ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy / White Collar, Government & Internal Investigations ADVISORY ■

OCTOBER 10, 2022

Lessons from DOJ's First Prosecution of a Company Executive Covering Up a Data Breach

by Kellen Dwyer, Kim Peretti, and Mario Ayoub

Uber's former chief security officer (CSO), Joe Sullivan, was found guilty on October 5, 2022 by a jury in federal court on charges of obstruction of justice (18 U.S.C. Section 1505) and misprision of a felony (18 U.S.C. Section 4) based on what the Justice Department called his "attempted cover-up of a 2016 hack of Uber."

In 2016, while the Federal Trade Commission (FTC) was investigating Uber for an earlier incident, Sullivan learned of a new incident that affected the Uber accounts of more than 57 million riders and drivers. The government alleged that, rather than disclose the 2016 incident to the FTC, the CSO took steps to hide the incident from the FTC, as well as from many of his colleagues at Uber, including its general counsel and outside attorneys. Most notably, he arranged a $100,000 payment to the hackers through Uber's "bug bounty" program in exchange for the hackers signing a nondisclosure agreement (NDA) promising not to reveal the incident and falsely stating that they did not exfiltrate sensitive customer information.

This case – which is the first time a company executive faced criminal prosecution over its response to a data incident – is troubling in that it blurs the line between "covering up" a data incident and merely declining to report it. At the time of the CSO's actions, there was no generally applicable statute requiring companies to disclose data security incidents to the federal government. And while President Biden recently signed legislation requiring companies considered "critical infrastructure" to report data security incidents in certain circumstances, that statute will not take effect until the Department of Homeland Security finalizes implementing regulations, likely in 2025.

Nonetheless, comments from the DOJ's leadership in the wake of the trial read as though there is already a duty to disclose such incidents to the federal government such that any nondisclosure is a "coverup." The U.S. Attorney for the Northern District of California, for instance, stated that the Justice Department "expect[s]" companies with access to sensitive consumer data "to protect that data and to alert customers and appropriate authorities when such data is stolen by hackers" and that "[w]e will not tolerate concealment of important information from the public by corporate

executives more interested in protecting their reputation … than in protecting users." Similarly, the special agent in charge of the FBI's San Francisco Field Office declared that "[t]he message in today's guilty verdict is clear: companies storing their customers' data have a responsibility to protect that data and do the right thing when breaches occur."

These broad statements notwithstanding, this case involved a number of aggravating factors that, taken together, crossed the line from mere silence to affirmative obstruction.

A Preexisting, Ongoing Government Investigation Changes Everything

At the time of the 2016 incident, Uber was already in the midst of an FTC investigation into its data security practices that arose from an incident in 2014. Importantly, it was this preexisting investigation that Sullivan was convicted of obstructing. In 2015, the FTC served a detailed civil investigative demand (CID) on Uber, demanding extensive information about any other instances of unauthorized access to user personal information and information on Uber's broader data security program and practices. As CSO, Sullivan was heavily involved in preparing Uber's response to the CID and, on November 4, 2016, was deposed by the FTC concerning Uber's data security practices. Ten days later, the CSO received an email from a hacker informing him of a new incident involving a significant amount of sensitive customer data. Employees on the CSO's team quickly verified the accuracy of these claims, which included records on approximately 57 million Uber users and 600,000 driver's license numbers.

The DOJ's obstruction theory appeared to be that, while the FTC's investigation remained ongoing, the CSO had a continuing duty to update the CID and his deposition testimony to disclose any significant new incident. Indeed, according to the DOJ press release, "despite knowing in great detail that Uber had suffered another data breach directly responsive to the FTC's inquiry, Sullivan continued to work with the Uber lawyers handling or overseeing that inquiry, including the General Counsel of Uber, and never mentioned the incident to them. Instead, he touted the work that he and his team had done on data security. Uber ultimately entered into a preliminary settlement with the FTC."

The key takeaway is that a preexisting and ongoing regulatory investigation into a previous incident or a company's data security practices can trigger a duty to disclose any new incidents to that same regulator. Even if the company has already responded to CIDs or provided testimony that was accurate at the time, the government may take the position that the company has a duty to update its statements and testimony if there is a new incident, at least while the government's investigation remains ongoing and, in particular, if the regulator had inquired about other security incidents. Companies defending such investigations should have procedures ensuring that the legal department is informed of new incidents that could potentially be reportable.

Rethink Your Bug Bounty Program and Ransom Payment Procedures

The second charge was an old and rarely used one: misprision of a felony. This common-law crime applies whenever someone is aware of a felony and takes an affirmative step to conceal it. The DOJ based this charge largely on the CSO's use of Uber's bug bounty program to prevent public disclosure of the 2016 incident. In particular, he arranged a $100,000 payment to the hackers in exchange for the hackers signing an NDA promising not to disclose the incident and falsely stating that the incident did not involve the compromise of sensitive data. In addition, according to a former in-house Uber attorney who testified pursuant to an immunity agreement, the CSO changed the NDA signed by the hackers to make it falsely seem that the hack was white hat research.

The misprision theory is the most troubling aspect of this case. Any company experiencing a ransomware event is aware of a felony; therefore, companies need to be very careful that any actions they take cannot be construed as "affirmative concealment" of that felony. Indeed, it is not hard to imagine that a ransom payment in exchange for an explicit or implicit promise not to disclose the existence of the incident could be considered affirmative concealment of the incident. The DOJ's press release is particularly concerning because it cited as aggravating factors that "Sullivan orchestrated [the payment] despite knowing that the hackers were hacking and extorting other companies as well as Uber" and "despite the fact that the hackers had refused to provide their true names." Of course, those same factors are present with nearly every ransom payment.

It is therefore critical that companies take the following steps to ensure that any payments to hackers are readily distinguishable from the payment in this case.

- First, companies should not ask hackers to agree to anything that is false or misleading, especially statements minimizing the extent of the incident.
- Second, while it is common and appropriate for companies to demand that hackers agree to destroy and not to publish information that was stolen, companies should be very careful about asking hackers not to disclose the existence of the incident itself.
- Third, companies should make clear distinctions between ransom payments on the one hand and bug bounty payments on the other. Bug bounty payments should be reserved for white hat hackers, in accordance with the rules of a written bug bounty program. If there is any reason to believe that someone was not acting fully in good faith and in compliance with the rules of the bounty program, companies should handle the matter as a black hat hacker demanding ransom rather than through the bounty program.
- Finally, companies must be sure to comply with the bug bounty rules that they set for themselves. At trial, the DOJ made much of the fact that the payment was 10 times the limit of Uber's bounty program and that the CSO arranged the payment without following the process required by Uber's program.

Be Careful What You Put in Writing

At trial, prosecutors repeatedly read from internal company communications in which the CSO stressed to others the need to keep the 2016 incident quiet. For instance, he told subordinates that they "can't let this get out," instructed them that the information needed to be "tightly controlled," and that the story outside the security group was to be that "this investigation does not exist."

While these statements are not flattering, it is not uncommon for companies to tightly control information about a cyber incident, especially while the investigation is ongoing. In order to avoid having statements taken out of context, company employees working on data incident investigations should minimize written statements, including statements over email, Slack, and shared tracking documents. What is put in writing should be minimal and addressed to counsel for the explicit purpose of obtaining legal advice.

Moreover, the only people who should advise employees about whether and how to share information about the existence and nature of the incident should be the attorneys coordinating the company's incident response. At the start of the investigation, incident response counsel should send a "rules of the road" email to all company attorneys working on the incident response, advising on when and how to communicate about the investigation, stressing the need to maintain privilege, and requiring that counsel approve any request to share information with company employees who are not part of the team investigating the incident.

Have a Written Incident Response Plan and Follow It

At trial, prosecutors faulted the CSO for sharing the existence of the incident with only a small group of what he called Uber's "A Team" of top executives, while keeping other employees in the dark. According to the government, outside of his own security team, the CSO disclosed the incident only to Uber's then-CEO and one member of its legal department, while keeping the matter from other key company figures, including Uber's general counsel.

In addition, the CSO allegedly tried to prevent Uber's new management from learning of the extent of the incident when it began investigating in 2017. According to the government, that included lies to Uber's CEO and outside counsel, falsely stating that the hackers had only been paid after they were identified and deleting from a draft summary of the incident statements that the hack had involved personally identifying information and a very large quantity of user data. Indeed, perhaps the worst moment of the trial for Sullivan came when Uber's CEO testified about his decision to fire the CSO for lying to him.

As noted above, there may be very good reasons for limiting the internal dissemination of information related to a data incident, including the need to preserve attorney-client and attorney work product privilege. But it is critical that decisions about whether and how such information is disseminated be made by legal counsel based on a written incident response plan. Security professionals should not attempt to make these determinations on their own.

Companies should ensure that they have written incident response plans in place that require security professionals to disclose material information related to significant data incidents to the legal department or the company's internal incident response team. The incident response plan should then specify that the legal department shall decide whether, to what extent, and to whom information about the incident is disclosed, given that there are an assortment of state and federal laws and regulations, in addition to company contracts, that may create disclosure obligations.

If asked about the incident by persons not part of the company's incident response team (whether internal or external), company employees can properly decline to comment, citing advice of counsel and the company's incident response plan. Declining to comment pursuant to company policy and legal advice is wholly appropriate, whereas providing a misleading response is never permissible and can lead to serious professional and legal consequences, as demonstrated by this case.

Ransomware Attacks Should Be Disclosed to the FBI Before Any Ransom Is Paid

Ransomware attacks should be disclosed to the FBI before any ransom payment is made for a variety of reasons, from good corporate citizenship, to reducing the chances of an enforcement action from the Office of Foreign Assets Control if the threat actor is a sanctioned entity, to the possibility of recovering funds. This trial adds a new reason: to protect against a misprision charge (although, admittedly, this is an infrequently used federal statute). Misprision only occurs when someone "fails to notify a federal authority as soon as possible" of a known felony and takes "an affirmative act to conceal the crime." Notifying the FBI of a data security incident when a company may be trying to influence a criminal actor to, for example, not make public stolen information negates both of these elements because it will show that the company did notify federal authorities of the crime and will undermine any claim that the ransom payment was intended to conceal the crime.

You can subscribe to future ***Privacy, Cyber & Data Strategy*** and ***White Collar, Government & Internal Investigations*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any of the following:

Privacy, Cyber & Data Strategy

Kimberly Kiefer Peretti
+1 202 239 3720
kimberly.peretti@alston.com

Kellen Dwyer
+1 202 239 3240
+1 212 905 9340
kellen.dwyer@alston.com

Mario Ayoub
+1 202 239 3284
mario.ayoub@alston.com

White Collar, Government & Internal Investigations

Joanna C. Hendon
212.210.1244
joanna.hendon@alston.com

Edward T. Kang
+1 202 239 3728
edward.kang@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32.2.550.3700 ■ Fax: +32.2.550.3719
CHARLOTTE: One South at The Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 4th Floor, Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333