AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Northern District of California

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:

Code Section	*Offense Description*
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

City and state: San Francisco, California

Hon. Joseph Spero, U.S. Magistrate Judge
Printed name and title

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

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.