Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Uber Exec's Charges In Data Breach Case Reveal Novel Risks

By **Michael Ward, Devika Kornbacher and Elizabeth Matthews**
(September 18, 2020, 6:05 PM EDT)

Michael Ward

Devika Kornbacher

Elizabeth Matthews

In-house lawyers are now very familiar with the anxiety of responding to the potential exposure of confidential information about employees and third parties.

But, until now, the criminal prosecution of company executives was not one of the expected consequences of not disclosing a breach. After the recently announced felony charges against a former Uber Technologies Inc. executive for failing to inform the Federal Trade Commission of a breach, in-house lawyers should now consider this disturbing possibility.

On Aug. 19, federal prosecutors filed criminal charges against former Uber executive Joseph Sullivan in connection with his alleged efforts to cover up a 2016 data breach. The events giving rise to the charges actually started out with Uber as the victim. In November 2016, Uber's systems were breached by cyberattackers who stole the personal data of 57 million users and drivers and demanded a six-figure payment from Uber.

At the time of the 2016 breach, Sullivan was Uber's chief security officer and deputy general counsel who was directly involved in the company's response to the Federal Trade Commission's investigation of a different and much smaller breach Uber had suffered in 2014.

Then, in November 2016, 10 days after providing sworn testimony to the FTC in connection with the 2014 breach investigation, Sullivan learned of the new and much larger breach.

Sullivan was charged with violating Title 18 of the U.S. Code, Section 4, an obscure statute called misprision of felony and one count of obstruction of justice. The complaint alleges three primary acts of concealment in support of the charges.

First, notwithstanding the absence of any federal breach notification law, the complaint alleges that, instead of promptly reporting the new breach to the FTC, Sullivan instead directed that the existence of the breach be kept tightly

controlled, even within Uber, due to the extremely sensitive nature of the materials subject to the breach.

Second, although it is not illegal per se for companies to pay ransom demands, the criminal complaint alleges that Sullivan concealed the breach by using the company's so-called bug bounty program to pay the $100,000 ransom via bitcoin. Like many large technology companies, Uber had a bug bounty program that rewards third parties for finding security gaps and product defects.

And third, the complaint alleged, Sullivan concealed the breach by demanding the cyberattackers execute nondisclosure agreements forbidding disclosure of the breach and related conversations.

The complaint does not allege that Sullivan made any affirmative misrepresentations to the FTC, and it does not appear that the FTC had even asked Sullivan or anyone else at Uber in the course of the 2014 breach investigation if there had been any other similar or subsequent data breaches.

The complaint also acknowledges that Uber's payment of the ransom and execution of the NDAs was with the full knowledge of and at the direction of Uber's then CEO. Uber also voluntarily disclosed the 2016 breach to the FTC before the 2014 breach investigation was concluded.

Novel Legal Issues to Contemplate

A Duty to Report a Crime?

It is often asserted that there is no affirmative obligation to report a crime. That notion is accurate, generally speaking. Most states do not impose such a general duty. However, under Texas law, for example, you can be charged with a Class A misdemeanor for failing to report an offense that resulted in serious bodily injury or death.[1] And, in Ohio, it is illegal to knowingly fail to report a felony.[2]

While these states are exceptions to the general rule, most states' mandatory reporting obligations require only certain professions to report crimes. These mandatory reporters generally include parents, teachers, school administrators, clergy, medical professionals, therapists, social workers and others. In some states, however, anyone who believes child abuse is taking place must report it.

Under federal law, there are mandatory disclosure rules for fraud involving government contractors,[3] affirmative disclosure obligations for specific employee safety issues,[4] and discharge disclosures under environmental statutes.[5]

In short, the general rule has too many exceptions to reflexively assume it will apply to any given context. Therefore, in-house counsel should determine if there are any statutory obligations to report a crime suffered by the company and also consider whether the company has made any factual representations in litigation or investigations or compliance certifications that have suddenly become false or misleading.

Misprision of Felony, Really?

The federal misprision of felony statute applied in the Sullivan case is a curious choice and particularly as applied against the putative victim of the underlying felony, which was the hacking and extortion scheme. Misprision is an often-criticized statute based on English common law, and it has actually been abolished throughout most common law jurisdictions.

A representative prosecution under the statute in 2019 involved an Ohio aluminum company that knew of and failed to disclose Occupational Safety and Health Administration violations committed and concealed by its Canadian subsidiary.[6]

In the Sullivan case, the misprision statute seems to be used as a substitute for a nonexistent federal data breach notification law. But, one reason such a law has not been passed is disagreement among Congress about which breach circumstances should require disclosure and to whom, the form of the disclosure, its timing, etc. This application of the misprision statute could be an end-run around those disagreements.

Acts of Concealment?

Under the misprision of felony statute, what transforms a permissible failure to report into criminal conduct is an act or acts of concealment.[7]

In the Sullivan case, it does not appear from the complaint that Sullivan or anyone else at Uber lied to the FTC about the existence of the 2016 breach. Instead, the alleged acts of concealment were Sullivan's enforcement of a very restrictive need-to-know approach internally and his use of NDAs with external parties like the cyberattackers.

In-house lawyers will likely find it unsettling to hear these tools and practices be characterized, without qualification, as acts of criminal concealment. The use of NDAs in the corporate environment is beyond ubiquitous. Companies routinely include such terms in agreements with customers, prospective customers, suppliers, current employees, departing employees, litigants and even mere visitors to the corporate campus. NDA terms are regularly included in negotiated terminations of employees or executives, or in disputes with suppliers or customers, where one or both are alleging that they were cheated or defrauded.

Are these instances of criminal concealment? If using an NDA with the generalized intention to keep information confidential is construed to include a specific intention to conceal from law enforcement, NDAs will become a greater source of risk.

Action Items for In-House Counsel

Plan Your Work; Work Your Plan

The fast paced, hectic, highly charged environment that accompanies a data breach and ransom demand is not the best time to decide policy questions, or who should be informed of the crisis. Companies should take the time before a crisis to establish a critical incident response plan, and among those critical incident variations must be a data breach. Contingencies and checklists should be established and thought through in advance so that issues and considerations don't get missed in the urgency of the moment.

Who's at the Table

General counsel should ensure that the company has an incident response plan that defines what events will trigger the plan and identifies the key stakeholders who must be immediately informed of the issue. Another good practice is a mandatory escalation policy that defines the types of issues that require

immediate notification of one or more senior executives and relevant board members.

One of the challenges in the Sullivan case is that the existence of the data breach and ransom demand was very closely held and the key decisions were made primarily by just two people. It's easy to imagine that Uber's general counsel and various board members might have counseled a different approach, but their voices were excluded. Excluding the board from participation in overseeing key enterprise risks is also a corporate governance question that is receiving growing scrutiny from Delaware courts.

Bug Bounties and Ransomware

Companies should review their approaches to bug bounties and data ransom demands. Many technology and other companies operate a bug bounty program that modestly rewards third parties for identifying security and other defects in networks and/or products. Almost all bug payments involve some restrictions on disclosure, i.e., an NDA, that either prohibit any disclosure or only after it has been patched. Most bugs do not involve criminal conduct, but ransomware demands invariably do. It is not per se illegal to pay a ransomware demand.

But, under the theory of the complaint in Sullivan, it might be illegal to not report the ransom demand. Where the explicit or implicit purpose of the ransom payment is to stop the cyberattackers from publicly disclosing that your company was hacked, companies should consider if it is advisable to notify law enforcement even if the notification is after the fact.

Nondisclosure Agreements

The use of NDAs in settlement agreements came under great scrutiny as part of the #MeToo movement, where they were seen as a tool that helped cover up and perpetuate continuing misconduct. Several companies resolved to discontinue their use in certain employment contexts.

To partially mitigate the risk that a prosecutor could construe the purpose of an NDA as intending to obstruct law enforcement, at a minimum, in-house counsel should include terms that exclude disclosures made in response to inquiries from law enforcement.

Assess Duty to Disclose

We have pointed out that the general principle that a company or person does not have a duty to report a crime is actually rife with exceptions. In the data security context, affirmative state data breach notification obligations abound. In the Sullivan case, the government suggests that the defendant had a greater burden to disclose because of the then-ongoing FTC investigation into a different breach.

Companies, especially government contractors and public companies, are also regularly making filings and representations in different venues. Any decision not to disclose a particular circumstance or event should be made with complete situational awareness to ensure that affirmative representations to the contrary have not already been made.

In-House Lawyer Jeopardy

In-house counsel should pause to consider that Sullivan was not just Uber's chief security officer but also an in-house lawyer. In-house counsel recognize how intertwined they are with decisions about data breaches specifically, voluntary disclosure decisions and, of course, the ubiquitous NDA usage.

Counsel should remind themselves and their internal stakeholders of the fragility of the attorney-client privilege. Even if validly applied and carefully protected in a particular context, the privilege can be pierced by the crime-fraud exception and it can be readily waived by new management. Participants may and should avail themselves of the privilege but it is good advice to always act and communicate with the expectation of future transparency.

Michael Ward is a partner at Vinson & Elkins LLP. He is a former federal prosecutor and former in-house chief compliance officer for multiple companies.

Devika Kornbacher is a partner and head of the cybersecurity and data privacy practice at V&E.

Elizabeth Matthews is an associate at the firm.

V&E associate Branden Stein contributed to this article.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See Tex. Trans. Code § 550.021.

[2] Ohio Rev. Code § 2921.22.

[3] See 48 C.F.R. §§ 9.406-2(b)(1)(vi), 9.407-2(a)(8).

[4] See 15 U.S.C. § 78m–2 (requiring reporting of certain mine safety incidents); see also 29 C.F.R. § 1904.39 (OSHA reporting obligation).

[5] See 42 U.S.C. § 9603; see also Incentives for Self-Policing: Discovery, Disclosure, Correction and Prevention of Violations (Audit Policy), 65 Fed. Reg. 19618 (Apr. 11, 2000)

[6] United States v. Extrudex Aluminum, Inc., No. 4:19-cr-00195 (N.D. Ohio 2019).

[7] In the 9th Circuit, where the Sullivan case is being prosecuted, a violation of 18 U.S.C. § 4 has the following elements: (1) that the principal committed and completed the felony alleged; (2) that the defendant had full knowledge of that fact; (3) that he failed to notify the authorities; and (4) that he took affirmative steps to conceal the crime of the principal. United States v. Olson, 856 F.3d 1216, 1220 (9th Cir. 2017).