigation; that Salgueiro showed up at the hearing following her threat to do so if KIESEL did not pay her; that Salgueiro's actions led to KIESEL renewing negotiations to pay Salgueiro $800,000 —— a dramatic increase from KIESEL's previous counteroffer of $60,000 —— in exchange in exchange for her silence and her assent to a confidentiality agreement; that KIESEL advised PETERS of the terms of the settlement; and that PETERS directed KIESEL to obtain a strong confidentiality agreement.

65. I believe that KIESEL's text message, "**Deal with J at 800. 450 within 7 days. Have 150 in sixty days balance by May 1,**" reflects his description to PETERS of his agreement to pay Salgueiro $800,000. This understanding is consistent with information separately provided by both PETERS and KIESEL as to their respective intents and understanding of this message.

66. I believe that PETERS's text message, "**Good job. Be sure there is a confidentiality agreement of a sort that would**

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

make Marty Singer envious," reflects PETERS's endorsement of KIESEL's decision to pay Salgueiro $800,000 to buy her silence as to the City Attorney's Office's litigation practices, and to obtain a strong and enforceable confidentiality agreement. I am aware from open-source media reports that Marty Singer is a prominent Hollywood-based attorney who is known for aggressive tactics including the use and enforcement of strong confidentiality agreements. This understanding is consistent with information separately provided by both PETERS and KIESEL as to their respective intents and understanding of this message. Moreover, based on my experience and knowledge of the investigation, the fact that the City (as conveyed by PETERS) was more concerned with the confidentiality portion of the agreement than its financial terms strongly suggests that the City's primary interest in the hush money payment was to buy Salgueiro's silence because of its potential damage to the City.

67. KIESEL and PARADIS both advised the government that after the confidential settlement agreement between KIESEL and Salgueiro was formalized, KIESEL paid Salgueiro $800,000, and PARADIS paid KIESEL $400,000.[25]

68. [redacted] participated in a voluntary interview with the prosecution team and advised as follows:

[25] According to PARADIS, the money that he contributed came from his own funds, and he did not inform PETERS that he had contributed to the settlement. According to PETERS, he believed, based on information later provided to him by PARADIS, that some portion of the settlement was paid by LANDSKRONER. Information from PARADIS and LANDSKRONER and review of their financial records does not indicate any such direct contribution by LANDSKRONER.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. [redacted] had no prior involvement in or knowledge of the issue before KIESEL asked him to attend the December 4, 2017 hearing and intervene with Salgueiro on KIESEL's behalf. [redacted] was aware that the hearing must have some significance to KIESEL but didn't know what it was. [redacted] understood that Salgueiro had taken some papers from KIESEL's office regarding a case, and that KIESEL wanted [redacted]'s help in getting them back. [redacted] volunteered his services and did not get anything in return.

b. At the hearing, [redacted] observed Salgueiro unsuccessfully attempt to give some papers to the court clerk.

c. Following the hearing, [redacted] saw Salgueiro approach [redacted], counsel for PwC, speak with him briefly, and take his business card.

d. [redacted] asked Salgueiro to meet with him and KIESEL over dinner, and she agreed. Salgueiro brought along her friend, Rosa (last name unknown to [redacted]). [redacted] could not recall the details of the negotiation session, but it was relatively short. KIESEL balked at paying the full amount that Salgueiro was demanding because he didn't have access to those funds at that time, and he asked if she would agree to a payment plan. [redacted] believed that they ultimately settled on approximately $800,000.

e. [redacted] knew PETERS from PETERS's tenure at KIESEL's firm, but they were not close. From the time that PETERS accepted a job with FEUER at the City Attorney's Office, it was [redacted]'s belief that PETERS intended to follow FEUER when FEUER proceeded to higher political offices after his tenure as City

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Attorney. [redacted] did not have further evidentiary support for his opinion and stated that it was just [redacted]'s belief.

f. PETERS's post-settlement report to FEUER that KIESEL had paid Salgueiro to resolve her threats and demands, and PETERS's post-settlement discussions of the situation with BRAJEVICH and CLARK

69. PETERS proffered that he did not recall reporting these events to FEUER on the day of the December 4, 2017 hearing, which PETERS described as "very unusual" given how concerned and focused FEUER was with respect to Salgueiro's threat to appear at the hearing that day if she did not receive the money she was demanding.

70. PETERS proffered that shortly after the December 4, 2017 hearing (likely on December 5, 2017, but PETERS was unsure of the exact date), PETERS met with FEUER in person, and the following took place:

a. PETERS reported to FEUER that KIESEL had "stepped up" and "reached an accommodation" with Salgueiro.

b. PETERS advised FEUER that settling the matter had "cost KIESEL a ton of money."

c. PETERS confirmed to FEUER that the City would get its documents back as the result of the settlement with Salgueiro, and that they would not be made public.

d. FEUER responded favorably, telling PETERS that this was "great" and that PETERS had done "good work" in facilitating the settlement.

e. FEUER did not ask PETERS for further details of the settlement, and PETERS did not provide them.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

71. PETERS proffered that he was "quite sure" that he would not have advised FEUER after the settlement as to the specific amount that KIESEL had paid, because FEUER would not have been interested in the dollar figure. Rather, FEUER's concern was that the threat of the documents being exposed had been mitigated.

72. PARADIS proffered that around the time of the December 4, 2017 *PwC* hearing where Salgueiro appeared in court (as described in more detail elsewhere), PETERS confirmed to PARADIS that he had in fact —— as PETERS had previously maintained —— told FEUER about Salgueiro's threats, including the nature of the material that she was threatening to reveal.[26] After PETERS confirmed that he had told FEUER about the Salgueiro threats and demands, PETERS also stated that FEUER knew about the "mediation" of her demands taking place on LADWP property, and that FEUER was "pissed" about it.

73. I believe that FEUER's reported displeasure about the use of LADWP headquarters as the venue for the mediation, as described herein, related to the fact that it linked the City to the mediation of Salgueiro's demands, which would, if discovered, cast the City in a negative light.

74. PETERS proffered that at some point after KIESEL settled the matter with Salgueiro, PETERS discussed it with CLARK. PETERS advised that he did not recall the specifics of

[26] PARADIS further advised that he believed that, based on what he knew of PETERS, PETERS indeed told FEUER about the looming threat, because PETERS would not have wanted to risk FEUER being blindsided if "all hell broke loose" and Salgueiro in fact went public with her information.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

that conversation, and he did not know whether CLARK had details about the Salgueiro matter. PETERS also advised that he could not recall whether he had other conversations with CLARK about the Salgueiro matter.

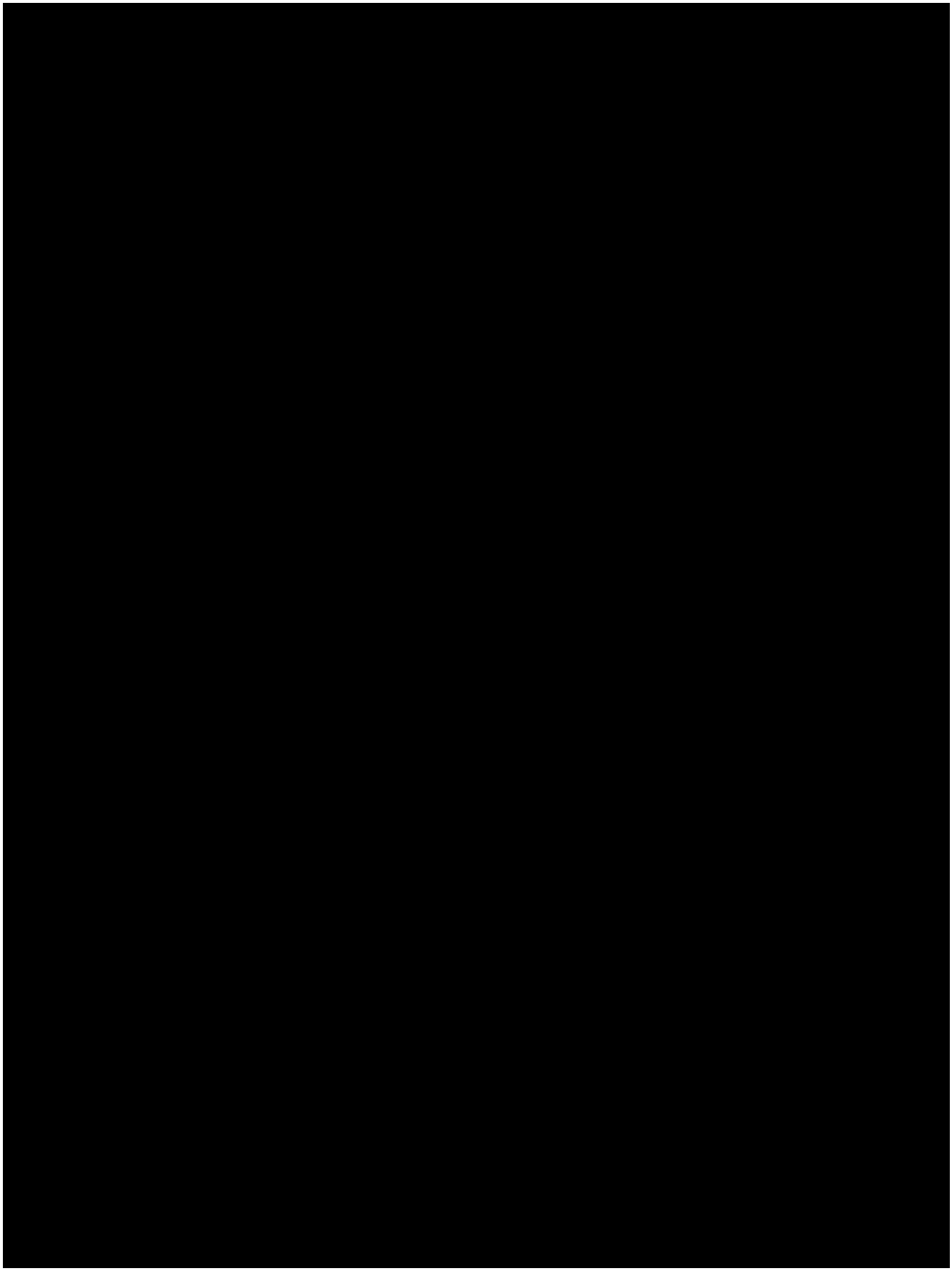
75. PETERS proffered that at some point after KIESEL settled with Salgueiro, PETERS and BRAJEVICH spoke again about the matter.

[redacted]

[redacted]

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB



Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

[redacted]

79. Based on the foregoing, I believe there is probable cause to believe that FEUER was in fact aware of Salgueiro's threats to reveal information about the City Attorney's Office's litigation practices unless she were paid for her silence, [redacted] Specifically, my belief is based on:

a. PETERS's proffered information that he advised FEUER about the details and context of Salgueiro's threats and demands, that FEUER was very upset and contemplated firing Special Counsel, and that FEUER expressed to PETERS that KIESEL needed to take care of the matter, which PETERS understood to mean that FEUER wanted him to make sure that KIESEL paid Salgueiro to ensure that the information was not revealed.

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. PARADIS's information that at their meeting on November 17, 2017, PETERS told him that he had notified FEUER of Salgueiro's threats, and that FEUER was very upset about the situation.

c. KIESEL's information that PETERS would fire him if he did not settle with Salgueiro, and that he believed PETERS would likely have discussed the matter with FEUER before making such a threat.

d. KIESEL's contemporaneous diary entry corroborating the information provided by both KIESEL and PARADIS that PETERS had threatened to fire KIESEL if he did not settle with Salgueiro.

e. The December 1, 2017 text message from PETERS to PARADIS stating, "Mike is not firing anyone at this point. But he is far from happy about the prospect of a sideshow. Also, mediating Paul [KIESEL]'s matter at DWP, not a popular move." In addition to PETERS's explanation that this message meant that FEUER had considered but rejected the idea of firing Special Counsel, and that he was displeased about the matter, I believe that this message corroborates the substantively consistent information from PETERS, PARADIS, and KIESEL, and from KIESEL's diary entry, as described above.

f. The December 1, 2017 text message from BRAJEVICH to PETERS asking to discuss "the fact that the mediation took place at DWP," the timing of that message contemporaneous to the above-described message from PETERS to PARADIS relating FEUER's displeasure with the situation and the fact that using LADWP as

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a venue for the mediation was "not a popular move," and BRAJEVICH's relationship with FEUER.

g. PETERS's proffered information that FEUER was aware that the "mediation" had taken place at LADWP, and that FEUER was displeased with that fact.

h. PARADIS's proffered information that PETERS had informed him that FEUER knew that the "mediation" of Salgueiro's demands had taken place on LADWP property, and that FEUER was "pissed" about it.

i. PETERS's proffered information that he discussed the matter with FEUER again after the settlement and advised that KIESEL had "stepped up" and settled the matter with Salgueiro, and that the resolution had "cost KIESEL a ton of money."

j. PARADIS's proffered information that shortly after KIESEL reached a settlement with Salgueiro on December 4, 2017, by agreeing to pay her $800,000, PETERS confirmed to PARADIS that PETERS had in fact told FEUER about Salgueiro's threats, including the nature of the material that she was threatening to reveal.

80. I believe that the above information, taken together, constitutes probable cause to believe that [redacted] FEUER not only was aware of Salgueiro's threats and demands, but he impliedly directed PETERS to ensure that KIESEL settled those demands by paying a large sum of hush money.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

B. [redacted]

81. As further described below, the evidence provides probable cause to believe that in January 2019, PETERS apprised FEUER that KIESEL and PARADIS had documents responsive to PwC's court-authorized discovery demand that would be damaging to the City. Specifically, according to multiple sources of evidence — — including a contemporaneous recorded conversation wherein PETERS recounted his recent conversations with FEUER —— PETERS told FEUER that the documents would reflect previously undisclosed coordination between Special Counsel and Jones's counsel, JACK LANDSKRONER, in filing the *Jones v. City* complaint, including potentially the fact that Special Counsel acting on behalf of the City had drafted the *Jones v. City* complaint.

82. According to PETERS, FEUER was very upset, reacted with extreme shock and dismay, and stated that the revelation of those facts would be a "catastrophe." Based on that interaction and his experience with FEUER, PETERS understood from their discussions that FEUER wanted PETERS to ensure that the documents were not produced or otherwise revealed. KIESEL and PARADIS both sent the documents to PETERS as discussed, but PETERS, at the perceived direction of FEUER, did not produce the documents to PwC or alert the state court or anyone else of their existence. Instead, PETERS, at FEUER's direction, appeared at a hearing in the *PwC* case and represented to the

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

state court that "there were documents that were requested of the City through that PMQ deposition notice.[28] We will be producing those documents."

83. As further detailed below, the evidence indicates that the documents that KIESEL sent to PETERS —— which were responsive to the PMQ document demand and which FEUER and PETERS knew would be damaging to the City's litigation position and the City Attorney's Office's, specifically including FEUER's, reputation —— eventually surfaced during a review of PETERS's hard drive that was directed by Browne George, the City's outside counsel. FEUER made official statements to the prosecution team [redacted] on this topic, along with various public statements and filings and sworn civil deposition testimony. The evidence provides probable cause to believe that FEUER's [redacted] official statements to the government were knowingly misleading, in that he did not first learn of the information revealed in the KIESEL Emails in late April 2019, which is when the KIESEL Emails were independently discovered and a need arose for FEUER to publicly address it. In fact, FEUER learned of this information months earlier, namely, not later than January 2019, after which he impliedly directed their concealment. Based on my training, experience, and knowledge of this investigation, I believe FEUER had a strong incentive to personally distance

[28] In California civil litigation, a PMQ deposition requires the "person most qualified" at an entity to testify on behalf of the entity as to certain relevant facts either known to the deponent or gathered through the deponent's investigation.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

himself from any knowledge of the collusive litigation for his own political gain (or to avoid political fallout).

1. The evidence indicates that FEUER, along with KAPUR and BRAJEVICH, learned about the KIESEL Emails in January 2019

84. On the afternoon of January 23, 2019, a hearing took place in the *PwC* case. According to the transcript of the hearing, the judge overruled the City's privilege objections to documents demanded by PwC and ordered the City to submit a "person most qualified" ("PMQ") to represent the City at a deposition. The judge further expressed concerns about the City's privilege assertions and related conduct, and asked KIESEL, who was representing the City at the hearing, to "bring these matters not only to the attention of the internal affairs department, if there is such a department, but also to bring it to the attention of the City Attorney, Mike Feuer, directly."

85. On January 23, 2019, at 4:59 p.m., BRAJEVICH (using **BRAJEVICH's ACCOUNT**) sent PETERS a text message stating, "Lets talk before you speak with mike [FEUER]." BRAJEVICH and PETERS exchanged additional text messages and agreed to speak the next day.

86. At 6:52 p.m. on January 23, 2019, PETERS sent an email to FEUER at **FEUER's EMAIL**. In the email, PETERS summarized the hearing, including the judge's invocation of FEUER's name. PETERS stated that **"[Judge] Berle is now aware of communications between Paradis and Landskroner about the latter taking over Mr. Jones' contemplated case against PwC, and the fact that such representation soon evolved into *Jones v. DWP*."** PETERS further

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

noted that the court "was wondering aloud today whether the *Jones* settlement is somehow vulnerable to being reevaluated due to possible conflicts by Paradis." PETERS opined that there were no ethical lapses by the City, but that they should discuss the matter soon. PETERS suggested a meeting with just PETERS, FEUER, and KAPUR, but he offered to involve PARADIS, KIESEL, or BRAJEVICH if FEUER so desired.

87. At 7:02 p.m. on January 23, 2019, FEUER replied from **FEUER's EMAIL** with a brief email directing PETERS to set up a meeting for January 25, 2019, with PETERS, FEUER, and KAPUR. Later that evening, PETERS replied that he had done so.

88. At 7:06 p.m. on January 23, 2019, FEUER (using **FEUER's EMAIL**) again replied to PETERS's original email, stating, "Although it may be too late to fix all this, it may be a good idea to have someone from our office at the next hearing before Judge Berle." Later that evening, PETERS replied, "I'll be there."

89. On January 24, 2019, KIESEL forwarded to PETERS, TUFARO, and BRAJEVICH (at **BRAJEVICH's EMAIL**) an email from counsel for PwC regarding the City's PMQ document and production of outstanding documents. PETERS replied to all asking whether the City owed documents to PwC, and indicating that if so, it should produce them. KIESEL forwarded the email to PARADIS, who replied to all stating, "Yesterday when we met with Thom [PETERS] (with Joe B. [BRAJEVICH] on the phone), Thom directed us to research and draft a writ to be filed in the very near future." PARADIS opined that the City should await resolution

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

of the writ before proceeding with either the PMQ deposition or the document production. PETERS replied to all asking when the writ could be ready, TUFARO replied with a projected date, and PETERS replied with an acknowledgement.

90. PETERS proffered that on January 24, 2019, he met with PARADIS, and the following took place:

a. PARADIS appeared very upset about the events that were unfolding in the *PwC* case, and he told PETERS, "I'm not going to go down for this bullshit."

b. PARADIS told PETERS that not only had PARADIS aided LANDSKRONER in the drafting of the *Jones v. City* complaint, but PARADIS had in fact personally drafted both the complaint and the settlement demand letter. PARADIS further advised that "everyone" at the City knew about this, including CLARK, DAVID WRIGHT, LADWP Board President MELTON EDISES LEVINE, Assistant City Attorney Eskel Solomon, and others.

c. PETERS told PARADIS that he wanted to review the documents that would reflect these facts.

91. On January 25, 2019, at 8:03 a.m., BRAJEVICH (using the **BRAJEVICH's ACCOUNT**) left a voicemail for PETERS indicating that BRAJEVICH had sent PETERS a couple of emails relating to two declarations filed by LANDSKRONER. BRAJEVICH stated that he had concerns about the declarations, specifically; 1) in a section denying any relationships with counsel in the case, LANDSKRONER omitted reference to PARADIS; and 2) LANDSKRONER stated that he had started working on the case in November 2014, which was inconsistent with the City's timelines in connection

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

with the City's attempt to assert a "common-interest defense" privilege.[29]

92. On January 25, 2019, at 8:42 a.m., BRAJEVICH (using the **BRAJEVICH's ACCOUNT**) left another voicemail message for PETERS, which expressed BRAJEVICH's desire to have TUFARO send legal authority for their position on the common-interest privilege. BRAJEVICH opined that the City needed to identify a common-interest agreement reached between Jones and the City, and that he wasn't sure how they would do that under existing legal authority. BRAJEVICH noted that "when you're making declarations it looks like you're hiding something when you're not disclosing it." BRAJEVICH opined that he thought they would be okay because the ratepayers got 100 cents on the dollar in the *Jones* settlement, but he was concerned about "how we get through all the appearances and the sloppy ass shit."

93. On January 25, 2019, at 8:44 a.m., BRAJEVICH, using **BRAJEVICH's ACCOUNT**, sent PETERS a text message stating that BRAJEVICH had "Left you 2 voicemails on your cell when you have a chance to listen."

94. KIESEL's law partner, [redacted], advised the government that on January 25, 2019, she participated in a conference call with PETERS, KIESEL, PARADIS, and TUFARO, during which the parties discussed whether a privilege would apply to the documents sought by PwC and whether the City would take a writ. [redacted] was generally unfamiliar with the case at that

[29] I have reviewed two emails that BRAJEVICH (using **BRAJEVICH's EMAIL**) sent to PETERS on January 25, 2019, which I believe are the emails referenced here.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

time. She recalled that during this discussion, PETERS appeared inclined to take a writ, but that PETERS said that he was going to discuss the matter with FEUER. [redacted] further recalled PETERS stating that he had a scheduled meeting with FEUER that evening (Friday, January 25), and that PETERS was not looking forward to giving FEUER bad news on a Friday evening.

a. An electronic calendar entry showed that on January 25, 2019, at 12:30 p.m., KIESEL invited PETERS, BRAJEVICH (on **BRAJEVICH's EMAIL**), PARADIS, TUFARO, and [redacted] to a "Follow Up Conference Call" on January 28, 2019, at 9:30 a.m.

b. I believe that this entry scheduling a "follow up" corroborates [redacted] recollection that she joined a call with PETERS, KIESEL, PARADIS, and TUFARO on January 25, 2019. I further believe that the inclusion of BRAJEVICH on the invitation, paired with BRAJEVICH's inclusion on the aforementioned January 24 email chain, suggests that BRAJEVICH may also have participated in the January 25 call that [redacted] recalled.[30]

c. I further believe that a voicemail from BRAJEVICH using **BRAJEVICH's ACCOUNT** to PETERS on the morning of January 28, 2019 (described in more detail below), to touch base about their planned 9:30 a.m. conference call set for that morning, additionally supports the other evidence that BRAJEVICH was

[30] A further calendar entry indicates that KIESEL canceled the January 28 call.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

aware of the issues being discussed and planned to take place in this "follow up" call.

95. On January 25, 2019, PETERS took part in a phone call with KIESEL, PARADIS, and TUFARO. [redacted] surreptitiously recorded a portion of the call and later provided the recording to the government.[31] I have reviewed the transcript, which reflects PETERS, PARADIS, and TUFARO discussing matters including: 1) the fact that the City had not disclosed the City's coordination with LANDSKRONER in drafting and filing the complaint, 2) their view that the City had not had an obligation to disclose it in the past, 3) whether or not to disclose it now, and 4) the possible reactions of the court to such a disclosure. PETERS opined that this was an "optical" problem, but stated that as a legal matter, he did not believe the City had done anything wrong.

96. FEUER's daily schedule, which was emailed to PETERS, indicates a scheduled meeting on Friday, January 25, 2019, from 4:30 p.m. to 5:00 p.m., between FEUER, KAPUR, and PETERS.

97. PETERS proffered that on either January 25, 2019, or January 28, 2019, PETERS attended a meeting with FEUER and KAPUR to discuss PwC's court-authorized demand for documents related

---

[redacted]

The metadata from the recording provided by [redacted] suggests that this recording was saved at 11:24 a.m. PST on January 25, 2019. It is unclear to me whether this is part of the same call that [redacted] participated in. [redacted] indicated that she did not speak during that call.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to the City's upcoming PMQ deposition. According to PETERS, the following occurred at that meeting:

a. PETERS advised that there were documents in KIESEL's and PARADIS' possession that would be damaging to the City.

b. PETERS told FEUER that he did not at that time know precisely what the documents contained, but that he believed they would show coordination between KIESEL/PARADIS and LANDSKRONER before the *Jones v. City* complaint was filed.

c. PETERS told FEUER that he anticipated that the documents would show the City providing existing complaints to KIESEL/PARADIS to aid their drafting of the *Jones v. City* complaint.

d. PETERS further stated that the documents would likely show that PARADIS drafted the *Jones v. City* complaint and the settlement demand letter.

e. FEUER's reaction was like nothing PETERS had seen before. FEUER was highly emotional and visibly upset, covering his face with his hands for a long period. FEUER repeated multiple times that this "can't be so." FEUER stated that this would be "catastrophic," which PETERS understood to reference the anticipated effect that disclosure of these facts would have on the *Jones* settlement and the reputation of FEUER's office.

f. PETERS told FEUER not to "panic," and told FEUER that he (PETERS) would look into the situation.

g. FEUER did not at any time ask to see the documents that PETERS had described, nor did he ever ask PETERS

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to obtain them, review them, or show them to FEUER or anyone else.

h. FEUER and PETERS discussed the next hearing before Judge Berle, which was set to occur the following Wednesday, January 30, 2019, in the *Jones* case. FEUER and PETERS agreed that they (officials from the City, not Special Counsel) needed to convey to Judge Berle the message that he had the attention of the City Attorney's Office, and that the City Attorney's Office would not tolerate any unethical conduct.

i. FEUER directed PETERS to draft, over the weekend, a script bearing this message, which PETERS would deliver in person at the *Jones* hearing the following Wednesday.

98. On Saturday, January 26, 2019, in a series of text messages that I have reviewed, PETERS asked KIESEL to set up a call for the next day. KIESEL agreed and asked, "Will Mike [FEUER] give us clearance for disclosure of documents and full disclosure on questions?" PETERS did not reply to that inquiry, and they set a call for 2:00 p.m. the following day with them and PARADIS.

99. On Saturday, January 26, 2019, in a series of text messages that I have reviewed, KIESEL asked PARADIS to participate in a call with PETERS the next day at 2:00 p.m. PARADIS agreed and asked whether KIESEL had "anything to report now." KIESEL replied that PETERS had left a message that FEUER had reached a decision on another issue, but KIESEL stated that PETERS "said nothing about the documents or objections."

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. Based on the context of the above two text exchanges and my knowledge of the investigation, I understand that KIESEL indicated that PETERS had not yet advised whether FEUER would authorize them to disclose the potentially damaging documents that PwC was demanding.

100. On January 27, 2019, at approximately 2:20 p.m. PST, PETERS, KIESEL, PARADIS, and TUFARO participated in a telephone call. [redacted] surreptitiously recorded a part of the conversation and later provided the recording and a draft transcript to the government.[32] The recording contains the following relevant portions:

> PETERS: Okay. **Here's what I would like to do though, at Mike's request. He said to me, "What are the very, very worst documents out there that we've created that would most likely lead to embarrassment** or serve as a basis for somebody's… or Jamie Court's allegations that there was, that there was some conflict… anything from the pinnacle or standpoint of ethics." . . .
>
> Now, I said to him "Ya know, Mike, I don't really know," and he kinda chided me for not knowing and that's a fair criticism from where I stand. **I said, "although it's not teed up yet, there's a probably greater than 50 percent likelihood that eventually it will be revealed that we drafted for Landskroner a draft complaint." Now, at first, there was a great gnashing of teeth.**
>
> . . .
>
> PETERS: But this is, **Mike is aware that this could get ugly for a while**. But he wants to let us get in there and tear off the band-aids because once you get beneath the smoke, you know, you'll see that there really is ultimately, no ethical fire.
>
> . . .

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

PETERS: And all of the story is going to be told through these emails? Right, Paul?

PARADIS: Yes. Yes.

KIESEL: Yes. And by the way, **there are emails with the City of L.A., discussing -- knowing we were doing this and encouraging us to do this quickly.**

PETERS: **Okay.**

. . .

KIESEL: And then, Tommy, the only other piece, at least on the emails I saw, was Michael Libman, who was gonna to be filing the Jones versus DWP complaint reached out to me. He was in trial, and he said, "Paul, I need the money to file the Jones action." And I said, maybe something like, "We'll take care of it." And Paul Paradis was copied on it. And Paul wrote back and said, “no Landskroner is picking up all costs, all expenses. It’s on Landskroner.” And Landskroner obviously paid for the filing of the complaint.

PETERS: **I will want to read that one** because that one, **because optically, someone is going to optically scratch their head on**. So, I'll know about that one. Yeah, so if you could **send those things to me so I can get through 'em before Wednesday morning**, that would make me more comfortable. **It's just what’s the universe of shit that’s going to happen. I can give a heads up to Mike.**

. . .

KIESEL: Well, let me just add that I am feeling a whole lot better after this conversation than I had been for the last 48 hours. This has been a difficult situation.

PETERS: What were you expecting? What were you figuring that Mike was gonna ask us to do?

KIESEL: **I was figuring that Mike was not gonna release the documents at all** but Mike wanted to take a writ on the objections and we were just gonna make this thing so much worse than it is, in the end. So, I’m thrilled that we’re getting transparency. Light is what will disinfect the situation, nothing more.

PETERS: Yep.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

101. Based on the context of the messages and my knowledge of the investigation, I believe the parties' references to "Mike" throughout the January 27 conversation refer to FEUER. I further believe that the reference to "Jamie Court" refers to the president of an organization called Consumer Watchdog, which has, according to open-source media reports and other information revealed during the investigation, raised public allegations of corruption and ethical violations by City Attorney's Office and LADWP regarding the billing system litigation.

102. PETERS proffered that he participated in a phone call with KIESEL and PARADIS on January 27, 2019, and provided the following information relevant to that call:

a. PETERS told KIESEL and PARADIS that he wanted to see the documents.

b. KIESEL asked whether FEUER would allow them to produce the documents, and PETERS stated that "I will take a look."

c. KIESEL "seemed resigned" to the fact that the documents would be produced. By contract, PARADIS was more reluctant and concerned about the possibility of production.

103. PETERS proffered that, at some point during this time period, he conveyed to KIESEL and PARADIS that FEUER was "not interested in producing these documents."[33]

[33] I recognize that this information is inconsistent with other evidence described herein and, if true, would appear to represent a change in direction from the discussion reflected in the aforementioned partially recorded call on January 27, 2019.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

104. On the morning of Monday, January 28, 2019, at 9:08 a.m., BRAJEVICH (using **BRAJEVICH's ACCOUNT**) left a voicemail for PETERS. BRAJEVICH stated that he was calling to touch base with PETERS before "the 9:30 call," which BRAJEVICH planned to take from the road.[34]

105. PETERS proffered that over the weekend of January 26-27, 2019, as directed by FEUER, PETERS drafted a written script to read in court at the January 30 *Jones* hearing

106. PETERS further proffered that the following took place at and between a series of meetings with FEUER and KAPUR early in the week of January 28, 2019:

a. In preparation for the January 30, 2019 hearing in the *Jones* case, PETERS and FEUER worked together to hone the written script that PETERS was instructed to read aloud in court.

b. To the best of PETERS' recollection, PETERS drafted his statement by hand on a yellow pad and delivered it orally to FEUER at FEUER's direction. FEUER then critiqued PETERS's performance and directed him to make various changes. According to PETERS, FEUER's changes were of the "micromanagerial" variety and included instructing PETERS to refrain from using a definitive article.

---

[34] As noted above, I believe that this referenced 9:30 a.m. conference call was a scheduled call that KIESEL had invited PETERS, BRAJEVICH, PARADIS, TUFARO, and [redacted] (via an electronic calendar invitation that I have seen) to join at that time. A further email from KIESEL at 9:24 a.m. on January 28, 2019, indicates that this call was cancelled a few minutes before it was to take place.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

c. FEUER had never required PETERS to do anything like this before. PETERS was embarrassed about being required, as a division chief, to deliver a mock presentation to the City Attorney.

d. In addition to FEUER and KAPUR, PETERS recalled that Wilcox was present for at least one of the mock presentations. PETERS further believed (but was uncertain) that BRAJEVICH may have been present.

107. An electronic calendar entry sent by Google calendar on behalf of FEUER at **FEUER's EMAIL** to PETERS and KAPUR at **KAPUR's EMAIL** indicates a scheduled meeting between FEUER, KAPUR, and PETERS on Monday, January 28, 2019, from 2:30 p.m. to 3:30 p.m (two days before the scheduled hearing on the documents).

108. On the evening of Monday, January 28, 2019, BRAJEVICH left a voicemail for PETERS. BRAJEVICH reported that he had a good meeting with Maribeth [Annaguey], and noted that he and PETERS were "on for 11:00 tomorrow." BRAJEVICH said that he told "them" that if there were "any particular buzz words" that PETERS should say when PETERS was "down there on Wednesday" [January 30, 2019], to give them to PETERS tomorrow.

a. I believe that BRAJEVICH's reference to buzz words that PETERS was supposed to say on January 30, 2019, indicates BRAJEVICH's awareness that PETERS was receiving direction from others about what to say at the January 30 hearing.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

109. FEUER's daily schedule, which was emailed to PETERS, indicates a scheduled meeting on Tuesday, January 29, 2019 (one day before the hearing), from 10:30 a.m. to 11:00 a.m., between FEUER, KAPUR, and PETERS.

110. I have reviewed a January 29, 2019 email from PARADIS to PETERS and TUFARO attaching a .pdf file. The attached .pdf files contained email correspondence reflecting PARADIS's and KIESEL's coordination with LANDSKRONER in drafting and filing the *Jones v. City* complaint.[35] In an email on January 30, 2019, PETERS replied to confirm receipt.

111. Both KIESEL and [redacted] advised the government that early in the week of January 28, 2019, KIESEL asked [redacted] to gather emails responsive to PwC's document request related to the City's PMQ deposition, that [redacted] worked with KIESEL's technical staff to do so, and that on January 30, 2019, [redacted] sent an email to PETERS and PARADIS with a Dropbox link to a .pst[36] file containing the emails from KIESEL's system that [redacted] found to be responsive.

---

[35] To my knowledge, these files from PARADIS, which I have reviewed, have not been revealed or produced by the City. I do not know whether they were recovered in the City's forensic examination of PETERS's computer (described below) or why they were not included in the City's below-described April 2019 filing revealing the KIESEL Emails.

[36] In computing, a Personal Storage Table (".pst") is an open proprietary file format used to store copies of messages, calendar events, and other items within Microsoft software such as Microsoft Exchange Client, Windows Messaging, and Microsoft Outlook.

a. I have reviewed this email from [redacted] to PETERS and PARADIS dated January 30, 2019, with a Dropbox link to a .pst file labeled "Emails Responsive to PMQ."

112. PETERS proffered as follows:

a. PETERS received the documents from both PARADIS and KIESEL on approximately January 29, 2019.

b. Believing that FEUER did not want the documents to come to light, PETERS did not tell FEUER that he had received these documents from PARADIS and KIESEL.

c. FEUER did not ask about the documents after the late-January meeting wherein PETERS told FEUER what he expected the documents to show, and PETERS understood that FEUER did not want him to produce the emails.

d. During this time period, on a date that he did not recall, PETERS informed KIESEL and PARADIS that "Mike has decided not to produce the documents," which PETERS believed to be FEUER's implicit directive to PETERS.

113. On the morning of January 30, 2019, PETERS appeared in court at the *Jones* hearing, as directed by FEUER. At the hearing, PETERS made the following statement (related in pertinent part), which was in substance the statement that FEUER had "flyspecked" and instructed him to make:

> My name is Tom Peters, and I'm appearing personally in this matter for the first time based on the court's request in the related case that the City Attorney be asked to review the status of these matters. That is being done, but I do want to make sure that you understand our commitment to assuring the court that . . . . This court needs to feel completely comfortable and at ease that its confidence in this settlement in justified. There are a few things I think we can do

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

to advance that goal. Look, from the summer of 2014, if not earlier, the Department of Water and Power knew there was a huge problem with the Customer Care and Billing System. We still have a dispute, as to this day, as to whether it was PwC's fault or DWP's. That's the related litigation.

Look, fundamentally, with respect to this lawsuit, the Jones, et al., ratepayer class actions, there was a shared objective between the Department and the ratepayers from the get-go to give them 100 percent on the dollar refund of every dollar that had been overbilled, not 99 percent or 98 percent, but, Your Honor, also we couldn't pay 101 or 102 percent. That's a gift of public funds. **So through arm's length negotiations, that goal was ultimately achieved** as was the interrelated goal of getting a meaningful, durable, thorough process underway to make sure that the Customer Care and Billing System was repaired such that there was not a repeat, and we're obviously still grappling with that problem to this day. **But to the extent that anybody continues to be concerned at a lack of arm's length negotiation, I have some proposals**, and I think hopefully everybody will think are good ideas. One is the City suggested that we have a deposition of retired federal judge Dikran Tevrizian who presided over the multiple mediation sessions we had because he's the one person who, better than anyone else, would know the nature of the negotiations. The City certainly doesn't object to that.

To the extent that people are concerned about how the remediation or the refund is going, the City would certainly not object to deposition of Mr. Bender or Ms. Barbara Berkovich I think is her name, who is the special master who knows about the appellate process. The court has asked that she give her report at the end of this. If anybody's curious on how things stand today, then they should do it. I should also report to the court that in the related case, the City is not going to take any sort of a writ related to the recent litigation related to the PMQ depo notices.[37]

---

[37] From review of the transcripts and related materials, I understand this as a reference to the court's order that the City submit a PMQ witness for a deposition and produce related documents, which was issued over the City's objection. I also understand that the documents discussed between PETERS and FEUER, sent to PETERS by KIESEL and PARADIS, and withheld by PETERS at FEUER's implied direction were arguably responsive to this PMQ notice.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

> **As the court will recall, there were documents that were requested of the City through that PMQ deposition notice. We will be producing those documents.** We will be producing, also, the Chief Deputy of the office, Jim Clark, coincidentally a partner until about six years ago of the Gibson firm which is defending PwC. He will respond, I think, to all of the categories of inquiry set forth in that notice.

a. Following this statement by PETERS, the court commented as follows:

> I think that matter [of the discovery issues raised in the *PwC* case], it seems to be viewed seriously, which I think is important, and **I hear your words about cooperation with the discovery that will be coming along.**

b. PETERS replied as follows:

> Yeah. **We should all be assured that the City Attorney's commitment to always practicing with the highest ethical standards in mind has indeed been advanced, and I think that once the totality is understood, everyone will conclude that that is precisely what has happened here**.

c. Based on my knowledge of the investigation, I believe that by directing PETERS to make this prepared statement, FEUER intended for the court, the parties, and PwC to believe that the City would no longer fight production of all materials responsive to PwC's PMQ notice, and that it would comply with the order to produce that discovery.

114. On January 30, 2019, at 11:28 a.m., PETERS sent an email to FEUER at **FEUER's EMAIL** and KAPUR at **KAPUR's EMAIL** with the subject line "Things went well in court this morning." In the three-paragraph email, PETERS summarized that morning's hearing in the *Jones* case, including the following:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

a. PETERS opined that he had expressed his thoughts well with a "non-apologetic" tone, and that the judge had responded well.

b. PETERS stated that the court indicated that the propriety of the settlement was not being questioned, and that the only issue was whether there was a conflict.

c. PETERS stated, "Because we believe that our team's ethics will be vindicated once all of the facts concerning the interaction with Jones/Landskroner are revealed and understood, I am anxious to get those facts out as soon as possible and have yet again expressed such to the Pauls [KIESEL and PARADIS], who agree."

d. "[O]ur purpose for the day appears to have been fulfilled. Now on to the implementation of our plan, where I will be working carefully to see that things go as smoothly as possible."

e. PETERS asked FEUER to advise whether PETERS should come to FEUER's office to discuss further.

115. Seventeen minutes later, using **FEUER's EMAIL**, FEUER replied to all, "Thank you so much, Thom. Deeply appreciated. I would be grateful for a few more minutes with you today on this point, but no emergency. Mike."

116. At 12:56 p.m. on January 30, KAPUR (using **KAPUR's ACCOUNT**) replied to just PETERS as follows: "Thom – glad to hear it went well – I know a big relief to you (and Mike) as it sounds that you were successful of starting to turn the course of the ship –- not an easy thing to do!"

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

117. PETERS proffered that soon after the January 30 hearing, and after PETERS sent the aforementioned email to FEUER and KAPUR reporting that the hearing had gone well, FEUER came down to PETERS's office, which was on a different floor, and the following events took place:

a. FEUER and PETERS did not have a meeting scheduled; rather, FEUER was dropping by unannounced.

b. FEUER left his security detail outside PETERS's office and shut the door.

c. FEUER expressed that he was very thankful that things had gone well at the hearing, and that PETERS had stuck to the script and delivered their message to FEUER's satisfaction.

d. FEUER stated that he was pleased that Maribeth Annaguey, the City's outside counsel, had given PETERS's performance a positive review.

e. FEUER was very effusive in his praise of PETERS and in expressing his gratitude.

f. FEUER apologized if he had offended PETERS for "treating him like a first-year associate" and requiring him to deliver mock performances in FEUER's office.

g. FEUER came around to PETERS's side of the desk and stood behind PETERS. FEUER "laid hands on" PETERS by placing both hands on PETERS's shoulders in a friendly and intimate gesture.

h. During the conversation, FEUER stated words to the effect that, "I've got your back," and "I've always taken care of you."

i. During this interaction, PETERS told FEUER words to the effect that, "By the way, you don't need to worry about those documents." FEUER replied with words to the effect that this was "great, wonderful. I appreciate it."

j. FEUER did not ask what documents PETERS was talking about, nor did he ask what PETERS meant. At no time did FEUER ever ask to see the documents, or ask whether PETERS had seen them or what they had revealed.

k. FEUER's unannounced visit to PETERS's office lasted approximately 10-15 minutes.

l. The interaction was unusual, and it was very significant to PETERS. PETERS interpreted it as confirmation that he had done the right thing in withholding the documents, because he had correctly intuited that FEUER did not want him to do so.

103. PETERS proffered that during this time period, BRAJEVICH was involved in discussions relating to the City's strategy for shielding from production the documents sought by PWC in its PMQ discovery demand.

104. I believe the evidence, including the above-described proffer information, voicemails, emails, and meeting invitations to or from BRAJEVICH, combined with BRAJEVICH's engaged role in this high-profile lawsuit involving LADWP, provides probable cause to believe that BRAJEVICH was involved in substantive

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

discussions as to the City's strategy to shield the damaging KIESEL and PARADIS PMQ documents, about which FEUER later gave the potentially false [redacted] statements described herein.[38]

2. The events between late January 2019 and April 2019

105. As further described in the omnibus affidavit, evidence indicates that the following relevant events took place between late January 2019 and April 2019:

a. In February 2019, FEUER and PETERS decided that CLARK would serve as the City's "person most qualified" witness in the City's PMQ deposition, notwithstanding the facts that 1) CLARK was set to return from a lengthy medical leave [redacted] just days before the deposition, and 2) CLARK was officially recused from the *PwC* case because he received retirement income from Gibson Dunn, PwC's counsel.

b. On February 26, 2019, CLARK testified as the City's PMQ witness. CLARK's testimony included the following:

[38] In a text message from BRAJEVICH to PETERS on March 2, 2019, BRAJEVICH stated that he "did not realize Paradis had prepared a complaint vs DWP and sent it to Jones." PETERS replied by text that he did not know that either. I do not know whether BRAJEVICH included this in a text message to falsely cover himself and/or PETERS as these issues were starting to become public, or whether BRAJEVICH was truly unaware that PARADIS had drafted the *Jones v. City* complaint. As discussed herein, the evidence indicates that by that date, PETERS was aware of that fact, notwithstanding his statement to the contrary in this text exchange.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

i. CLARK first learned that Jones would be suing LADWP in March 2015, after it became clear that the *Jones v. PwC* lawsuit was not going to go forward.

ii. The City expected the *Jones v. City* complaint before it was filed on April 1, 2015.

iii. After PARADIS concluded that he had a conflict in representing Jones against the City, which was PARADIS's client, CLARK was aware that PARADIS recommended that LANDSKRONER be brought in as Jones's new counsel, and that CLARK assumed that someone at the City authorized that action.

iv. CLARK understood that the City had recommended LANDSKRONER to represent Jones because the lawyers in the class actions that had already been filed against the City were intransigent and difficult to deal with, and CLARK didn't know if they were "willing to do what DWP wanted."

c. On March 14, 2019, the City submitted on CLARK's behalf a lengthy "errata" containing 54 changes to CLARK's testimony, many of them substantive, including the following:[39]

i. CLARK was asked, "How much earlier than April 1 did you know that the settlement demand would be forthcoming at some point and that you would be settling with Mr. Jones?" CLARK replied, "Sometime during the latter half of —— the end of March." In his errata, the City retracted this answer and changed it to, "I didn't."

[39] The errata was signed by CLARK. Information from multiple sources, including CLARK, indicates that the errata document was the result of one or more lengthy discussions among lawyers from the City Attorney's Office and outside counsel, who determined that CLARK's answers needed to be amended.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

ii. In a reply to a question as to why one of the existing class counsel was not recommended to Jones, CLARK testified as follows: "My understanding, and this is mostly from outside counsel, the Liner [law firm] people, who have been trying to deal with [the plaintiffs' lawyers for the existing class actions], that they were just intransigent, couldn't —— they wouldn't —— didn't want to negotiate or propose things that were not —— were not acceptable. And I don't know if they were willing to do what DWP wanted, which was basically —— there would have been overcharge repaid and have the —— and have oversight of the system to correct it." The City's errata changed CLARK's answer to, "I don't know what Mr. Paradis recommended to Mr. Jones."

iii. At his deposition, CLARK was asked the following question: "No one brought Mr. Landskroner into the case because he was viewed as someone who would be the most zealous advocate available for Mr. Jones to pursue claims; correct?" CLARK replied, "That's —— that's right." In his errata, the City changed CLARK's reply to, "I don't know why Mr. Paradis recommended him to Mr. Jones."

d. On or about March 6, 2019, shortly after LANDSKRONER invoked the Fifth Amendment in court in response to questions by the judge about whether any of his attorney's fees had been paid to PARADIS and the Special Counsels' representation of Jones was revealed in court, the City Attorney's Office announced that both PARADIS and KIESEL had stepped down or been terminated.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

e. On or about March 22, 2019, the City Attorney's Office announced that PETERS had resigned in the wake of media requests for information about PETERS' receipt of outside counsel referral fees unrelated to the LADWP billing litigation.

3. The City's April 26, 2019 filing and press release claiming that the KIESEL Emails had just been discovered

106. On April 26, 2019, under FEUER's name and at his direction, the City filed a "Notice Re: Documents" in the *City v. PwC* case. The Notice stated that "[o]n April 24, 2019, at approximately 5:30 p.m., counsel for the City learned that a .pst file labeled "Emails Responsive to PMQ(1).pst existed on a forensically imaged hard drive."[40] The Notice went on to describe certain emails between and among PARADIS, KIESEL, LANDSKRONER, and LIBMAN indicating that PARADIS and KIESEL had prepared and filed the *Jones v. City* complaint on behalf of LANDSKRONER and LIBMAN, along with other coordination. The Notice specifically noted that "No City employee or officer sent or received any of these emails." The Notice attached some of the emails and indicated that the emails had been produced to PwC after they were discovered.[41]

[40] According to multiple sources, including FEUER, the hard drive in question had been used by PETERS and, after PETERS's resignation, was forensically imaged by an outside vendor at the direction of the Browne George law firm representing the City after PETERS resigned in late March 2019.

[41] The omnibus affidavit articulated my understanding at that time that the .pst file —— which the City's April 26, 2019 filing described as containing 131 records but attached only a fraction (approximately 29) of that number —— contained at least some of the emails among City personnel that later emerged during the *PwC* litigation notwithstanding the City's stringent efforts to shield those emails from production. This

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

107. Contemporaneous with the City's Notice, the City issued a press release that included the following statement by Rob Wilcox, spokesperson for the City Attorney's Office:

> **The emails we've just discovered reveal a reprehensible breach of ethics** by outside lawyers in whom our office placed trust. **The conduct of outside counsel now coming to light** was outrageous and inexcusable.

108. I believe that the City's filing and public statement were intended to convey that no City official or employee, to include FEUER, knew about Special Counsel's coordination with LANDSKRONER and LIBMAN in advance of the *Jones v. City* complaint until the KIESEL Emails were discovered in a forensic review of PETERS' hard drive on April 24, 2019.

---

understanding was informed in part by information provided by KIESEL, and in part by my review of the complex and dynamic factual landscape of the *Jones* and *PwC* litigation.

The prosecution team's review of the contents of the .pst file was hindered by privilege protections and technical difficulties. Only after those issues were successfully mitigated was I finally able to review the contents of the file. This was after the omnibus affidavit was filed and when I learned that it contained 145 items. Several of these, in a folder marked "Deleted Items," were email chains and attachments that reflected communications between and among City employees and officials related to the LADWP billing litigation. The file did not contain other emails to and from City personnel that the City sought to shield and that later emerged.

I do not know how the City arrived at the count of 131 records itemized in its April 2019 notice, or whether the hard drive that the FBI obtained (from the City's vendor with assistance from the City) after execution of the search warrant was in the same condition as when it was earlier reviewed by the City's outside counsel. Nor is it clear whether the City's counsel, upon reviewing the .pst file and making the representation that none of the emails were sent to or from City employees or officials, viewed the items in the folder marked "Deleted Items." The FBI continues to investigate these and other questions related to the .pst file and the hard drive, both through forensic examination and through witness interviews and other investigative means.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

4. FEUER's initial interview with the prosecution team

109. On July 22, 2019, while agents were executing the July 2019 search warrants, including at the City Attorney's Office, FEUER met with the prosecution team and requested to be interviewed immediately. The interview was recorded, and I have reviewed the transcript.

110. During that interview, FEUER advised the government as follows:

> Q: Are you aware of whether anybody in your office, including special counsel or anybody else, forwarded or provided internal privy information to the Jones litigators in order to help it achieve that hierarchy?
>
> A: I would have been horrified, and had I been cognizant of that activity, whoever provided it would not have been engaged with the City, on the staff, or outside counsel then or ever again.
>
> Q: Why is that?
>
> A: Because I would not have considered that ethical behavior.
>
> Q: Have you since learned that any of that occurred?
>
> A: What I have since learned is that, because **I've seen email traffic that emerged fairly recently, in April** that —— especially Mr. Kiesel, and it appeared, from the email traffic, Mr. Paradis, had been assisting in the filing of the Jones and DWP litigation with Plaintiff's counsel.
>
> And to anticipate a question, **around mid to late April, something in that time frame, three months ago or so, I received a phone call** from our counsel indicating that they had found, I think, a thumb drive or something on the computer that had not been opened. There had been attempts made to open it a couple times, and they had found a way to open it. And that that drive contained emails that I just referred to. And they described the content of those emails to me at that point. Maybe early April something like that. And we agreed on that conversation —— I remember the conversation. I was

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

> on my way to an event that night. **And we agreed that information had to be immediately disclosed to the Court and to opposing counsel.**

111. In the interview, FEUER further advised the government as follows as part of a lengthy statement about KIESEL's deposition testimony that the City directed his actions on behalf of the *Jones* plaintiff who sued the City:[42]

> A: "When the —— **in April when I learned about the email exchange** and subsequent to that when there was testimony by Mr. Kiesel in deposition that our office was cognizant of that activity, it really made little sense to me."

112. During the interview, FEUER further stated as follows:

> A: **When the emails in mid to late April emerged**, I actually asked Mr. George to inquire as to whether [CLARK] knew anything about that.
>
> Q: To inquire of Mr. Clark?
>
> A: Yes. I don't remember for sure, but I believe that during that period his deposition was still forthcoming, and I wanted really to just create enough distance that Mr. Clark felt he could say whatever he thought the truth was about any of these issues.
>
> But Mr. George reported to me that he did ask Mr. Clark. He said Mr. Clark was infuriated by the **revelation of those emails**. And Mr. Clark . . . referred in passing to Mr. Kiesel has having perjured himself in his testimony with regard to whether our office was cognizant of any of these.
>
> **I asked Mr. George to ask Mr. Clark on or about April 20-something if he had any possible awareness of anything close to what was being memorialized in those emails.** To which Mr. George said Mr. Clark responded by becoming infuriated, said absolutely not, that's completely unethical, no one should ever do that. But was very – I was told was very exercised that someone he'd been working with had engaged in that behavior.
>
> . . .

[42] As FEUER's statement was not directly relevant to a pending question, no question is indicated here.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

> And I needed – **facts kept emerging of which I was unaware. The fact of the email, for example**, you know, what I thought we were at a stage where I thought I had a handle on what transpired, which – at that stage, with the exception of Mr. Landskroner invoking the Fifth Amendment [and] Mr. Paradis doing the same - **I thought I had a handle on exactly what had taken place here.**
>
> **And now this email exchange comes to light**.

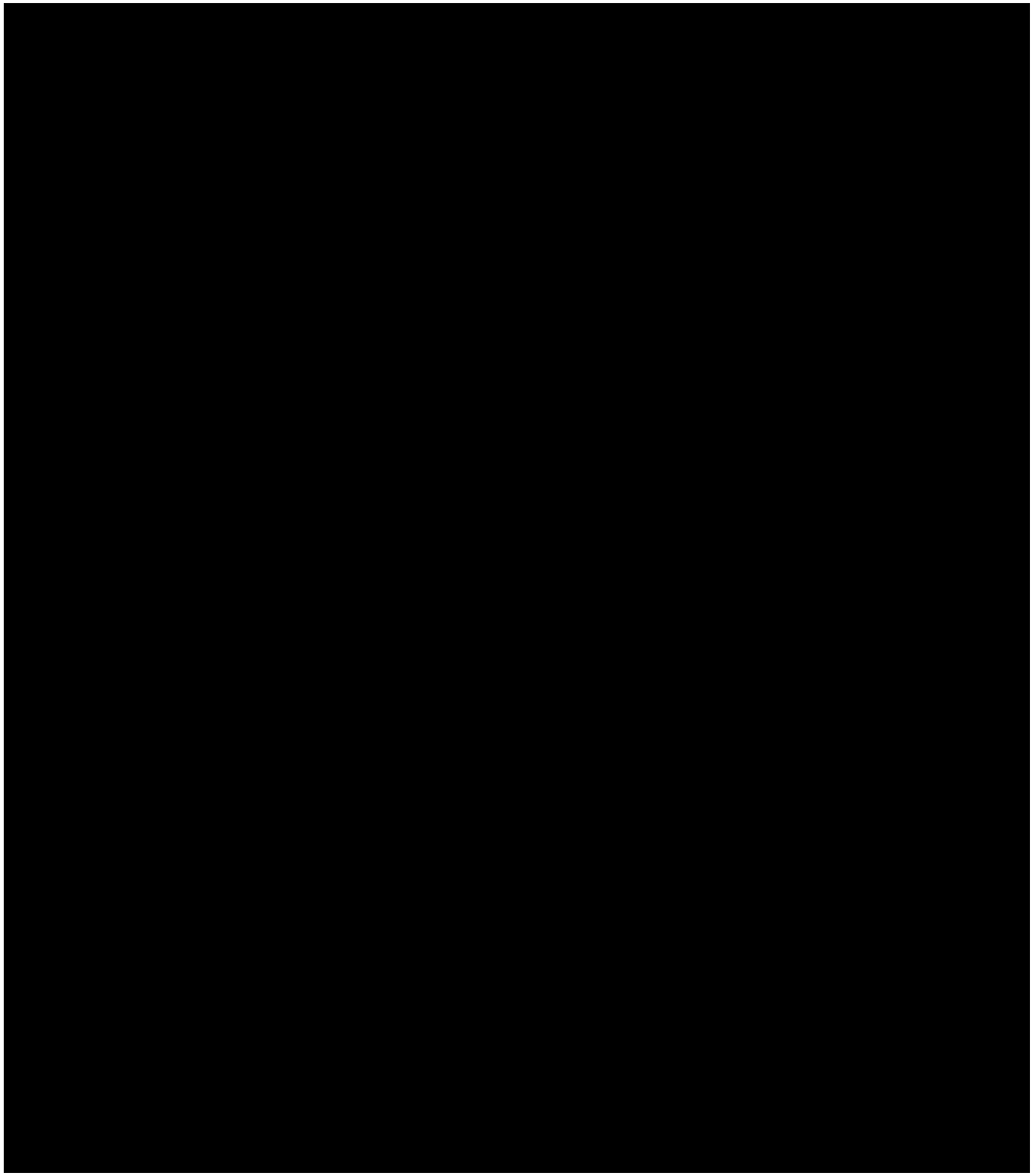
113. I believe that in these statements, FEUER intended to convey to the government that – consistent with the City's April 26, 2019 Notice and accompanying press release - FEUER had no awareness of Special Counsel's coordination with LANDSKRONER and LIBMAN in advance of the *Jones v. City* complaint until the KIESEL Emails were discovered in a forensic review of PETERS' hard drive on April 24, 2019. I further believe that these official statements by FEUER were material and misleading, based on the below-described evidence indicating that PETERS apprised FEUER in late January 2019 of both the existence of the KIESEL Emails and the damaging information that they likely contained, after which FEUER directed PETERS to take care of the KIESEL Emails, FEUER did not follow up to find out what was in the KIESEL Emails, and FEUER did not disclose the KIESEL emails to the Court or PwC. I believe that FEUER was motivated to provide such misleading statements in order to distance himself as far as possible from the, at minimum, unethical conduct engaged in by attorneys in his office and working on behalf of his office because of the resulting political damage to his reputation and that of the City Attorney's Office.

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

[redacted]

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB



Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

116. On August 13, 2019, FEUER testified in a deposition in the *PwC* case.[44] The deposition transcript reflects that FEUER testified as follows:

> **Q: On April 26, when this filing was made, did you authorize this filing?**
>
> **A. I directed it.**
>
> Q. Mr. Wilcox also made a statement on that day to The Los Angeles Times; is that correct?
>
> A. Correct.

[44] The information in this paragraph is derived from the deposition transcript, which I have reviewed.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Q. It accused Mr. Kiesel and Mr. Paradis of a egregious breach of ethics or a reprehensible breach of ethics, if I remember correctly; is that right?

A. Yes.

Q. Nothing was said about Mr. Peters; is that correct?

A. Correct.

. . .

Q: Did you have any understanding as to why Mr. Peters did not produce "Emails Responsive to PMQ" that had been provided to him by Mr. Kiesel's office?

A: At what time?

Q: On April 26, 2019.

A: My understanding was that the —— that analysis had been done that revealed that there had not been —— that the document had not successfully been opened.

Q: Did you understand that Mr. Kiesel's office had provided an email to Mr. Peters which provided him with instructions on how to open it and indicated that the name of the file was "Emails Responsive to PMQ"?

A: No.

Q: Do you have any understanding as to how —— as to why it is that Mr. Peters says he didn't open a file called "Emails Responsive to PMQ" in preparation for a PMQ deposition that he was defending after a court order requiring the production of responsive documents?

A: No.

. . .

Q: **At the time that you learned about the documents, April 26**, did you have any concern about the fact that those documents had been identified as being responsive to the PMQ notice, that the second PMQ deposition had taken place after these documents were provided to Mr. Peters, and that Mr. Peters never produced them to PwC?

A: I wanted to know whether Mr. Peters was cognizant of the content of those documents at the time that they were transmitted to him.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

117. I believe that by this sworn testimony, FEUER intended to convey that he had no awareness of the facts that were ultimately revealed in the KIESEL Emails prior to learning about those emails shortly after his counsel discovered them on approximately April 24, 2019. I further believe that this sworn testimony was intended to convey that upon learning of the KIESEL Emails in late April 2019, FEUER immediately directed that the emails be filed with the court and produced to the defendant, and simultaneously authorized a statement condemning the conduct revealed by the emails as a "reprehensible breach of ethics." I believe that this testimony was misleading, given the evidence described herein. While false or misleading sworn testimony at a civil deposition in a state case would not, standing alone, violate federal law, it is consistent with what I perceive as FEUER's misleading or false narrative in an interview with the federal government [redacted] intended to convey that he was unaware of the KIESEL Emails until April 2019, when he immediately directed their disclosure.

6. Contacts regarding CLARK's and PETERS's depositions

118. On April 9 and April 29, 2019, CLARK provided additional testimony at his court-ordered PMQ deposition in the *PwC* case. CLARK prefaced his testimony with a prepared statement blaming poor preparation by his attorneys for what he described as his inaccurate testimony during his February 26, 2019 deposition. As noted above, I believe that his February 26

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

testimony was largely accurate, and that his subsequent errata purporting to correct critical parts of that testimony was largely inaccurate. CLARK's testimony on April 9 and April 29, 2019, was generally inconsistent with his February 26 testimony and consistent with his errata, and for the aforementioned reasons, I believe that CLARK's April 9 and April 26 testimony contained material false statements related to the collusive litigation described herein.

119. On May 1 and May 2, 2019, following his aforementioned March 2019 resignation from the City Attorney's Office, PETERS provided testimony at a court-ordered deposition in the *PwC* case. A review of PETERS' phone indicates no text messages between **CLARK's ACCOUNT** and PETERS after PETERS's March resignation until Monday, May 6, 2019. On May 6, 2019, one business day after PETERS' deposition testimony, CLARK texted PETERS from **CLARK's ACCOUNT** and asked PETERS to call him. After a series of text exchanges, the two men made an appointment for CLARK to call PETERS the following Friday afternoon using either **CLARK's ACCOUNT** or CLARK's home phone.

7. Contacts regarding KIESEL's deposition

120. On April 29, 2019, counsel for PwC contacted KIESEL and offered him an opportunity to sit for a deposition in which KIESEL could address what PwC viewed as the City's "Ro[gue] Special Counsel theory of the case, which is inconsistent with [PwC's] view of the evidence." KIESEL agreed. Before the end of May, KIESEL had agreed to be deposed in the *PwC* case.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Case 2:24-cv-01650-SB Document 28 Filed 06/07/24 Page 1287 of 1425 Page ID #:2493

Case 2:24-cv-01650-SB Document 28 Filed 06/07/24 Page 1288 of 1425 Page ID #:2494

including that by February 2015, members of the City Attorney's Office authorized the plan to have Jones sue the City in order to obtain a favorable settlement of all of the existing class actions. KIESEL further testified that by early March 2015, both CLARK and PETERS were aware of the plan to file the *Jones v. City* complaint, and that both CLARK and PETERS were present when the decision was made for LIBMAN to serve as local counsel to LANDSKRONER, who had already been "recruited" to take over the representation of Jones.

127. KIESEL advised the government as follows with respect to his May 2019 deposition:

a. CLARK and PETERS attended KIESEL's deposition.

b. Despite the fact that PETERS had already abruptly resigned from the City Attorney's Office by that time, PETERS did not appear adverse to the City.

c. During breaks, CLARK and PETERS would huddle together with the City's outside counsel and look at KIESEL. CLARK's face was red, and "it looked like [CLARK] was going to have a stroke." KIESEL perceived these actions as an "intimidation tactic."

128. Based on the above information and my knowledge of the investigation, I believe that CLARK used **CLARK's ACCOUNT** to contact PETERS on May 24, 2019, to discuss KIESEL's upcoming deposition testimony, which the City had reason to know would be adverse to the City and contrary to the City's false or misleading narrative regarding the collusive litigation described herein.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

129. Again, I believe all of the foregoing narrative of apparent obfuscation, false and misleading statements, and omissions are part of FEUER's campaign to distance himself as far as possible from the, at minimum, unethical conduct engaged in by attorneys in his office and working on behalf of his office because of the resulting political damage to his reputation and that of the City Attorney's Office.

C. General Proffer Information about FEUER, KAPUR, BRAJEVICH, and CLARK

60. PETERS proffered that FEUER and KAPUR were very close, and that KAPUR usually attended PETERS' meetings with FEUER. PETERS opined that KAPUR had "extraordinary loyalty" toward FEUER, and that she was "very effective in enacting FEUER's directives." PETERS recalled that FEUER's schedule required him to be out of the office a lot, and that KAPUR did not generally travel with FEUER. However, PETERS believed that FEUER and KAPUR kept in close touch throughout the day and after hours on matters important to FEUER.

61. PETERS proffered that FEUER had hired BRAJEVICH for his current position as LADWP General Counsel, and that BRAJEVICH was "very well connected" in the City Attorney's Office and in political circles in the City more generally. PETERS believed that BRAJEVICH was somewhat close to FEUER. PETERS noted that on the *PwC* case, BRAJEVICH reported directly to FEUER, in light of CLARK's recusal from that matter.

62. PARADIS proffered to the government the following relevant information regarding BRAJEVICH:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

m. At one point, PETERS told PARADIS that he had told BRAJEVICH about Salgueiro's threats, and that BRAJEVICH was upset that the mediation of her demands had taken place at LADWP. PARADIS was unsure when this conversation with BRAJEVICH took place, other than it was during November or December 2017.

n. PARADIS did not recall specifically what PETERS said he had told BRAJEVICH. PARADIS had the sense that BRAJEVICH knew everything that FEUER knew about cases involving LADWP, but he could not provide a factual basis for that understanding.

o. PARADIS observed that BRAJEVICH was obsequious toward FEUER. PARADIS further proffered that although he did not witness many interactions between BRAJEVICH and FEUER and thus could not speak to the closeness of their relationship, he observed on multiple occasions BRAJEVICH "kissing up" to KAPUR, whom PARADIS understood to be FEUER's "gatekeeper."

118. PARADIS advised that he and BRAJEVICH "tolerated each other" but did not really like each other. PARADIS further informed the government that PARADIS and FEUER "hated" each other.

a. BRAJEVICH did not like to use email and frequently asked PARADIS not to discuss sensitive things with him by email but to instead contact him by phone or text.[46]

[46] WRIGHT proffered that BRAJEVICH was very careful about using both email and text messages, because of general concerns about discoverability. WRIGHT further noted that he was not aware of any nefarious reason for BRAJEVICH's caution about written communications.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

119. DAVID WRIGHT (former LADWP General Manager) proffered that BRAJEVICH —— as an Assistant City Attorney assigned as General Counsel for LADWP —— reported to FEUER. According to WRIGHT, the role of an LADWP General Counsel was to protect the City, and as such, BRAJEVICH's loyalties lay with the City Attorney's Office rather than with LADWP in instances where their respective interests diverged.

120. CLARK proffered that he and FEUER used to be very close, with a relationship of mutual trust and respect. However, after the FBI executed a search warrant at the City Attorney's Office, and specifically in CLARK's office, CLARK perceived that FEUER kept him at a distance.

D. Summary of Probable Cause for the TARGET ACCOUNTS

130. Based on my knowledge of the investigation and the information herein, I believe there is probable cause to believe that evidence of the Target Offenses and criminal schemes may be located in the **TARGET ACCOUNTS**. In particular, BRAJEVICH's use of **BRAJEVICH'S ACCOUNT** and **BRAJEVICH's EMAIL** to contact PETERS to discuss the KIESEL Emails and issues relating to disclosure in late January 2019, as well as other matters relating to the City's strategy in responding to allegations about the collusive litigation, indicates that **BRAJEVICH's ACCOUNT** and **BRAJEVICH's EMAIL** may contain evidence of the Target Offenses and criminal schemes.[47] Moreover, BRAJEVICH's reported caution in using email

[47] On or about December 6, 2019, I served on Microsoft an order pursuant to 18 U.S.C. § 2703(d) for **BRAJEVICH's EMAIL**. Microsoft advised that the only responsive information they had

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

Case 2:24-cv-01650-SB Document 28 Filed 06/07/24 Page 1293 of 1425 Page ID #:2498
Case 2:24-cv-01650-SB Document 28-1 Filed 06/07/24 Page 1293 of 1425 Page ID #:2498

a. On July 18, 2015, during the period in which City was mediating the allegedly preordained settlement in the *Jones* case to resolve all of the class actions on terms favorable to the City, PETERS sent FEUER a text message on **FEUER's ACCOUNT** advising FEUER of KIESEL's cell phone number (which I assume, based on context and my knowledge of the investigation, FEUER had requested from PETERS). Later that day, FEUER acknowledged the information with a text from **FEUER's ACCOUNT** reading, "Thank you."

b. On March 12, 2019, within days of KIESEL's and PARADIS's withdrawal as Special Counsel, PETERS texted FEUER on **FEUER's ACCOUNT** to advise as follows relevant to the collusive litigation and the City's correlated public-relations problems:

> "Hello. Eric George [of the Browne George law firm] has agreed to take the case and has what is, in my view, a very solid approach to [Judge] Berle's and the press's concerns. I think you will benefit from learning the particulars. Eric also has a couple of tactical thoughts which you should hear and deci whether to approve. When able, please call him. [redacted]. Thank you."

i. As detailed above and in the omnibus affidavit, the Browne George law firm was involved in the City's media and public-relations strategy following the public revelation in March 2019 that PARADIS and KIESEL had represented Jones, and also in crafting FEUER's and the City's response to the discovery of the KIESEL Emails on PETERS's hard drive in April 2019. I believe that the use of **FEUER's ACCOUNT** to discuss the ongoing public-relations crisis —— which FEUER was very concerned about and which I believe, as stated above,

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

caused FEUER to make the false and/or misleading statements described herein —— constitutes probable cause to believe that evidence of the Target Offenses and criminal schemes will be found on **FEUER's ACCOUNT**.

134. Moreover, the evidence shows that FEUER relied on members of his trusted inner circle —— including CLARK, KAPUR, and possibly BRAJEVICH —— and therefore, it is more likely that FEUER would have communicated with others, including **BRAJEVICH's ACCOUNT** and **CLARK's ACCOUNT,** about the facts underlying the Target Offenses and criminal schemes.

135. I believe that this evidence, coupled with other evidence -- including that articulated in the omnibus affidavit -- gives rise to probable cause to believe that the **TARGET ACCOUNTS** will contain evidence of violations of the Target Offenses and criminal schemes.

IX. BACKGROUND ON E-MAIL AND THE PROVIDERS

136. In my training and experience, I have learned that providers of e-mail and/or social media services offer a variety of online services to the public. Providers, like the PROVIDER, allow subscribers to obtain accounts like the **TARGET ACCOUNTS**. Subscribers obtain an account by registering with the provider. During the registration process, providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail or social media account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of

payment (including any credit or bank account number). Some providers also maintain a record of changes that are made to the information provided in subscriber records, such as to any other e-mail addresses or phone numbers supplied in subscriber records. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of an account.

137. Therefore, the computers of a PROVIDER are likely to contain stored electronic communications and information concerning subscribers and their use of the PROVIDER's services, such as account access information, e-mail or message transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of a SUBJECT ACCOUNT.

138. A subscriber of a PROVIDER can also store with the PROVIDER files in addition to e-mails or other messages, such as address books, contact or buddy lists, calendar data, pictures or videos (other than ones attached to e-mails), notes, and other files, on servers maintained and/or owned by the PROVIDER. In my training and experience, evidence of who was using an account may be found in such information.

139. In my training and experience, e-mail and social media providers typically retain certain transactional information about the creation and use of each account on their systems.

This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail and social media providers often have records of the Internet Protocol ("IP") address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a **TARGET ACCOUNT**.

140. In my training and experience, e-mail and social media account users will sometimes communicate directly with the service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers of e-mails and social media services typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of a **TARGET ACCOUNT**.

141. I know from my training and experience that the complete contents of an account may be important to establishing the actual user who has dominion and control of that account at a given time. Accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. Given the ease with which accounts may be created under aliases, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of an account, investigators often have to rely on circumstantial evidence to show that an individual was the actual user of a particular account. Only by piecing together information contained in the contents of an account may an investigator establish who the actual user of an account was. Often those pieces will come from a time period before the account was used in the criminal activity. Limiting the scope of the search would, in some instances, prevent the government from identifying the true user of the account and, in other instances, may not provide a defendant with sufficient information to identify other users of the account. Therefore, the contents of a given account, including the e-mail addresses or account identifiers and messages sent to that account, often provides important evidence regarding the actual user's dominion and control of that account. For the purpose of searching for content demonstrating the actual user(s) of a **TARGET ACCOUNT**, I am requesting a warrant requiring the PROVIDER to turn over all information

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

associated with a **TARGET ACCOUNT** with the date restriction included in Attachment B for review by the search team.

142. Relatedly, the government must be allowed to determine whether other individuals had access to a **TARGET ACCOUNT**. If the government were constrained to review only a small subsection of an account, that small subsection might give the misleading impression that only a single user had access to the account.

143. I also know based on my training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as “lol” to express “laugh out loud”), or codewords (which require entire strings or series of conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of a message or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and parenthesis :) to convey a smile or agreement) to discuss matters. “Keyword searches” would not account for any of these possibilities, so actual review of the contents of an account by law enforcement personnel with information regarding the identified criminal activity, subject to the search procedures set forth in Attachment B, is necessary to find all relevant evidence within the account.

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

144. This application seeks a warrant to search all responsive records and information under the control of the PROVIDER, which is subject to the jurisdiction of this court, regardless of where the PROVIDER has chosen to store such information.

145. As set forth in Attachment B, I am requesting a warrant that permits the search team to keep the original production from the PROVIDER, under seal, until the investigation is completed and, if a case is brought, that case is completed through disposition, trial, appeal, or collateral proceeding.

a. I make that request because I believe it might be impossible for a provider to authenticate information taken from a **TARGET ACCOUNT** as its business record without the original production to examine. Even if the provider kept an original copy at the time of production (against which it could compare against the results of the search at the time of trial), the government cannot compel the provider to keep a copy for the entire pendency of the investigation and/or case. If the original production is destroyed, it may be impossible for the provider to examine a particular document found by the search team and confirm that it was a business record of the provider taken from a **TARGET ACCOUNT**.

b. I also know from my training and experience that many accounts are purged as part of the ordinary course of business by providers. For example, if an account is not accessed within a specified time period, it -- and its contents

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

-- may be deleted. As a consequence, there is a risk that the only record of the contents of an account might be the production that a provider makes to the government, for example, if a defendant is incarcerated and does not (perhaps cannot) access his or her account. Preserving evidence, therefore, would ensure that the government can satisfy its Brady obligations and give the defendant access to evidence that might be used in his or her defense.

X. REQUEST FOR NON-DISCLOSURE

134. Pursuant to 18 U.S.C. § 2705(b), I request that the Court enter an order commanding the PROVIDER not to notify any person, including the subscribers of the **TARGET ACCOUNTS**, of the existence of the warrant until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date the requested warrant is signed by the magistrate judge, or such later date as may be set by the Court upon application for an extension by the United States. There is reason to believe that such notification will result in: (1) flight from prosecution; (2) destruction of or tampering with evidence; (3) intimidation of potential witnesses; (4) otherwise seriously jeopardizing the investigation; or (5) exposing the identities of confidential sources who have cooperated with the government and in some cases may continue to actively and covertly cooperate.

XI. CONCLUSION

135. Based on the foregoing, I request that the Court issue the requested search warrants.

ANDREW CIVETTI, Special Agent
Federal Bureau of
Investigation

Subscribed to and sworn before
me on January 31, 2020.

HONORABLE PATRICK J. WALSH
UNITED STATES MAGISTRATE JUDGE

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

EXHIBIT 2

From: Leela Kapur <leela.kapur@lacity.org>
Received(Date): Mon, 25 Mar 2019 00:28:55 +0100
Subject: Jim's Deposition
To: Mike Feuer <mike.feuer@lacity.org>

Mike: The following are some excerpts from Jim's depo. I am paraphrasing but you will get the gist. O: indicates his original response and R: his revised. A: answers that weren't amended. Statements in quotation marks are statements Jim made (again sometimes paraphrased) but without the question attached. While I suspect much of this can be explained as the questions were less than precise, etc., I wanted you to get a feeling for the breadth of the confusing responses — many of which are not objectively clarified through documentation.

Did Mr. Tom tell you he was aware that P had an atty/client relationship with Jones?
O: I think so
R: He did not

Did P brief any (of our DWP attorneys) on nature of his representation of Jones?
O: I don't know
R: They say he did not.

Was Maribeth provided a copy of draft complaint?
O: Yes
R: No apparently not.

In talking about the Liner memo cautioning against P dual representation of City and Jones v. PWC — Did Liner provide memo to City Attorney's office?
O: I don't know.
R: Yes
O: We don't have a copy now
R: We do

"I discarded my notes last Friday. I don't need them (4-5 pages). Doesn't know and didn't ask if a retention order in place."

Inconsistent testimony as to whether he knew of the draft complaint before Thom requested it be prepared.

"I understand there were 2 draft complaints. One was sent to Jones — no City person saw it. Just learned of it but I was screened so someone else may have known of it."

Was Feuer part of decision to not file Jones v. PWC complaint?
O: I don't remember Mike taking part in that discussion. I am sure I reported it to him but don't think he was involved decision.
R: I don' think he was involved in the recommendation.

When did he (Feuer) first learn of the existence of the complaint?
A: I have no idea.

Did you apprise him (Feuer) of the fact?

A: I'm sure I did. We met twice a week. I advised him of what's going on. I have no specific recollection of advising him.

At any time did City Attorney or DWP voice concerns about propriety of P serving as counsel for Jones and City?
O: Not that I recall.
R: Yes, Richard Tom passed on outside counsel advice that shouldn't represent both against PWC.

"I am sure I heard Landskroner's (LK) name before 4/1/15." But then "learn of LK when complaint came out." But then "heard of him before that by a few days." And "When it became clear to P that PWC suit by Jones not going forward, P contacted LK, with whom he had a prior relationship based on another case and Cleveland system issues."

Did you understand at that time Jones had determined to sue LA?
A: I think we were told that.

Your understanding that before 3/26, Jones had instructed P to file against the City?
A: I don't know. P told me the he told Jones that couldn't represent him because Jones wanted to sue City not PWC.

Did P tell you he told Jones that P represented the City?
A: Sure Jones was aware. Because there two suits were contemplated. One by DWP and one by Jones.

Your understanding that 4/1/15 complaint against DWP was originally drafted by P?
A: I think he had — not sure— he had some role
A: Based on P, he prepared the earlier complaint and gave to LK.
A: (after lunch break) Clarified that he meant that P had given other class complaints to LK. No reason to believe P and role in actual drafting of the complaint against DWP. Don't know one way or the other.

Do you know if ever a time in their relationship that Jones was NOT considering potential suits against DWP?
A: I don't. P may have told me that LK would be filing against DWP.

Did any one in City Attorney's office authorize P to bring in LK for purpose of suing City?
O: I think the City was informed that once P concluded to have a conflict. I assume somebody authorized it but not me.
R: Struck last sentence.

At point P recommending LK, you personally understood reason was for LK to sue City?
O: Correct
R: Correct as to PWC, not City.

Why not refer Jones to Blood or other class plaintiff counsel?
A: They were unreasonable. Refused to toll claims. LK more reasonable, based on P.
O: Understnding from Liner that Blood et al were intransigent. Didn't want to negotiate. Were not acceptable. Didn't have same goals as DWP.

R: I don't know why P recommended to Jones.

No one brought LK into case because viewed as someone who would be most zealous advocate for Jones?
O: That's right
R: Don't know why P recommended him.

"Sure we knew before 4/1/15 that Jones would be filing against City."

Did you know there would be an immediate settlement request?
A: We were trying to settle. I think I knew.

Some questions about a meeting or phone call between Feuer, Blood and Clark. Jim doesn't remember it.

"P provided LK other complaints for purpose of making easier for LK to draft complaint covering all causes of action."

When asked about City's knowledge of LK's actual hours worked, Jim stated we agreed to the fees without seeing hours claimed.

How much earlier than 4/1/15 did you know the settlement demand would be forthcoming at some point and you would be settling with Jones?
O: Sometime letter half to end of March.
R: I didn't

P was involved in remediation before filing of Jones complaint?
O: I think that is right
R: No

He was asked why P participated in Jim's due diligence interviews as he was prepping for PMK depo (e.g., interviews with our CA staff and DWP staff). Jim didn't really answer the question.

Sent from my iPad

--
**********Confidentiality Notice **********
This
electronic message transmission contains information
from the Office of the
Los Angeles City Attorney, which may be confidential or protected by the attorney-client privilege and/or the work product doctrine. If you are not the intended recipient, be aware that any disclosure, copying, distribution
or use of the content of this information is prohibited. If you have received this communication in error, please notify us immediately by e-mail and delete the original message and any attachments without reading or saving in any manner.

****

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
MICHAEL "MIKE" FEUER, Date of Birth [redacted] 1958

Case No. 2:20-MJ-3799

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California:

See Attachment A-1

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by referenced

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 8/14/2020 4:00 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh- United States Magistrate Judge
Printed name and title

AUSA: Melissa Mills

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

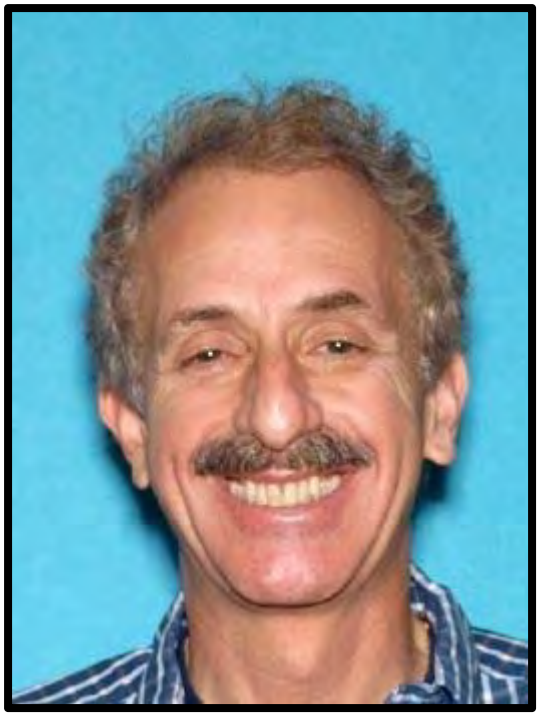
_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-1

PROPERTY TO BE SEARCHED

The person to be searched is **MICHAEL "MIKE" FEUER**, date of birth [redacted] 1958, as pictured below:



Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

ATTACHMENT B

I. CELL PHONE ITEMS TO BE SEIZED

1. Law enforcement personnel are authorized to seize the cellular telephones with telephone numbers [redacted] ("**FEUER'S PHONE**"), [redacted] ("**KAPUR'S PHONE**"), and [redacted] ("**BRAJEVICH'S PHONE**") (collectively, the "**TARGET PHONES**" or the "digital devices").

2. During the execution of this search warrant, law enforcement is permitted to: (1) depress the thumb and/or fingers of **MIKE FEUER**, **LEELA KAPUR**, or **JOSEPH BRAJEVICH** onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of **FEUER, KAPUR,** or **BRAJEVICH** with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

3. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations, between November 1, 2017, and the present, of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False

Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding) (collectively, the "Subject Offenses"), namely:

a. Information as to who accessed or used the **TARGET PHONES**, including records about their identities.

b. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Retention of PAUL PARADIS and PAUL KIESEL, or entities related thereto, to represent the City of Los Angeles, and the ensuing representation;

ii. Communications involving or about any party to, or to counsel for any party to, *Jones v. City of Los Angeles* (the "*Jones* matter") or *City of Los Angeles v. PricewaterhouseCoopers* (the "*PwC* matter"), including communications regarding these matters with or referencing the persons identified in paragraphs 10-22 of Exhibit 1 to the affidavit supporting this warrant, and other counsel for and parties to these matters;

iii. The litigation of the *Jones* matter and the *PwC* matter, including discovery disputes, the deposition of the City's "person most qualified," and emails and other materials arguably or allegedly responsive to discovery demands or court orders;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

iv. Efforts to conceal the litigation practices of the City Attorney's Office's or members or representatives thereof in the litigation involving the LADWP billing system;

v. Efforts to conceal actions by the City Attorney's Office or members or representatives thereof in the litigation involving the LADWP billing system, including shielding documents from production, filing false or misleading documents with the court, and offering false or misleading testimony;

vi. The City's actions, strategy, or tactics in responding to revelations or allegations of fraud, discovery violations, and unethical conduct in the litigation involving the LADWP billing system, including media outreach and contacts, litigation decisions, and notification or lack of notification to the court of relevant developments;

vii. Negotiations or agreements to conceal business practices used in the LADWP billing litigation by the City Attorney's Office or members thereof, and communications involving or referencing the same;

viii. Destruction or concealment of evidence relevant to the LADWP billing litigation.

c. Any **TARGET PHONE** which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

d. With respect to any **TARGET PHONE** containing evidence falling within the scope of the foregoing categories of items to be seized:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

5. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

6. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

review only digital device data which has been released by the Privilege Review Team.

7. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

8. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

9. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

10. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

11. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

12. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

13. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

14. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

15. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001317
Page 1317 of 1425

data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

16. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

17. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

18. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

19. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of Los Angeles City Hall East, 200 N. Main Street, 8th Floor, Los Angeles, CA, Office of the City Attorney ("**FEUER's OFFICE**")	)	Case No. 2:20-MJ-3800

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California:

See Attachment A-2

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by referenced

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 8/14/2020 4:00 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh- United States Magistrate Judge
Printed name and title

AUSA: Melissa Mills

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-2

PROPERTY TO BE SEARCHED

The premise to be searched is Los Angeles City Hall East, 200 N. Main Street, 8th Floor, Los Angeles, CA, Office of the City Attorney ("**FEUER's OFFICE**").

ATTACHMENT B

I. CELL PHONE ITEMS TO BE SEIZED

1. Law enforcement personnel are authorized to seize the cellular telephones with telephone numbers [redacted] ("**FEUER'S PHONE**"), [redacted] ("**KAPUR'S PHONE**"), and [redacted] ("**BRAJEVICH'S PHONE**") (collectively, the "**TARGET PHONES**" or the "digital devices").

2. During the execution of this search warrant, law enforcement is permitted to: (1) depress the thumb and/or fingers of **MIKE FEUER**, **LEELA KAPUR**, or **JOSEPH BRAJEVICH** onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of **FEUER, KAPUR,** or **BRAJEVICH** with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

3. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations, between November 1, 2017, and the present, of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False

Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding) (collectively, the "Subject Offenses"), namely:

a. Information as to who accessed or used the **TARGET PHONES**, including records about their identities.

b. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Retention of PAUL PARADIS and PAUL KIESEL, or entities related thereto, to represent the City of Los Angeles, and the ensuing representation;

ii. Communications involving or about any party to, or to counsel for any party to, *Jones v. City of Los Angeles* (the "*Jones* matter") or *City of Los Angeles v. PricewaterhouseCoopers* (the "*PwC* matter"), including communications regarding these matters with or referencing the persons identified in paragraphs 10-22 of Exhibit 1 to the affidavit supporting this warrant, and other counsel for and parties to these matters;

iii. The litigation of the *Jones* matter and the *PwC* matter, including discovery disputes, the deposition of the City's "person most qualified," and emails and other materials arguably or allegedly responsive to discovery demands or court orders;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

iv. Efforts to conceal the litigation practices of the City Attorney's Office's or members or representatives thereof in the litigation involving the LADWP billing system;

v. Efforts to conceal actions by the City Attorney's Office or members or representatives thereof in the litigation involving the LADWP billing system, including shielding documents from production, filing false or misleading documents with the court, and offering false or misleading testimony;

vi. The City's actions, strategy, or tactics in responding to revelations or allegations of fraud, discovery violations, and unethical conduct in the litigation involving the LADWP billing system, including media outreach and contacts, litigation decisions, and notification or lack of notification to the court of relevant developments;

vii. Negotiations or agreements to conceal business practices used in the LADWP billing litigation by the City Attorney's Office or members thereof, and communications involving or referencing the same;

viii. Destruction or concealment of evidence relevant to the LADWP billing litigation.

c. Any **TARGET PHONE** which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

d. With respect to any **TARGET PHONE** containing evidence falling within the scope of the foregoing categories of items to be seized:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

5. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

6. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

review only digital device data which has been released by the Privilege Review Team.

7. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

8. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

9. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001328
Page 1328 of 1425

by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

10. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

11. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001329
Page 1329 of 1425

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

12. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

13. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

14. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

15. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001330
Page 1330 of 1425

data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

16. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

17. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

18. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

19. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
[redacted], Los Angeles, California,
("**FEUER's RESIDENCE**")

Case No. 2:20-MJ-3801

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California:

See Attachment A-2

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by referenced

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for____days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 8/14/2020 4:00 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh- United States Magistrate Judge
Printed name and title

AUSA: Melissa Mills

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-3

PROPERTY TO BE SEARCHED

The premises to be search is [redacted], Los Angeles, California, ("**FEUER's RESIDENCE**"). FEUER's RESIDENCE is pictured below.

[redacted]

ATTACHMENT B

I. CELL PHONE ITEMS TO BE SEIZED

1. Law enforcement personnel are authorized to seize the cellular telephones with telephone numbers [redacted] ("**FEUER'S PHONE**"), [redacted] ("**KAPUR'S PHONE**"), and [redacted] ("**BRAJEVICH'S PHONE**") (collectively, the "**TARGET PHONES**" or the "digital devices").

2. During the execution of this search warrant, law enforcement is permitted to: (1) depress the thumb and/or fingers of **MIKE FEUER**, **LEELA KAPUR**, or **JOSEPH BRAJEVICH** onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of **FEUER, KAPUR,** or **BRAJEVICH** with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

3. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations, between November 1, 2017, and the present, of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False

Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding) (collectively, the "Subject Offenses"), namely:

a. Information as to who accessed or used the **TARGET PHONES**, including records about their identities.

b. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Retention of PAUL PARADIS and PAUL KIESEL, or entities related thereto, to represent the City of Los Angeles, and the ensuing representation;

ii. Communications involving or about any party to, or to counsel for any party to, *Jones v. City of Los Angeles* (the "*Jones* matter") or *City of Los Angeles v. PricewaterhouseCoopers* (the "*PwC* matter"), including communications regarding these matters with or referencing the persons identified in paragraphs 10-22 of Exhibit 1 to the affidavit supporting this warrant, and other counsel for and parties to these matters;

iii. The litigation of the *Jones* matter and the *PwC* matter, including discovery disputes, the deposition of the City's "person most qualified," and emails and other materials arguably or allegedly responsive to discovery demands or court orders;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

iv. Efforts to conceal the litigation practices of the City Attorney's Office's or members or representatives thereof in the litigation involving the LADWP billing system;

v. Efforts to conceal actions by the City Attorney's Office or members or representatives thereof in the litigation involving the LADWP billing system, including shielding documents from production, filing false or misleading documents with the court, and offering false or misleading testimony;

vi. The City's actions, strategy, or tactics in responding to revelations or allegations of fraud, discovery violations, and unethical conduct in the litigation involving the LADWP billing system, including media outreach and contacts, litigation decisions, and notification or lack of notification to the court of relevant developments;

vii. Negotiations or agreements to conceal business practices used in the LADWP billing litigation by the City Attorney's Office or members thereof, and communications involving or referencing the same;

viii. Destruction or concealment of evidence relevant to the LADWP billing litigation.

c. Any **TARGET PHONE** which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

d. With respect to any **TARGET PHONE** containing evidence falling within the scope of the foregoing categories of items to be seized:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

5. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

6. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

review only digital device data which has been released by the Privilege Review Team.

7. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

8. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

9. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

10. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

11. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

12. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

13. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

14. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

15. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001343
Page 1343 of 1425

data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

16. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

17. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

18. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

19. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
LEELA KAPUR, date of birth [redacted] 1961

Case No. 2:20-MJ-3802

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California:

See Attachment A-4

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by referenced

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 8/14/2020 4:00 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh- United States Magistrate Judge
Printed name and title

AUSA: Melissa Mills

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-4

PROPERTY TO BE SEARCHED

The person to be searched is **LEELA KAPUR**, date of birth [redacted] 1961, as pictured below:

ATTACHMENT B

I. CELL PHONE ITEMS TO BE SEIZED

1. Law enforcement personnel are authorized to seize the cellular telephones with telephone numbers [redacted] ("**FEUER'S PHONE**"), [redacted] ("**KAPUR'S PHONE**"), and [redacted] ("**BRAJEVICH'S PHONE**") (collectively, the "**TARGET PHONES**" or the "digital devices").

2. During the execution of this search warrant, law enforcement is permitted to: (1) depress the thumb and/or fingers of **MIKE FEUER**, **LEELA KAPUR**, or **JOSEPH BRAJEVICH** onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of **FEUER, KAPUR,** or **BRAJEVICH** with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

3. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations, between November 1, 2017, and the present, of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False

Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding) (collectively, the "Subject Offenses"), namely:

a. Information as to who accessed or used the **TARGET PHONES**, including records about their identities.

b. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Retention of PAUL PARADIS and PAUL KIESEL, or entities related thereto, to represent the City of Los Angeles, and the ensuing representation;

ii. Communications involving or about any party to, or to counsel for any party to, *Jones v. City of Los Angeles* (the "*Jones* matter") or *City of Los Angeles v. PricewaterhouseCoopers* (the "*PwC* matter"), including communications regarding these matters with or referencing the persons identified in paragraphs 10-22 of Exhibit 1 to the affidavit supporting this warrant, and other counsel for and parties to these matters;

iii. The litigation of the *Jones* matter and the *PwC* matter, including discovery disputes, the deposition of the City's "person most qualified," and emails and other materials arguably or allegedly responsive to discovery demands or court orders;

iv. Efforts to conceal the litigation practices of the City Attorney's Office's or members or representatives thereof in the litigation involving the LADWP billing system;

v. Efforts to conceal actions by the City Attorney's Office or members or representatives thereof in the litigation involving the LADWP billing system, including shielding documents from production, filing false or misleading documents with the court, and offering false or misleading testimony;

vi. The City's actions, strategy, or tactics in responding to revelations or allegations of fraud, discovery violations, and unethical conduct in the litigation involving the LADWP billing system, including media outreach and contacts, litigation decisions, and notification or lack of notification to the court of relevant developments;

vii. Negotiations or agreements to conceal business practices used in the LADWP billing litigation by the City Attorney's Office or members thereof, and communications involving or referencing the same;

viii. Destruction or concealment of evidence relevant to the LADWP billing litigation.

c. Any **TARGET PHONE** which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

d. With respect to any **TARGET PHONE** containing evidence falling within the scope of the foregoing categories of items to be seized:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

5. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

6. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001353
Page 1353 of 1425

review only digital device data which has been released by the Privilege Review Team.

7. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

8. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

9. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001354
Page 1354 of 1425

by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

10. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

11. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001355
Page 1355 of 1425

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

12. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

13. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

14. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

15. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001356
Page 1356 of 1425

data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

16. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

17. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

18. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

19. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
[redacted]-2:20-MJ-3802	8/26/2020, 3:15PM	Leela Kapur

Inventory made in the presence of:
SA Nicolls, SA Losen + Leela Kapur

Inventory of the property taken and name of any person(s) seized:

see attached

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 8/27/2020

Kathleen Nicolls
Executing officer's signature

Kathleen Nicolls, Special Agent
Printed name and title

FD-597 (Rev. 4-13-2015) Page 1 of 1

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property

[redacted]

Case ID: 194B-LA-3082417

On (date) _____

item (s) listed below were:
- [x] Collected/Seized
- [ ] Received From
- [ ] Returned To
- [ ] Released To

(Name) LEELA KAPUR, [redacted]

(Street Address) 200 Main St., 8th Floor, ~~#~~

(City) Los Angeles, CA

Description of Item (s):

PW [redacted]

I Phone SE
Serial # F17575G8H2XG

KW

Received By: Kathleen Nicolls (Signature) Received From: Leela Kapur (Signature)

Printed Name/Title: Kathleen Nicolls Special Agent Printed Name/Title: Leela Kapur

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of Los Angeles City Hall East, 200 N. Main Street, 8th Floor, Los Angeles, CA, Office of the Chief of Staff to the City Attorney ("**KAPUR's OFFICE**")	)	Case No. 2:20-MJ-3803

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California:

See Attachment A-5

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by referenced

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 8/14/2020 4:00 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh- United States Magistrate Judge
Printed name and title

AUSA: Melissa Mills

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-5

PROPERTY TO BE SEARCHED

The premises to be search is Los Angeles City Hall East, 200 N. Main Street, 8th Floor, Los Angeles, CA, Office of the Chief of Staff to the City Attorney ("**KAPUR's OFFICE**").

ATTACHMENT B

I. CELL PHONE ITEMS TO BE SEIZED

1. Law enforcement personnel are authorized to seize the cellular telephones with telephone numbers [redacted] ("**FEUER'S PHONE**"), [redacted] ("**KAPUR'S PHONE**"), and [redacted] ("**BRAJEVICH'S PHONE**") (collectively, the "**TARGET PHONES**" or the "digital devices").

2. During the execution of this search warrant, law enforcement is permitted to: (1) depress the thumb and/or fingers of **MIKE FEUER**, **LEELA KAPUR**, or **JOSEPH BRAJEVICH** onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of **FEUER, KAPUR,** or **BRAJEVICH** with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

3. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations, between November 1, 2017, and the present, of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False

Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding) (collectively, the "Subject Offenses"), namely:

a. Information as to who accessed or used the **TARGET PHONES**, including records about their identities.

b. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Retention of PAUL PARADIS and PAUL KIESEL, or entities related thereto, to represent the City of Los Angeles, and the ensuing representation;

ii. Communications involving or about any party to, or to counsel for any party to, *Jones v. City of Los Angeles* (the "*Jones* matter") or *City of Los Angeles v. PricewaterhouseCoopers* (the "*PwC* matter"), including communications regarding these matters with or referencing the persons identified in paragraphs 10-22 of Exhibit 1 to the affidavit supporting this warrant, and other counsel for and parties to these matters;

iii. The litigation of the *Jones* matter and the *PwC* matter, including discovery disputes, the deposition of the City's "person most qualified," and emails and other materials arguably or allegedly responsive to discovery demands or court orders;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

iv. Efforts to conceal the litigation practices of the City Attorney's Office's or members or representatives thereof in the litigation involving the LADWP billing system;

v. Efforts to conceal actions by the City Attorney's Office or members or representatives thereof in the litigation involving the LADWP billing system, including shielding documents from production, filing false or misleading documents with the court, and offering false or misleading testimony;

vi. The City's actions, strategy, or tactics in responding to revelations or allegations of fraud, discovery violations, and unethical conduct in the litigation involving the LADWP billing system, including media outreach and contacts, litigation decisions, and notification or lack of notification to the court of relevant developments;

vii. Negotiations or agreements to conceal business practices used in the LADWP billing litigation by the City Attorney's Office or members thereof, and communications involving or referencing the same;

viii. Destruction or concealment of evidence relevant to the LADWP billing litigation.

c. Any **TARGET PHONE** which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

d. With respect to any **TARGET PHONE** containing evidence falling within the scope of the foregoing categories of items to be seized:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001366
Page 1366 of 1425

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

5. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

6. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

review only digital device data which has been released by the Privilege Review Team.

7. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

8. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

9. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001369
Page 1369 of 1425

by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

10. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

11. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001370
Page 1370 of 1425

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

12. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

13. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

14. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

15. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001371
Page 1371 of 1425

data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

16. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

17. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

18. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

19. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
[redacted], Toluca Lake, California,
("**KAPUR's RESIDENCE**")

Case No. 2:20-MJ-3804

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California:

See Attachment A-6

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by referenced

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 8/14/2020 4:00 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh- United States Magistrate Judge
Printed name and title

AUSA: Melissa Mills

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

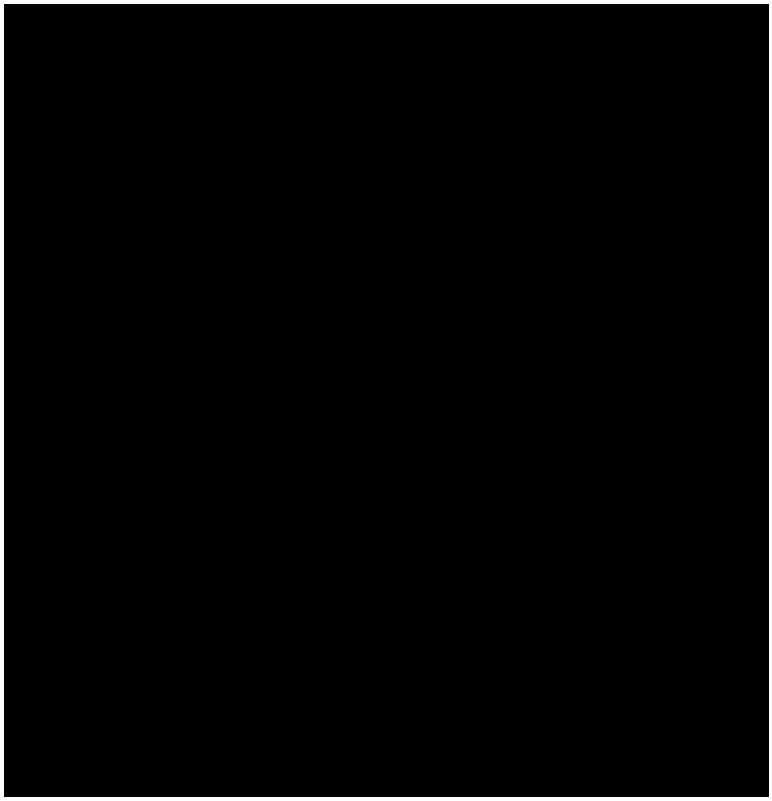
_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-6

PROPERTY TO BE SEARCHED

The premises to be search is [redacted] Toluca Lake, California, ("**KAPUR's RESIDENCE**"). KAPUR's RESIDENCE is pictured below.



ATTACHMENT B

I. CELL PHONE ITEMS TO BE SEIZED

1. Law enforcement personnel are authorized to seize the cellular telephones with telephone numbers [redacted] ("**FEUER'S PHONE**"), [redacted] ("**KAPUR'S PHONE**"), and [redacted] ("**BRAJEVICH'S PHONE**") (collectively, the "**TARGET PHONES**" or the "digital devices").

2. During the execution of this search warrant, law enforcement is permitted to: (1) depress the thumb and/or fingers of **MIKE FEUER**, **LEELA KAPUR**, or **JOSEPH BRAJEVICH** onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of **FEUER, KAPUR,** or **BRAJEVICH** with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

3. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations, between November 1, 2017, and the present, of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False

Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding) (collectively, the "Subject Offenses"), namely:

a. Information as to who accessed or used the **TARGET PHONES**, including records about their identities.

b. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Retention of PAUL PARADIS and PAUL KIESEL, or entities related thereto, to represent the City of Los Angeles, and the ensuing representation;

ii. Communications involving or about any party to, or to counsel for any party to, *Jones v. City of Los Angeles* (the "*Jones* matter") or *City of Los Angeles v. PricewaterhouseCoopers* (the "*PwC* matter"), including communications regarding these matters with or referencing the persons identified in paragraphs 10-22 of Exhibit 1 to the affidavit supporting this warrant, and other counsel for and parties to these matters;

iii. The litigation of the *Jones* matter and the *PwC* matter, including discovery disputes, the deposition of the City's "person most qualified," and emails and other materials arguably or allegedly responsive to discovery demands or court orders;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

iv. Efforts to conceal the litigation practices of the City Attorney's Office's or members or representatives thereof in the litigation involving the LADWP billing system;

v. Efforts to conceal actions by the City Attorney's Office or members or representatives thereof in the litigation involving the LADWP billing system, including shielding documents from production, filing false or misleading documents with the court, and offering false or misleading testimony;

vi. The City's actions, strategy, or tactics in responding to revelations or allegations of fraud, discovery violations, and unethical conduct in the litigation involving the LADWP billing system, including media outreach and contacts, litigation decisions, and notification or lack of notification to the court of relevant developments;

vii. Negotiations or agreements to conceal business practices used in the LADWP billing litigation by the City Attorney's Office or members thereof, and communications involving or referencing the same;

viii. Destruction or concealment of evidence relevant to the LADWP billing litigation.

c. Any **TARGET PHONE** which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

d. With respect to any **TARGET PHONE** containing evidence falling within the scope of the foregoing categories of items to be seized:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

5. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

6. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

review only digital device data which has been released by the Privilege Review Team.

7. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

8. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

9. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001382
Page 1382 of 1425

by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

10. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

11. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

12. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

13. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

14. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

15. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

16. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

17. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

18. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

19. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of)
)
)
JOSEPH BRAJEVICH, date of birth [redacted],)
1965)
)
)
)
)

Case No. 2:20-MJ-3805

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California:

See Attachment A-7

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by referenced

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 8/14/2020 4:00 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh- United States Magistrate Judge
Printed name and title

AUSA: Melissa Mills

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-7

PROPERTY TO BE SEARCHED

The person to be searched is **JOSEPH BRAJEVICH**, date of birth [redacted] 1965, as pictured below:

ATTACHMENT B

I. CELL PHONE ITEMS TO BE SEIZED

1. Law enforcement personnel are authorized to seize the cellular telephones with telephone numbers [redacted] ("**FEUER'S PHONE**"), [redacted] ("**KAPUR'S PHONE**"), and [redacted] ("**BRAJEVICH'S PHONE**") (collectively, the "**TARGET PHONES**" or the "digital devices").

2. During the execution of this search warrant, law enforcement is permitted to: (1) depress the thumb and/or fingers of **MIKE FEUER**, **LEELA KAPUR**, or **JOSEPH BRAJEVICH** onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of **FEUER, KAPUR,** or **BRAJEVICH** with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

3. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations, between November 1, 2017, and the present, of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False

Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding) (collectively, the "Subject Offenses"), namely:

a. Information as to who accessed or used the **TARGET PHONES**, including records about their identities.

b. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Retention of PAUL PARADIS and PAUL KIESEL, or entities related thereto, to represent the City of Los Angeles, and the ensuing representation;

ii. Communications involving or about any party to, or to counsel for any party to, *Jones v. City of Los Angeles* (the "*Jones* matter") or *City of Los Angeles v. PricewaterhouseCoopers* (the "*PwC* matter"), including communications regarding these matters with or referencing the persons identified in paragraphs 10-22 of Exhibit 1 to the affidavit supporting this warrant, and other counsel for and parties to these matters;

iii. The litigation of the *Jones* matter and the *PwC* matter, including discovery disputes, the deposition of the City's "person most qualified," and emails and other materials arguably or allegedly responsive to discovery demands or court orders;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

iv. Efforts to conceal the litigation practices of the City Attorney's Office's or members or representatives thereof in the litigation involving the LADWP billing system;

v. Efforts to conceal actions by the City Attorney's Office or members or representatives thereof in the litigation involving the LADWP billing system, including shielding documents from production, filing false or misleading documents with the court, and offering false or misleading testimony;

vi. The City's actions, strategy, or tactics in responding to revelations or allegations of fraud, discovery violations, and unethical conduct in the litigation involving the LADWP billing system, including media outreach and contacts, litigation decisions, and notification or lack of notification to the court of relevant developments;

vii. Negotiations or agreements to conceal business practices used in the LADWP billing litigation by the City Attorney's Office or members thereof, and communications involving or referencing the same;

viii. Destruction or concealment of evidence relevant to the LADWP billing litigation.

c. Any **TARGET PHONE** which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

d. With respect to any **TARGET PHONE** containing evidence falling within the scope of the foregoing categories of items to be seized:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

5. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

6. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

review only digital device data which has been released by the Privilege Review Team.

7. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

8. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

9. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

10. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

11. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001396
Page 1396 of 1425

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

12. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

13. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

14. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

15. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001397
Page 1397 of 1425

data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

16. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

17. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

18. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

19. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of Los Angeles Department of Water and Power, 221 N. Figueroa Street, 10th Floor, Los Angeles, CA, Office of the General Counsel ("**BRAJEVICH'S OFFICE**").	)	Case No. 2:20-MJ-3806

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California:

See Attachment A-8

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by referenced

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for____days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 8/14/2020 4:00 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh- United States Magistrate Judge
Printed name and title

AUSA: Melissa Mills

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-8

PROPERTY TO BE SEARCHED

The premises to be searched is Los Angeles Department of Water and Power, 221 N. Figueroa Street, 10th Floor, Los Angeles, CA, Office of the General Counsel ("**BRAJEVICH'S OFFICE**").

ATTACHMENT B

I. CELL PHONE ITEMS TO BE SEIZED

1. Law enforcement personnel are authorized to seize the cellular telephones with telephone numbers [redacted] ("**FEUER'S PHONE**"), [redacted] ("**KAPUR'S PHONE**"), and [redacted] ("**BRAJEVICH'S PHONE**") (collectively, the **"TARGET PHONES"** or the "digital devices").

2. During the execution of this search warrant, law enforcement is permitted to: (1) depress the thumb and/or fingers of **MIKE FEUER**, **LEELA KAPUR**, or **JOSEPH BRAJEVICH** onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of **FEUER, KAPUR,** or **BRAJEVICH** with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

3. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations, between November 1, 2017, and the present, of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False

Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding) (collectively, the "Subject Offenses"), namely:

a. Information as to who accessed or used the **TARGET PHONES**, including records about their identities.

b. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Retention of PAUL PARADIS and PAUL KIESEL, or entities related thereto, to represent the City of Los Angeles, and the ensuing representation;

ii. Communications involving or about any party to, or to counsel for any party to, *Jones v. City of Los Angeles* (the "*Jones* matter") or *City of Los Angeles v. PricewaterhouseCoopers* (the "*PwC* matter"), including communications regarding these matters with or referencing the persons identified in paragraphs 10-22 of Exhibit 1 to the affidavit supporting this warrant, and other counsel for and parties to these matters;

iii. The litigation of the *Jones* matter and the *PwC* matter, including discovery disputes, the deposition of the City's "person most qualified," and emails and other materials arguably or allegedly responsive to discovery demands or court orders;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

iv. Efforts to conceal the litigation practices of the City Attorney's Office's or members or representatives thereof in the litigation involving the LADWP billing system;

v. Efforts to conceal actions by the City Attorney's Office or members or representatives thereof in the litigation involving the LADWP billing system, including shielding documents from production, filing false or misleading documents with the court, and offering false or misleading testimony;

vi. The City's actions, strategy, or tactics in responding to revelations or allegations of fraud, discovery violations, and unethical conduct in the litigation involving the LADWP billing system, including media outreach and contacts, litigation decisions, and notification or lack of notification to the court of relevant developments;

vii. Negotiations or agreements to conceal business practices used in the LADWP billing litigation by the City Attorney's Office or members thereof, and communications involving or referencing the same;

viii. Destruction or concealment of evidence relevant to the LADWP billing litigation.

c. Any **TARGET PHONE** which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

d. With respect to any **TARGET PHONE** containing evidence falling within the scope of the foregoing categories of items to be seized:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

5. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

6. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

review only digital device data which has been released by the Privilege Review Team.

7. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

8. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

9. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001408
Page 1408 of 1425

by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

10. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

11. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB
USAO_001409
Page 1409 of 1425

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

12. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

13. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

14. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

15. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

16. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

17. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

18. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

19. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of [redacted], Los Angeles, California, ("**BRAJEVICH's RESIDENCE**")	)	Case No. 2:20-MJ-3807

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California:

See Attachment A-9

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by referenced

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 8/14/2020 4:00 p.m.

Patrick J. Walsh
Judge's signature

City and state: Los Angeles, CA

Patrick J. Walsh- United States Magistrate Judge
Printed name and title

AUSA: Melissa Mills

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-9

PROPERTY TO BE SEARCHED

The premises to be search is [redacted], Los Angeles, California, ("**BRAJEVICH's RESIDENCE**"). BRAJEVICH's RESIDENCE is pictured below.

ATTACHMENT B

I. CELL PHONE ITEMS TO BE SEIZED

1. Law enforcement personnel are authorized to seize the cellular telephones with telephone numbers [redacted] ("**FEUER'S PHONE**"), [redacted] ("**KAPUR'S PHONE**"), and [redacted] ("**BRAJEVICH'S PHONE**") (collectively, the "**TARGET PHONES**" or the "digital devices").

2. During the execution of this search warrant, law enforcement is permitted to: (1) depress the thumb and/or fingers of **MIKE FEUER**, **LEELA KAPUR**, or **JOSEPH BRAJEVICH** onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of **FEUER, KAPUR,** or **BRAJEVICH** with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

3. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations, between November 1, 2017, and the present, of 18 U.S.C. §§ 371 (Conspiracy); 666 (Bribery and Kickbacks Concerning Federal Funds); 1001 (False

Statements); 1341 (Mail Fraud); 1343 (Wire Fraud); 1346 (Deprivation of Honest Services); 1505 (Obstructing Federal Proceeding); 1510 (Obstruction of Justice); 1951 (Extortion); 1956 (Money Laundering); and 1621 (Perjury in a Federal Proceeding) (collectively, the "Subject Offenses"), namely:

a. Information as to who accessed or used the **TARGET PHONES**, including records about their identities.

b. Records, documents, communications, memoranda, agendas, minutes, notes, calendar entries, recordings, programs, applications, or other materials referencing:

i. Retention of PAUL PARADIS and PAUL KIESEL, or entities related thereto, to represent the City of Los Angeles, and the ensuing representation;

ii. Communications involving or about any party to, or to counsel for any party to, *Jones v. City of Los Angeles* (the "*Jones* matter") or *City of Los Angeles v. PricewaterhouseCoopers* (the "*PwC* matter"), including communications regarding these matters with or referencing the persons identified in paragraphs 10-22 of Exhibit 1 to the affidavit supporting this warrant, and other counsel for and parties to these matters;

iii. The litigation of the *Jones* matter and the *PwC* matter, including discovery disputes, the deposition of the City's "person most qualified," and emails and other materials arguably or allegedly responsive to discovery demands or court orders;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

iv. Efforts to conceal the litigation practices of the City Attorney's Office's or members or representatives thereof in the litigation involving the LADWP billing system;

v. Efforts to conceal actions by the City Attorney's Office or members or representatives thereof in the litigation involving the LADWP billing system, including shielding documents from production, filing false or misleading documents with the court, and offering false or misleading testimony;

vi. The City's actions, strategy, or tactics in responding to revelations or allegations of fraud, discovery violations, and unethical conduct in the litigation involving the LADWP billing system, including media outreach and contacts, litigation decisions, and notification or lack of notification to the court of relevant developments;

vii. Negotiations or agreements to conceal business practices used in the LADWP billing litigation by the City Attorney's Office or members thereof, and communications involving or referencing the same;

viii. Destruction or concealment of evidence relevant to the LADWP billing litigation.

c. Any **TARGET PHONE** which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

d. With respect to any **TARGET PHONE** containing evidence falling within the scope of the foregoing categories of items to be seized:

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

5. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

6. The Privilege Review Team will review the identified digital devices as set forth herein. The Search Team will

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

review only digital device data which has been released by the Privilege Review Team.

7. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

8. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms, names of any identified spouses or their email addresses, and generic words such as "privileged" "work product." The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

9. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team ("PRT") member to confirm that they contain potentially privileged information. Documents or data that are determined

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT attorney Documents or data identified by the PRT attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT attorney determines it to be appropriate, the PRT attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

10. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

11. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

12. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

13. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

14. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

15. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain forensic copies of the digital device but may not access

Provided Pursuant to 4/16/2024 Court Order (Dkt. No. 24)
In Re Application of Consumer Watchdog et al., 2:24-cv-01650-SB

data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

16. The government may also retain a digital device if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

17. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

18. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

19. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.