On August 20, 2020, a criminal complaint was filed charging Joseph Sullivan, Uber’s former chief security officer, with obstruction of justice and misprision of a felony in connection with an alleged attempted cover-up of a 2016 data breach. These are serious charges for which Mr. Sullivan has the presumption of innocence.

At the time of the 2016 data breach, Uber was being investigated by the US Federal Trade Commission (FTC) in connection with a prior data breach that occurred in 2014. According to the complaint, the hackers behind the 2016 breach stole a database containing the personal information of about 57 million Uber users and drivers. The hackers contacted Uber to inform the company of the attack and demanded payment in return for their silence. According to the complaint, Uber’s response was to attempt to recast the breach as a legitimate event under Uber’s “bug bounty” program and pay a bounty. An affidavit submitted with the complaint portrays a detailed story of deliberate steps undertaken by Mr. Sullivan to allegedly conceal the 2016 breach from the FTC, law enforcement and the public.
Contemporaneous with the filing of the complaint, the Department of Justice (DOJ) submitted a press release quoting US Attorney for the Northern District of California David L. Anderson:

“We expect good corporate citizenship. We expect prompt reporting of criminal conduct. We expect cooperation with our investigations. We will not tolerate corporate cover-ups. We will not tolerate illegal hush money payments.”

The press release also quoted Federal Bureau of Investigation (FBI) Deputy Special Agent in Charge Craig Fair:

“Concealing information about a felony from law enforcement is a crime. While this case is an extreme example of a prolonged attempt to subvert law enforcement, we hope companies stand up and take notice. Do not help criminal hackers cover their tracks. Do not make the problem worse for your customers, and do not cover up criminal attempts to steal people’s personal data.”

Collectively, the case and statements from the DOJ are probably a unicorn based on, if the facts as alleged are true, a case involving a deliberate cover-up of a data breach in the course of an active FTC investigation. However, many of the statements from the DOJ and the specific allegations in the complaint appear to have potentially far-reaching implications (for companies, their executives and cybersecurity professionals) that breach response counsel must seriously consider in future incidents.

A common question when responding to a ransomware or other cyberattack is whether and when to inform law enforcement. The criminal complaint has the potential to make this an even more difficult decision for future cyberattack victims. Further, while the alleged conduct at issue may seem particularly egregious, the DOJ’s statements could cause a blurring of the lines between what the government may contend is illegal concealment of a security incident and activities generally thought to be legitimate security incident risk and exposure mitigation. We explore these and other key takeaways from the criminal complaint in more detail below.

The Criminal Complaint

Mr. Sullivan is charged with two offenses: obstruction of justice and “misprision of felony.” In support of the obstruction charge, the complaint focuses on Mr. Sullivan’s failure to notify the FTC of the 2016 breach despite its ongoing investigation into a previous and very similar data breach in 2014. Mr. Sullivan, the complaint alleges, had significant involvement in the FTC’s investigation, participating in conference calls, reviewing submissions to the FTC, giving a presentation to the FTC and sitting for a sworn investigative hearing similar to a deposition. Mr. Sullivan reportedly learned of the 2016 breach approximately 10 days after providing his sworn testimony to the FTC. In the months that followed Mr. Sullivan’s discovery of the 2016 breach, the complaint provides that he continued to respond to FTC inquiries without any mention of the incident, notwithstanding that he was “aware that the FTC’s investigation focused on data security, data breaches and protection of
personally identifiable information (PII)."

In addition to his general failure to update or inform the FTC of the 2016 breach, the complaint describes an elaborate attempt on the part of Mr. Sullivan to conceal the breach from the FTC, Uber leadership and the public by recasting the 2016 breach as a legitimate event under the company’s bug bounty program. In connection with this effort, Mr. Sullivan is described as having insisted that the hackers behind the 2016 breach execute a nondisclosure agreement (NDA), which, in addition to not being customary under Uber’s bug bounty program, specifically required the hackers to represent that they had not obtained or stored any data during their intrusion—a factually inaccurate statement. In addition, the hackers were paid a $100,000 bounty, considerably more than any bounty Uber had previously paid under its bug bounty program.

The complaint does not allege that Mr. Sullivan made false statements in any communications with the FTC. Instead, the complaint alleges that Mr. Sullivan took numerous actions to conceal the breach from the FTC and Uber’s new executive leadership team (which had joined the company after the breach), including hiding aspects of the breach from certain engineers, lawyers and executives. The former CEO—who was still in his position at the time of the 2016 breach—however, was allegedly informed by Mr. Sullivan about the incident.

The second charged offense in the complaint is “misprision of felony” under 18 U.S.C. 1515(b):

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.

This rarely charged offense has been interpreted under case law to require an individual to have knowledge that a felony has been committed by another person and fail to report that crime to authorities, and also take affirmative steps to conceal another person’s commission of a felony. The complaint is somewhat vague on the basis for this charge as there are multiple instances of concealment alleged, including concealment vis-à-vis the FTC, law enforcement, Uber’s leadership and the public.

Lessons for Businesses, Executives and Advisors

The complaint offers little guidance to definitively identify actions that must and must not be taken in response to a breach. Indeed, Mr. Sullivan is entitled to the presumption of innocence and may, as a matter of fact and/or law, prevail against the government’s case. Nevertheless, the complaint and the DOJ’s press release shed light on the degree of transparency and cooperation expected by the government, or at the very least what it won’t tolerate. The following are preliminary takeaways and issues for consideration.

**Draw Lines Carefully as to Whether, When and How to Disclose Incidents**
The obstruction of justice charge highlights the importance of making good decisions as to how to characterize a security incident, carefully considering where to draw the line between concealing an incident and downplaying its significance in communications with regulators and the public, and of providing careful, complete answers to inquiries when notifying or otherwise corresponding with regulators or investigators. Omission of facts later deemed to be “material” in such communications may be as serious as making outright false representations.

**Senior Executives Will Need to Be Mindful That Statements They Make (Or Fail to Update) Could Subject Them Individually to Criminal Liability**

Security and other executives should be mindful that potential criminal liability is no longer limited to the company. Employees, in their individual capacities, may be held criminally accountable for inadequate, misleading or deceptive responses.

The allegation of misprision of a felony in the context of a data breach raises important questions as to what constitutes “concealment” of a felony. While intentionally lying to law enforcement, regulators, and other governmental authorities is already a crime, senior executives may be even more cautious if their own freedom may be at risk should they fail to report a cyber incident, such as a ransomware attack. Even if the company reports the incident, if it chooses not to disclose particular aspects of that incident on the basis that they are not “material” or don’t meet other notification thresholds, such as state breach notification obligations, the complaint raises the possibility that such selective disclosure might be perceived as illegal concealment, which may encourage companies to err on the side of disclosure.

As a practical matter, the risk of potential personal criminal liability for decisions made based on the ambiguous and uncertain information inherent in incident response could mean that fewer executives will be eager to sign off on disclosure decisions.

**Companies Investigating a Security Incident Will Need to Consider the Possibility of Whistleblowers**

When this complaint was made public, the news spread rapidly through cybersecurity industry news feeds and blogs. Security executives will have this case front of mind during their next security incident. If a decision is made by the company’s executives or counsel not to notify law enforcement, regulators or the public about a security incident, or if a company decides to disclose something less than the total facts and circumstances of the incident, security executives may feel it necessary to blow the whistle.

**Be Thoughtful about External and Internal Communications Regarding an Incident**

The concealment charge highlights the thin line between coordinating with attackers in responding to an attack, and participating in the criminal activity itself. In responding to incidents, close care must be paid to any communications with attackers. In particular, for ransomware attacks, the company’s first responders
should be clear about the company’s motivations prior to engaging in any negotiation with the attackers. Each decision should be viewed in the context of whether the company is trying to regain access to its assets or prevent the spread of knowledge related to the attack. Companies, with the advice of their counsel, should consider documenting the rationale and business case supporting its decision to engage with the attackers or pay the ransom.

Throughout the complaint, the DOJ alleges that Mr. Sullivan and others developed numerous pieces of documentary evidence developed during the course of the incident that are referred to by the special agent (e.g., an early draft of an executive summary allegedly developed for Mr. Sullivan to use to advise Uber’s CEO about the 2016 incident). These documents reinforce the need for good counsel from the outset of an incident response. Counsel should give their clients good advice regarding the creation of written correspondence or other documents during an incident response. While it is sometimes appropriate to create written documentation during incident response, written materials taken out of context could later be used to build a case directly against an individual.

**Consider the Risks of Voluntary Cooperation with Law Enforcement**

Companies affected by a data security incident are often cautious about disclosing an incident to the FBI. Such apprehension may be well founded, since the FBI’s motives and decisions do not always align with corporate interests.

In recent years, however, companies have warmed to the idea of seeking law enforcement assistance with, and information about, a security incident, especially when they have been victimized by sophisticated attackers using evolving attack methods and tools. Indeed, ransomware attacks have been evolving at an alarming rate, and the FBI has proven to be frequently helpful, sharing attribution information, indicators of compromise and other forensic indicators that can be valuable when attempting to track down and remove malicious trojans and other tools that enable bad actors to have persistent access to a company’s environment.

The complaint against Mr. Sullivan potentially raises the stakes of working with law enforcement, since it may create the impression that failing to disclose all facts about an incident, no matter how small or immaterial, could lead to a criminal concealment accusation. In addition, there may be aspects of an incident that executives may believe should not be disclosed, including to law enforcement. In such cases, it may be safer not to notify law enforcement at all.

**Conclusion**

While the charges in the criminal complaint filed by the DOJ against Mr. Sullivan remain unproven, they are clearly a shot across the bow of corporate executives engaged in incident response efforts. The threat of criminal prosecution of individuals raises the stakes, particularly with regard to the core questions of when, to whom and what to disclose. Security executives in particular now appear to be stuck in the middle, trying to protect the interests of the company while keeping themselves clear of criminal allegations.