New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
ALM.
MAY 6, 2022

Cybersecurity and Individual Liability: 'U.S. v. Sullivan' and the Criminalization of a Cyber Attack Response

By Jonathan S. Sack and Christopher M. Hurley

Cyberattacks, data breaches, ransomware—these are now the stuff of corporate and boardroom discussion. Hardly a day goes by without a reminder of the centrality of cybersecurity to business and government. In one of many recent headlines, the country's largest oil and gas pipeline system, Colonial Pipeline, was the target of a cyberattack in 2021 and a demand for a $4.4 million ransom, which was paid with the support of federal authorities. War in the Ukraine has heightened already intense concern about the vulnerability of critical infrastructure to cyberattacks.

To date, cybersecurity has generally been viewed as an organizational responsibility, and data breaches similarly have been treated as organizational weaknesses or failures. States have enacted laws that require organizations to report incidents of data theft "expeditiously" to state authorities and individuals adversely affected. In addition, public companies are required to disclose information about data breaches when such information is material to investors.

Against this backdrop of organizational responsibility, the Department of Justice has brought a noteworthy criminal case against an individual for his personal response to a corporate data breach. In *United States v. Sullivan*, Case No. 3:20-cr-00337-WHO (N.D. Cal.), the defendant, a former employee of Uber Technologies (Uber), has been charged with wire fraud and other offenses that arise from his handling of a ransomware attack against Uber in 2016. While Uber settled potential civil charges with state attorneys general and the Federal Trade Commission (FTC), Uber was not charged criminally.

In this article, we begin with a description of the events underlying the charges in *Sullivan* and then discuss the theories of prosecution and defense. Next, we turn to the present regulatory framework for data breach reporting and consider the impact of new rules—most notably, the SEC's recent proposed regulation on cyber incident disclosure. We conclude with observations about the prospect of individual liability in this rapidly evolving and vital area of the law.

'Sullivan' Background

The events underlying the *Sullivan* prosecution began in September 2014, when Uber suffered a data breach that resulted in the theft of personal information for approximately 50,000 drivers (the 2014 Breach).

In February 2015, Uber reported the 2014 Breach to the FTC, which then launched an investigation into Uber's data security practices. Shortly before the FTC investigation began, Sullivan became Uber's Chief Security Officer (CSO), and in that capacity he assisted with Uber's responses to the FTC investigation. The facts set forth below are based on allegations in a criminal complaint filed against Sullivan in August 2020.

On Nov. 14, 2016, while the FTC investigation was pending, Sullivan discovered that Uber's cyber defenses had again been breached, and that hackers had obtained information about roughly 600,000 drivers (the 2016 Breach)—more than 10 times the number of drivers affected by the 2014 Breach. Within 24 hours, Sullivan discussed the breach with Uber's then CEO, Travis Kalanick. Over the next month, Sullivan arranged a payment of $100,000 to the

hackers under Uber's "bug bounty" program on the condition that the hackers sign non-disclosure agreements (NDAs).

Uber's bug bounty program offered money to individuals who brought data security vulnerabilities to its attention. According to DOJ, the program was not intended to reward someone who actually accessed or obtained sensitive data, and a reward was not typically conditioned on signing an NDA. The criminal complaint alleged that the hackers, in fact, had obtained sensitive data, and that the NDAs falsely represented that they had not.

According to the criminal complaint, Sullivan did not report the 2016 Breach to the FTC and did not raise the 2016 Breach again with Uber management until September 2017, when he was asked to brief Uber's new CEO on the 2016 Breach. Sullivan reportedly indicated that the bug bounty payment had been made only after Uber learned the hackers' true identity and did not mention that the hackers had actually taken Uber drivers' sensitive data. After further investigation, Uber learned the full extent of the 2016 Breach and ultimately disclosed it to the FTC and the public in November 2017, and then fired Sullivan.

'Sullivan' Prosecution

In September 2020, a grand jury in the Northern District of California returned an indictment against Sullivan which charged him with obstruction of administrative proceedings, in violation of 18 U.S.C. §1505; and misprision of a felony, in violation of 18 U.S.C. §4. In the government's view, Sullivan knew the 2016 Breach was relevant to the FTC's investigation of the 2014 Breach, but willfully failed to report it to the FTC and took steps to prevent its discovery.

In a December 2021 superseding indictment, the government added charges of wire fraud, in violation of 18 U.S.C. §1343. According to the government, Sullivan made false and misleading statements with the intent to deprive Uber drivers of their legal right to notification under California law, and that such notification would have been material to an Uber driver's decision whether to continue to pay Uber's "Service Fee." In support of this charge, the superseding indictment alleges that Sullivan sought to conceal the 2016 Breach by, among other things, falsely characterizing payments to the hackers as legitimate payments under the bug bounty program, and orchestrating false and misleading NDAs.

Sullivan pled not guilty and recently moved to dismiss the wire fraud charges. In the defense's view, Uber made Sullivan the fall-guy for the 2016 Breach to "burnish the image of its new CEO" and deflect from Uber's corporate responsibility for the response to the 2016 Breach. The defense denies that Sullivan concealed information from Uber and points to knowledge of the 2016 Breach on the part of various members of Uber's legal department and management.

Sullivan has taken aim at what he argues is an improper theory of wire fraud. Sullivan's primary argument is that Uber's continued receipt of service fees from affected drivers, the money or property allegedly at issue, was no more than an "incidental byproduct" of the charged scheme to conceal the 2016 Breach and certainly not the *object* of the scheme, as required by *Kelly v. United States*, 140 S. Ct. 1565 (2020). Two of Sullivan's other arguments are noteworthy. He contends that the wire fraud charges "violate the convergence principle of *United States v. Lew*, 875 F.2d 219 (9th Cir. 1989)" to the extent they depend on misrepresentations that he made to Uber's CEO or outside counsel because they "were not among the persons from whom Sullivan allegedly intended to continue receiving money or property," i.e., the drivers. In addition, Sullivan contends that a fraud charge premised on a failure to make a disclosure under California law would run afoul of "federalism principles" by transforming "almost any violation of a state data breach notification law into a federal felony."

In its opposition to Sullivan's motion to dismiss, the government countered that Uber's receipt of service fees was "at the center" of Sullivan's plan, and that the defense was raising an issue of intent which may not be decided on a motion to dismiss. The government also argued that the charges do not violate *Lew*'s "convergence principle" because Sullivan did not need to misrepresent anything directly to the drivers so long as misrepresentations were made to them as "part of a larger scheme" under *United States v. Ali*, 620 F.3d 1062 (9th Cir. 2010). Lastly, the government pointed to cases in which fraud charges based on omissions were upheld under similar or even less compelling circumstances than those in the instant case.

Regulatory Environment

The prosecution of Sullivan cuts against the grain of prevailing regulation. State data breach reporting laws impose duties on organizations, not individuals. See, e.g., *Data Breach Notification Laws by State*, IT Governance. The same is true under federal law. At present, regulations

issued by the FTC and the Department of Health and Human Services require organizations that collect confidential medical information to report data breaches. More generally, the FTC has issued guidance that organizations should notify affected parties and law enforcement promptly following a data breach. Recent remarks from FTC Chair Lina Khan suggest that more formal regulatory action may be coming. See Lina M. Khan, Chair, Remarks as Prepared for Delivery at IAPP Global Privacy Summit 2022 (April 11, 2022). In 2011 and 2018, the SEC issued guidance to public companies regarding the disclosure of cybersecurity incidents and risks. This guidance derives from a public company's duty to report material information. To date, the reach of federal law is limited and does not establish comprehensive reporting rules on organizations, much less on individuals.

The reporting framework for public companies may change significantly if proposed SEC regulations, issued on March 9, 2022, are adopted in something like their present form. The proposal addresses public company disclosures related to companies' cybersecurity risks and incidents. See *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, 87 FR 16590 (proposed March 9, 2022). The proposed rule would require disclosure of a cybersecurity incident within four business days of a determination that it is material. Other proposals would mandate periodic reports regarding an issuer's policies and procedures to identify and manage cybersecurity risks. On this latter point, companies would need to report whether the company has designated a chief information security officer (CISO) as well as the relevant cybersecurity experience of the CISO and any members of the board. See 87 FR at 16600 (proposed).

In light of its significance and breadth, the proposed rule will likely attract a significant number of comments. Critics may build on a sharply worded dissent filed by Commissioner Hester M. Pierce, which took issue with the proposal's "unprecedented micromanagement" of corporate management and directors in their handling of cybersecurity. See Hester M. Pierce, *Dissenting Statement on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposal*, SEC (March 9, 2022).

Barely a week after issuance of the proposed Cybersecurity regulations, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022, H.R. 2471, 116th Cong. (CIRCI). CIRCI requires entities to report (1) any "substantial" cyber incidents no later than 72 hours after discovery or (2) any ransomware payments made as a result of a digital attack against critical infrastructure within 24 hours after the payment is made. H.R. 2471 §§2242(a)(1)(A), 2242(a)(2)(A). The entities covered by the law have not yet been determined, but CIRCI cites Presidential Policy Directive 21's broad definition of "an entity in a critical infrastructure sector." H.R. 2471 §2240(5).

Both CIRCI and the SEC's proposed rule would impose detailed requirements rather than leave key decisions to the judgment of organizations based on general standards such as materiality. Significantly, neither the new law nor proposed regulations (if adopted) would impose liability on individuals like Sullivan, except, perhaps, as a secondary actor under the securities laws in certain situations.

Conclusion

In recent pronouncements, DOJ has made it clear that the prosecution of white-collar offenses, particularly individual offenders, is a high priority of the present administration. Sullivan was initially charged in the Trump Administration, and wire fraud charges were added in a superseding indictment in the Biden Administration. In this case, what stands out is not so much a change of administration but, rather, whether the *Sullivan* case signifies an intention to hold individuals accountable for perceived failings in an organization's response to a cyber incident. This intention is reflected, in particular, by the recent addition of wire fraud charges which, if upheld, could be the basis for charging many other individuals whose response to a cyber incident might be found deficient.

Cyber incidents are challenging to any organization; they require gathering facts under great pressure, assessing the damage, containing the damage to the organization's business—all while trying to comply with the letter and spirit of multiple laws. In this context, the question of individual liability may take on greater significance as the rules governing cyber incidents become more and more specific and demanding.

Jonathan S. Sack *is a member of Morvillo Abramowitz Grand Iason & Anello P.C. and a former chief of the criminal division in the U.S. Attorney's Office for the Eastern District of New York.* **Christopher M. Hurley** *is an associate at the firm.*