

UNITED STATES DISTRICT COURT

for the

Northern District of California

United States of America)

v.)

JOSEPH SULLIVAN)

Case No. 3-20-71168 JCS)

Defendant

SUMMONS IN A CRIMINAL CASE

YOU ARE SUMMONED to appear before the United States district court at the time, date, and place set forth below to answer to one or more offenses or violations based on the following document filed with the court:

- Indictment Superseding Indictment Information Superseding Information Complaint
- Probation Violation Petition Supervised Release Violation Petition Violation Notice Order of Court

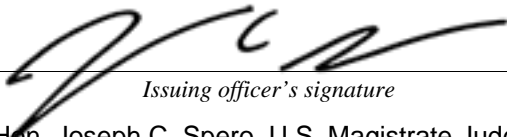
U.S. Marshals Service, Northern District of California Place: 450 Golden Gate Avenue, 20th Floor San Francisco, CA 94102	Courtroom No.: N/A <hr/> Date and Time: 08/27/2020 10:00 am
--	--

This offense is briefly described as follows:

- Obstruction of Justice, in violation of 18 U.S.C. § 1505 (One Count)
- Misprision of a Felony, in violation of 18 U.S.C. § 4 (One Count)

This summons directs you to U.S. Marshals Service for federal processing. The U.S. Marshals will provide you with additional information regarding your initial (telephonic) appearance before the U.S. Magistrate Judge.

Date: 08/19/2020



Issuing officer's signature
 Hon. Joseph C. Spero, U.S. Magistrate Judge

Printed name and title

I declare under penalty of perjury that I have:

- Executed and returned this summons
- Returned this summons unexecuted

Date: _____

Server's signature

Printed name and title

Case No. _____

**This second page contains personal identifiers and therefore should not be filed in court with the summons unless under seal.
(Not for Public Disclosure)**

INFORMATION FOR SERVICE

Name of defendant/offender: Joseph Sullivan

Last known residence: _____

Usual place of abode (if different from residence address): _____

If the defendant is an organization, name(s) and address(es) of officer(s) or agent(s) legally authorized to receive service of process: _____

If the defendant is an organization, last known address within the district or principal place of business elsewhere in the United States: _____

PROOF OF SERVICE

This summons was received by me on (date) _____.

I personally served the summons on this defendant _____ at (place) _____ on (date) _____; or

On (date) _____ I left the summons at the individual's residence or usual place of abode with (name) _____, a person of suitable age and discretion who resides there, and I mailed a copy to the individual's last known address; or

I delivered a copy of the summons to (name of individual) _____, who is authorized to receive service of process on behalf of (name of organization) _____ on (date) _____ and I mailed a copy to the organizations' last known address within the district or to its principal place of business elsewhere in the United States; or

The summons was returned unexecuted because: _____

I declare under penalty of perjury that this information is true.

Date returned: _____

Server's signature

Printed name and title

Remarks:

Print

Save As...

Reset

UNITED STATES DISTRICT COURT

for the

Northern District of California

FILED

Aug 20 2020

SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

United States of America)

v.)

JOSEPH SULLIVAN)

Case No. 3-20-71168 JCS)

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of Nov. 15, 2016 to Nov. 21, 2017 in the county of San Francisco and elsewhere in the Northern District of California, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1505	Count One: Obstruction of Justice Max. Penalties: 5 years in prison; \$250,000 fine; 3 years of supervised release; \$100 special assessment; restitution; forfeiture
18 U.S.C. § 4	Count Two: Misprision of a Felony Max. Penalties: 3 years in prison; \$250,000 fine; 1 year of supervised release; \$100 special assessment; restitution; forfeiture

This criminal complaint is based on these facts:

The attached affidavit of FBI Special Agent Mario C. Scussel.

Continued on the attached sheet.

Approved as to form _____ /s/
AUSA Andrew Dawson

s/
Complainant's signature
Mario C. Scussel, SA FBI

Printed name and title

Sworn to before me by telephone.

Date: 08/19/2020



Judge's signature
Hon. Joseph Spero, U.S. Magistrate Judge

Printed name and title

City and state: San Francisco, California

Print

Save As...

Attach

Reset

**AFFIDAVIT OF SPECIAL AGENT MARIO C. SCUSSEL IN SUPPORT OF
CRIMINAL COMPLAINT**

I, Mario C. Scussel, a Special Agent of the Federal Bureau of Investigation, being duly sworn, hereby declare as follows:

I. OVERVIEW AND AGENT BACKGROUND

1. I make this affidavit in support of a two-count Criminal Complaint against JOSEPH SULLIVAN (hereinafter SULLIVAN):

- a. Count One: Obstruction of Justice, in violation of 18 U.S.C. § 1505;
- b. Count Two: Misprision of a Felony, in violation of 18 U.S.C. § 4.

For the reasons set forth below, I believe there is probable cause to believe SULLIVAN has committed each of the foregoing violations of federal law.

2. The statements contained in this affidavit come from my personal observations, my training and experience, information from records and databases, and information obtained from other agents and witnesses. This affidavit summarizes such information in order to show that there is probable cause to believe that SULLIVAN has committed the violations listed above. This affidavit does not purport to set forth all of my knowledge about this matter, or to name all of the persons who participated in these crimes.

3. I am a Special Agent of the Federal Bureau of Investigation (“FBI”) and have been so employed for approximately 12 years. I am currently assigned to the Complex Financial Crime Squad of FBI’s San Francisco Field Division. As part of my assigned duties, I investigate possible violations of federal criminal law, specifically investigations involving white collar crimes. I successfully completed 21 weeks of New Agent Training at the FBI Academy in Quantico, Virginia in January 2009. During that time, I received training in legal statutes and procedures, financial investigations, money laundering techniques, asset identification, forfeiture

and seizure, physical surveillance, confidential source management, and electronic surveillance techniques.

4. During my employment with the FBI, I have conducted interviews of witnesses, victims, and subjects; conducted physical surveillance, executed search warrants and arrests; reviewed evidence and documents; transported evidence, and prisoners. Prior to my employment as a Special Agent, I also worked for the FBI, as an Investigative Specialist conducting surveillance operations for Counterintelligence and Counterterrorism investigations. I earned a Master's Degree in Business Administration from the University of California at Berkeley – Haas Business School as well as Master of Arts and a Bachelor of Arts Degrees in Psychology from Stanford University.

II. APPLICABLE LAW

5. Title 18, United States Code, Section 1505 provides: “Whoever corruptly, or by threats or force, or by any threatening letter or communication influences, obstructs, or impedes or endeavors to influence, obstruct, or impede the due and proper administration of the law under which any pending proceeding is being had before any department or agency of the United States, or the due and proper exercise of the power of inquiry under which any inquiry or investigation is being had by either House, or any committee of either House or any joint committee of the Congress—Shall be fined under this title, imprisoned not more than 5 years or, if the offense involves international or domestic terrorism (as defined in section 2331), imprisoned not more than 8 years, or both.”

6. Title 18, United States Code, Section 1515(b) provides: “As used in section 1505, the term ‘corruptly’ means acting with an improper purpose, personally or by influencing another, including making a false or misleading statement, or withholding, concealing, altering, or destroying a document or other information.”

7. Title 18, United States Code, Section 4 provides: “Whoever, having knowledge of

the actual commission of a felony cognizable by a court of the United States, conceals and does not as soon as possible make known the same to some judge or other person in civil or military authority under the United States, shall be fined under this title or imprisoned not more than three years, or both.”

III. FACTS SUPPORTING PROBABLE CAUSE

A. Summary

8. SULLIVAN is a 52-year-old male, living in Palo Alto, CA. Between approximately April 2015 and November 2017, SULLIVAN served as Chief Security Officer for Uber Technologies Inc. (“Uber”). During his tenure, SULLIVAN assisted in overseeing Uber’s response to a Federal Trade Commission (“FTC”) investigation into Uber’s data security practices. That investigation had been triggered, in part, by a data breach suffered by Uber in approximately 2014.

9. In the course of Uber’s response to the FTC’s investigation, SULLIVAN participated in conference calls with FTC attorneys; reviewed Uber’s submissions to the FTC; gave a presentation to FTC staff in Washington, D.C.; and sat for a sworn investigative hearing similar to a deposition. SULLIVAN was therefore intimately familiar with the nature and scope of the FTC’s investigation, and he held himself out as familiar with that investigation. Nevertheless, when SULLIVAN learned that Uber’s systems had been hacked in approximately November 2016—approximately ten days after SULLIVAN had provided sworn testimony to the FTC—SULLIVAN engaged in a scheme to withhold and conceal from the FTC both the hack itself and the fact that the data breach had resulted in the hackers obtaining millions of records associated with Uber’s users and drivers. When Uber brought in a new CEO in 2017, SULLIVAN lied to him about the circumstances surrounding that data breach. Uber’s new management ultimately disclosed the breach to the FTC in November 2017, explaining that the hackers had obtained the names and driver’s license numbers of approximately 600,000 Uber

drivers and some personal information associated with 57 million Uber users and drivers.

SULLIVAN's employment was terminated by Uber at approximately the same time.

10. In sum, business records generated in the course of the response to the breach reflect that SULLIVAN instructed his team to keep knowledge of the 2016 Breach tightly controlled. Witnesses reported SULLIVAN was visibly shaken by the events. A witness also reported that SULLIVAN stated in a private conversation that he could not believe they had let another breach happen and that the team had to make sure word of the breach did not get out. SULLIVAN instructed the team that knowledge of the breach was to be disclosed outside the security team only on a need-to-know basis and the company was going to treat the incident under its "bug bounty" program. Bug bounty programs are designed to incentivize white-hat hackers, or "researchers," to identify security vulnerabilities by offering a monetary reward in exchange for such efforts. However, the terms and conditions of Uber's bug bounty program did not authorize rewarding a hacker who had accessed and obtained personally identifiable information of users and drivers from Uber-controlled systems. Nevertheless, Uber arranged for its bug bounty vendor to pay the hackers \$100,000, which at the time was by far the largest bounty that Uber had ever paid through the program.

11. SULLIVAN further insisted that the hackers agree to sign non-disclosure agreements ("NDAs") in exchange for the \$100,000 bounty payment that would supplement the standard terms of Uber's bug bounty program. Such a supplemental NDA was not a typical component of a bug bounty claim, and witnesses I have interviewed do not recall Uber requiring a supplemental NDA in any other bug bounty claim. Moreover, the NDA SULLIVAN authorized falsely represented that the hackers had not obtained or stored any data during their intrusion. Both the hackers and SULLIVAN knew at the time that this representation in the NDA was false. This misrepresentation concealed the fact that the hackers had, in fact, stolen data, thereby falsely giving the incident the appearance of a typical bug bounty claim rather than

a data breach. The hackers' ransom was paid in December 2016 via bitcoin, even though the hackers by that time had refused to sign the NDAs in their true names and had not yet been identified by Uber. Uber's staff continued to work on identifying the hackers and were able to eventually identify them in January 2017, at which point SULLIVAN dispatched security staff to interview both hackers and obtain signed NDAs from them in their true names. The true-identity NDAs continued to include the claim that SULLIVAN, Uber, and the hackers knew to be false: that the hackers had not taken data from Uber.

12. Records further indicate Uber's management team, with the sole exception of Uber's C.E.O. at the time, had no contemporaneous knowledge of the details of the data breach and had no role in the decision to treat the breach under the Bug Bounty program.

13. In the months following the data breach, Uber and SULLIVAN continued to respond to the FTC's inquiries. For example, in December 2016, SULLIVAN was aware that Uber was preparing to provide an update to the FTC about employee access to personally identifying information. Nevertheless, SULLIVAN never informed the FTC of the 2016 data breach, even though he was aware that the FTC's investigation focused on data security, data breaches, and protection of PII. In addition, witness interviews indicate that SULLIVAN did not inform the Uber attorneys working on the FTC investigation—either in-house or outside counsel—that the breach had occurred.

14. In approximately August 2017, Uber named a new Chief Executive Officer. Two months later, Uber disclosed the 2016 data breach publicly, apologizing for the failure to do so promptly. Uber fired SULLIVAN and a security attorney assigned to his team.

B. The Federal Trade Commission Investigation

15. In February 2015, Uber informed the FTC that it had suffered a data breach in September 2014 ("the 2014 Breach"). The FTC subsequently began investigating the circumstances of the 2014 Breach, gathering information via document requests and

interrogatories contained in Civil Investigative Demands. Uber was in frequent contact with the FTC via outside counsel, sharing information on a proactive basis and in response to both formal and informal inquiries from FTC staff.

a. 2014 Data Breach

16. According to Uber's disclosures to the FTC, the 2014 Breach occurred when an outsider was able to gain access to data Uber stored on an Amazon Web Services ("AWS") platform known as S3. The outsider located an AWS access ID and secret key in software code posted to GitHub, which is a web-based platform used by software developers to store and share code. The outsider then used that access ID and secret key to gain access to Uber's data. Uber later determined the file accessed by the outsider contained enough information to allow a user to match names and drivers' license numbers of approximately 50,000 drivers. According to Uber's disclosures, the database was not encrypted.

b. First Civil Investigative Demand

17. On May 21, 2015, the FTC issued a Civil Investigative Demand ("CID"). Included in the CID were four interrogatories, each with various subparts. The fourth interrogatory required Uber to provide, "[w]ith respect to any Breach or suspected breach," a variety of information including:

- "When and how the Company learned of the breach,"
- "The location, type(s), and amount(s) of Personal Information that unauthorized person(s) could have accessed or viewed,"
- "The location, type(s), and amount(s) of Personal Information that the unauthorized person(s) did copy, download, or remove"; and
- "[W]hen and . . . how the Company notified Consumers, law enforcement, and other third parties about the Breach."

18. The CID defined “breach” as “unauthorized access into the Company’s systems or to Personal Information in the Company’s file(s), including but not limited to the unauthorized access to the Company’s database(s) that took place on or around May 12, 2014 [the 2014 Data Breach].” “Personal Information” was defined broadly as “individually identifiable information from or about an individual Consumer,” specifically including “a driver’s license . . . or other personal identification number.” The applicable time period was defined as “from January 1, 2014, until the date of full and complete compliance with this CID.”

c. SULLIVAN’s Role in the FTC Investigation

19. On September 25, 2015, Uber provided a set of interrogatory responses which explained its use of Amazon’s S3 platform. The responses disclosed that SULLIVAN and one of his direct reports “supervised the preparation of Uber’s response to this CID.” The response explained that “Uber’s Amazon S3 datastore is divided into 101 buckets,” and these buckets could be divided into three types: (1) application logs; (2) static files; and (3) other buckets, which included “storage of database backups and database prunes” As to the storage of “database backups and database prunes,” Uber explained that a “complete database backup” is “retained to allow service restoration in the event of system failure,” while a “database prune” is a “snapshot containing limited data used to realistically simulate the production environment for purposes of development and testing” Uber further stated that beginning in August 2014, all new database backup files were encrypted.

d. SULLIVAN’s FTC Testimony

20. On June 10, 2016, the FTC issued a second CID, which required Uber to designate an officer to provide sworn testimony on a variety of topics. As a focus among these topics, the FTC compelled testimony on a variety of issues related to S3, Uber’s use of encryption, and Uber’s retention of personally identifying information (“PII”). Uber designated SULLIVAN as its witness, and he was prepared extensively for the hearing by both in-house and

outside counsel, over the course of approximately four days which spanned several weeks, with meetings ranging from an hour to an entire day.

21. The hearing took place on November 4, 2016. By this time, the FTC's investigation was focused in large part on Uber's use of S3 and its implications for data privacy. SULLIVAN testified that he understood that the 2014 Breach, which predated SULLIVAN's employment at Uber, involved an Amazon Web Services access ID that had been inadvertently posted publicly on GitHub. That ID gave an outsider access to Uber's data. SULLIVAN elaborated that it was common at the time to write access IDs and other secrets directly into code when that code needed to call for information from another service. This practice had implications when code was exposed to outsiders, because the code itself would give them access to Uber's data. SULLIVAN explained that "key management"—that is, ensuring secret keys are not exposed to bad actors—"is always an important part of an overall security program for any company."

22. SULLIVAN also testified about Uber's storage of database backups in AWS. He was asked about Uber's statement in an interrogatory response that all new database backup files had been encrypted as of August 2014, and he testified in detail about the weaknesses in Amazon's native encryption functions and the fact that encryption became much more important as companies began moving to cloud-based infrastructure. SULLIVAN never contested that the 2014 Breach was a data breach and, in fact, acknowledged that.

C. The 2016 Breach and Cover-Up

23. Approximately ten days after SULLIVAN's testimony, he learned that Uber's AWS S3 datastore had been breached again. On November 14, 2016, SULLIVAN received an email from "johndoughs@protonmail.com" claiming to have found a "major vulnerability in uber," and that "I was able to dump uber database and many other things."

24. At SULLIVAN's direction, Uber's security team began an investigation. Within approximately a day, the security team realized an unauthorized person or persons had accessed AWS and obtained, among other things, a copy of a database containing approximately 600,000 drivers' license numbers for Uber drivers. Based on documents I have reviewed and witness interviews I have conducted, within approximately the same time period SULLIVAN became aware the attackers had accessed AWS in almost the identical manner the 2014 attacker had used. That is, the attackers were able to access Uber's source code on GitHub (this time by using stolen credentials), locate an AWS credential, and use that credential to download Uber's data.

25. Contemporaneous documentation reflects SULLIVAN understood the sensitivity of this information. The response team generated a shared document referred to as the Preacher Central Tracker ("the Tracker"), which was used to record progress in the investigation and tasks assigned to various team members. In an update dated November 14, the Tracker stated:

access key has not be rotated [sic] since [it was created in 2013]. None of the people are at the company any longer. Task was to rotate keys within S3 to ensure this could not happen in the future but there are thousands of tasks. Joe was just deposed on this specific topic and what the best or minimum practices that any company should follow in this area.

26. Based on the context within the Tracker and my review of the transcript of SULLIVAN's testimony, I believe the reference to "Joe was just deposed" refers to SULLIVAN's testimony to the FTC. The comment demonstrates that the similarity and connection between the 2014 Breach and the 2016 Breach was apparent to the response team at an early phase.

27. A later update recorded in the Tracker reflected the need to keep news of the breach confidential:

Information is extremely sensitive and we need to keep this tightly controlled. Discussion with other Engineers must be tightly controlled. Joe is communicating directly to the A-Team.

28. Based on my investigation, I believe the term “A-Team” refers to the executive management team within Uber, representing the C.E.O.’s direct reports. SULLIVAN was a member of the A-Team. Based on my investigation and interviews with other management team members, I believe that contrary to the representation in the Tracker, only the C.E.O. and SULLIVAN had contemporaneous knowledge of the details of the 2016 Breach, including that drivers’ license numbers had been stolen.

29. Uber’s response to the breach, as reflected in the Tracker and other business records, required that engineers within the company take a variety of steps to lock down Uber’s data and prevent further access by the hackers. The Tracker contained the following guidance on how to justify such broad action without disclosing the nature of the 2016 Breach more widely within the company:

What is our position to the company to talk about what we are doing? We had a data breach in 2014, we learned our lesson and we need to get our house in order. Hundred service centers must rotate their secrets. Our common story has to be:

- This investigation does not exist.
- We are doing this in order to better protect our information.

D. Bug Bounty and Non-Disclosure Agreements

30. The hackers made clear early in their email correspondence with Uber that they expected a six-figure payout. Email and text correspondence demonstrate that SULLIVAN and others considered using Uber’s bug bounty program to pay the hackers, even though that program had never awarded a bounty even close to \$100,000 and had a nominal cap of \$10,000. Moreover, Uber’s Hacker One policy terms contained language specifying that dumping user data from AWS did not comply with Uber’s policy:

If you get access to an Uber server please report it us [sic] and we will reward you with an appropriate bounty taking into full consideration the severity of what could be done. . .
. Using AWS access key to dump user info? Not cool.

31. Soon after learning drivers' license numbers had potentially been exposed (at approximately 1:00am Pacific time on November 15, 2016), SULLIVAN reached out to Uber's then-CEO via text message. At approximately 1:28am on November 15, SULLIVAN sent the following text:

I have something sensitive I'd like to update you on if you have a minute.

32. Call records reflect that SULLIVAN and Uber's then-CEO had a series of conversations via phone and/or FaceTime lasting approximately five minutes. At approximately 1:38am, the CEO responded:

Need to get certainty of what he has, sensitivity/exposure of it and confidence that he can truly treat this as a bounty situation... resources can be flexible in order to put this to bed but we need to document this very tightly

33. Based on the timing and content of the text messages, compared with the timestamps visible in the Tracker, I believe SULLIVAN was informing the CEO that outside hackers had potentially accessed Uber's data, specifically approximately 600,000 drivers' license numbers. The CEO's response reflects that the prospect of treating the incident under the bug bounty program was already being discussed.

34. SULLIVAN advised certain members of his team that the hackers would need to sign non-disclosure agreements ("NDAs"). To the best of my knowledge, Uber had not previously required a supplemental NDA in order to pay out a bug bounty claim, and SULLIVAN's team began drafting a new contract. The primary author of the NDA was an attorney assigned to SULLIVAN's group, but multiple individuals, including SULLIVAN, made edits over the course of the drafting process. The NDA forbade the hackers from disclosing "anything about the vulnerabilities or your dialogue with us to anyone for any purpose without our written permission. This includes any analysis or postmortem in any medium or forum."

That gag provision stands in stark contrast with the standard terms of Uber’s bug bounty program at that time. Uber’s policy at that time contained a Frequently Asked Questions provision. One listed question was “Can I blog about my bug?” The answer:

Yes, but we ask that you wait until the issue is both fixed and paid out before you publish the blog post. We also prefer that you request disclosure through HackerOne so that readers of your blog post can get the full background on the issue.

35. The NDA also contained the following “promise,” under the “Your promises” section, which applied to the hackers: “You promise that you did not take or store any data during or through your research and that you have delivered to us or forensically destroyed all information about and/or analyses of the vulnerabilities.” Notwithstanding this “promise,” SULLIVAN and the hackers all knew that hackers had, in fact, already taken Uber’s data. In fact, the stolen data, and the risk that it could be publicly exposed or sold on the black market, is what gave the hackers leverage in demanding an unprecedented six-figure payout. But the language created the false impression to third parties, in the event the NDAs were ever publicly disclosed, that the hackers had complied with the terms of Uber’s bug bounty program and had never obtained copies of user or driver data.

36. Prior to sending the NDAs to the hackers for signature, SULLIVAN was advised of the false language in the NDA, and he responded that the language would stay in the agreements.¹ Based on my experience in this investigation, I believe this false and misleading provision reflects SULLIVAN’s intent to conceal the truth of the 2016 Breach—namely, the theft of vast quantities of PII—the from the public, from law enforcement, and from the FTC.

¹ The witness who recalls this conversation initially asserted his rights under the Fifth Amendment and declined to be interviewed. He ultimately agreed to be interviewed pursuant to an agreement with the United States Attorney’s Office for the Northern District of California (“USAO”). In summary, the USAO agreed not to use any of the witness’s statements against him in exchange for his cooperation with the investigation.

37. The hackers initially signed the NDAs using pseudonyms. Despite their refusal to provide their real names, Uber arranged to have Hacker One pay the agreed-upon bounty. Payment was made on December 8, 2016. The next month, Uber personnel were able to identify two individuals responsible for the breach. Uber approached them, interviewed them, and arranged for them to sign fresh copies of the NDAs in true name.

E. Resolving the FTC Investigation

38. In the months following the breach, Uber and SULLIVAN continued to respond to the FTC's investigation, but SULLIVAN never disclosed the 2016 Breach to the Uber personnel working on that response. For example, on December 20, 2016, SULLIVAN received by email a copy of a draft set of supplemental interrogatory responses, sent by the in-house attorney responsible for managing the FTC investigation. Language in those responses claimed once again that "all new database backup files" had been encrypted since August 2014. SULLIVAN responded "I think for FTC we can could present a pretty compelling narrative given how much we have done." He did not disclose in the email, or in any other communications with the in-house attorney of which I am aware, that Uber had suffered another data breach in the weeks preceding the interrogatory responses.

39. In or about April 2017, SULLIVAN received a draft letter Uber planned to send to the FTC requesting that the FTC close its investigation into Uber. The cover email, to which the draft of the letter was attached, contained the following summary of the letter:

we argue (1) Uber's record of cooperation and engagement with FTC staff over the last 28 months has been exemplary; (2) even before the receipt of compulsory process, Uber came forward to provide information on a voluntary basis and has provided exhaustive information to staff; and (3) the data security incidents at issue reflect no misdirected priorities, no failure to appreciate risks, and no lack of security knowledge or care.

The cover email again made no mention of the 2016 data breach. SULLIVAN responded:

“Letter looks ok to me. Thanks.”²

40. Uber sent the finalized letter to the FTC on April 19, 2017. The letter argued that

Uber:

has cooperatively provided information and has also prepared exhaustive interrogatory responses, produced documents, conducted telephonic and in-person briefings through inside and outside counsel on myriad topics, conducted an in-person briefing by senior members of its data security team, sat for an investigational hearing, repeated explanations of processes and systems when staff handling the investigation changed, and responded to follow-up questions from DPIP staff on multiple occasions. No request to Uber from staff is open or unanswered.

41. In addition, Uber highlighted what it claimed were significant new protections it had deployed to the S3 datastore:

Since the time of the [2014 data breach], now almost three years ago, Uber has put in place numerous and extensive additional protections for the data it stores in the S3 datastore, as well as company-wide improvements in credential protection and management and other aspects of data security. . . . Uber described these improved and updated practices extensively in the course of this investigation.

42. Uber relied on these supposed improvements in arguing that the FTC should not bring a claim against the company, arguing that Uber had become a more sophisticated company since 2014. Similarly, Uber argued that the industry at large had become more adept since 2014 at protecting private data in the cloud, and that Uber should not be judged for “what a company did *then* (back when the company was much smaller and the technology at issue was evolving) according to the standards that the agency thinks are appropriate *now* (given the current sophistication of the company and current industry best practices).” Uber made these arguments via letter in April 2017, approximately five months after the 2016 Breach.

² While I have been able to review portions of the cover email, as quoted above, Uber has asserted the attorney-client privilege over most of the contents of the draft letter itself. As noted in subsequent paragraphs, I have reviewed the letter that Uber ultimately sent to the FTC requesting that the investigation be closed.

43. Based on my investigation, I do not believe that any of the individuals responsible for drafting the April 19 letter to the FTC had been made aware of the 2016 data breach.³ SULLIVAN was consulted on the letter in its draft form, but he withheld knowledge of the breach from others within Uber who were in a position to disclose that information to the FTC.

F. Scrutiny from New Management

44. In September 2017, SULLIVAN was asked to brief Uber's new CEO on the 2016 incident. SULLIVAN asked his team to prepare a summary, which they did. After receiving that summary, however, SULLIVAN removed certain details from the summary that would have illustrated the true scope of the breach. SULLIVAN's changes resulted in both affirmative misrepresentations and misleading omissions of fact. In my training and experience, these changes demonstrate SULLIVAN's ongoing intent to obstruct the FTC (which had not yet fully resolved its investigation) and his consciousness of guilt regarding his actions.

45. For example, the summary SULLIVAN received from his staff accurately disclosed that the hackers had gained access to "AWS buckets that contained potentially all rider and driver data in plaintext," and that the hackers "still had possession of our data" when they reached out to Uber in November 2016. The summary that SULLIVAN subsequently provided to the new CEO via email, however, disclosed only that the hackers had gained access to "some rider and driver data" and removed any admission that the hackers actually took the data.

46. In addition, the summary provided to the new CEO falsely stated that the bug bounty payment had been made only after the hackers had been identified. SULLIVAN falsely stated that his team told the hacker(s) that "we would only pay the bounty if he signed documents in his real identity," and further that the hacker "fully cooperated" with this condition. In reality, SULLIVAN authorized paying the \$100,000 bounty in December 2016 even though

³ While there is some evidence that Uber's general counsel was aware by this time of a security incident, I have seen no evidence that the general counsel was aware of the details, such as the nature of the attack or the PII that was stolen.

the hackers had not yet been identified, and even though the hackers refused to identify themselves. Uber was only able to identify them in January 2017, weeks after the payment had been made.

47. The misrepresentations in SULLIVAN's summary are consistent with the false language in the NDA, as both sets of statements create the false impression that the hackers had not stolen data from Uber. I believe the misrepresentations in SULLIVAN's summary further reflect SULLIVAN's intent to withhold the details of the 2016 Breach even from the company's new CEO.

G. The Breach Is Disclosed to the FTC

48. On November 21, 2017, Uber's new CEO issued a press release stating that he had recently become aware of the details of the 2016 Breach. At approximately the same time, the 2016 Breach was disclosed to the FTC. By November 2017, Uber and the FTC had reached a tentative agreement resolving the FTC's investigation, which included a draft complaint and consent order with various provisions Uber was required to comply with. The agreement was not yet final, and after the FTC learned of the 2016 Breach, it effectively withdrew from that tentative agreement.

49. In light of the new information regarding the 2016 Breach, the FTC effectively withdrew its previous settlement terms and added further requirements to the resolution with Uber. The revised draft complaint included a recitation of facts related to the 2016 Breach, and the revised draft consent order withdrew certain concessions it had made to Uber and added a new, affirmative notification provision regarding any future breaches. The FTC gave final approval to the revised Complaint and Consent Order on October 26, 2018.

H. The Hackers Pleaded Guilty to Federal Crimes.

50. On August 2, 2018, a Grand Jury in the Northern District of California returned an indictment charging Brandon Charles GLOVER and Vasile MEREACRE with crimes related

to extortion involving computers under 18 U.S.C. § 1030(a)(7)(B) and 1030(c)(3)(A). The indictment alleged that GLOVER and MEREACRE, between December 2016 and January 2017, conspired to extort an online employment-oriented service (“COMPANY ONE”) by obtaining over 90,000 confidential user accounts and using those accounts as a means to obtain money.

51. On October 30, 2019, GLOVER pleaded guilty to a single count in a Superseding Information charging a conspiracy to commit crimes under 18 U.S.C. § 1030. GLOVER admitted that he and MEREACRE agreed to extort COMPANY ONE, and further that a separate object of the conspiracy was the scheme to extort Uber in connection with the 2016 data breach. GLOVER further admitted that he and MEREACRE enlisted the help of a third party to identify valuable information in Uber’s S3 datastore. GLOVER has admitted in interviews that while he and MEREACRE requested that the third party delete his copy of the data after Uber made the payment, he does not know if the third party actually did so. GLOVER and MEREACRE agreed to pay the third party a portion of the overall bounty, but they did not disclose to Uber that a third individual had been involved. GLOVER stated in an interview that he was surprised that Uber had paid the full amount that he and MEREACRE had requested. He explained that he learned only later that Uber had suffered a different data breach in 2014, and that this revelation explained in his mind why Uber was willing to pay so much to keep the breach quiet.

52. On October 30, 2019, MEREACRE pleaded guilty to a single count in a Superseding Information charging a conspiracy to commit crimes under 18 U.S.C. § 1030. MEREACRE admitted that he and GLOVER agreed to extort COMPANY ONE, and further that a separate object of the conspiracy was the scheme to extort Uber in connection with the 2016 data breach. MEREACRE has also admitted, as did GLOVER, that he and GLOVER enlisted the help of a third party in identifying particularly valuable data in Uber’s S3 datastore, and that this third party had his own copy of data downloaded from Uber’s S3 datastore. MEREACRE has admitted that when he initially attempted to open a HackerOne account in order to receive

the \$100,000 bounty from Uber, his application was rejected because he had used a fake name and fake social security number. MEREACRE was surprised when Uber was ultimately able to bypass those requirements and to accomplish the payment, and this bypassing convinced MEREACRE that Uber was going to great lengths to keep the breach quiet

53. Based upon the evidence I have reviewed and the statements of GLOVER and MEREACRE, GLOVER and MEREACRE chose to target and successfully hack other technology companies and their users' data—including but not limited to COMPANY ONE—after they successfully extorted Uber for \$100,000. Those hacks occurred after SULLIVAN failed to bring the Uber data breach to the attention of law enforcement and after SULLIVAN and Uber created and signed the false NDAs with GLOVER and MEREACRE.

IV. CONCLUSION

54. In summary, based on the evidence gathered through this investigation, I believe that there is probable cause to believe that the defendant engaged in a cover-up intended to obstruct the lawful functions and official proceedings of the Federal Trade Commission. SULLIVAN intended that the cover-up would obscure from the proceedings before the FTC that Uber had been breached again in 2016 during the FTC's pending proceedings. SULLIVAN further intended that the cover-up would obscure from the FTC's proceedings that millions of additional individuals had their personal data—kept by Uber—accessed and downloaded by hackers. It is my belief that SULLIVAN further intended to spare Uber and SULLIVAN negative publicity and loss of users and drivers that would have stemmed from disclosure of the hack and data breach.

55. I further believe that there is probable cause to believe that SULLIVAN was aware of the illegal hack of Uber in 2016. Despite that knowledge, SULLIVAN did not report the illegal hack to law enforcement. Additionally, SULLIVAN took it upon himself and Uber to conceal and disguise the hack from law enforcement and from the public. In so doing,

SULLIVAN and Uber prevented law enforcement from apprehending the hackers. Had SULLIVAN and Uber promptly reported the illegal hack to law enforcement, the hacks of multiple additional large tech companies and the theft of the personal data of millions of additional customers and users may have been prevented. The illegal hack was not disclosed to the FTC, to law enforcement, and to the public until new management took over these decisions at Uber.

56. Thus, it is my opinion that there is probable cause to believe that Joseph SULLIVAN has committed the following violations of federal law:

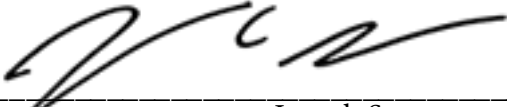
- a. Count One: Obstruction of Justice, in violation of 18 U.S.C. § 1505;
- b. Count Two: Misprision of a felony, in violation of 18 U.S.C. § 4.

I declare under penalty of perjury that the above is true and correct to the best of my knowledge.

s/

MARIO C. SCUSSEL
Special Agent
Federal Bureau of Investigation

Sworn to before me over the telephone and signed by me this 19th day of August, 2020.



~~HON. LAUREL BEELER~~ Joseph Spero
United States Magistrate Judge