New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 261—NO. 38
WEDNESDAY, FEBRUARY 27, 2019

Outside Counsel

Will 2019 Be the Year of Blockbuster Cybersecurity Enforcement by the SEC?

By **Joseph Facciponti**

And **Katherine McGrail**

After years of admonishing financial institutions and public companies to take cybersecurity more seriously, the U.S. Securities and Exchange Commission (SEC) appears ready to back up its words with investigations and penalties. Starting with Jay Clayton's confirmation as SEC Chair in 2017, the agency has enhanced its efforts to protect investors and markets from increasingly dangerous and costly cyber threats. Indeed, the SEC's conduct over the past two years—including creating a dedicated Cyber Unit in its Enforcement Division and by bringing several first-of-their-kind cybersecurity enforcement actions—foretell that the agency is prepared to take an even more aggressive approach in addressing cybersecurity issues among the entities it supervises. As a result, firms that have yet to dedicate sustained attention to their cyber threats and risks may find that the SEC is far more willing to use a stick rather than a carrot to obtain compliance.

JOSEPH FACCIPONTI *and* KATHERINE McGRAIL *are partners at Murphy & McGonigle, P.C., a financial services law firm. Mr. Facciponti is a former cybercrime prosecutor at the U.S. Attorney's Office for the Southern District of New York. Ms. McGrail counsels financial institutions on compliance with industry regulations and serves as the firm's chief diversity and inclusion officer.*

The SEC's Focus On Cybersecurity

Since his confirmation as SEC Chair in 2017, Clayton has made cybersecurity one of the SEC's main priorities. In 2017, Clayton formed the cybersecurity working group, an initiative to coordinate information sharing, risk monitoring, and incident response throughout the SEC. In discussing the working group, Clayton defined the SEC's cyber focus as "identifying and managing cybersecurity risks and ensuring that market participants—including issuers, intermediaries, investors and government authorities—are actively engaged in this effort and are appropriately informing investors and other market participants of these risks." See SEC Public Statement, *Statement on Cybersecurity* (Sept. 20, 2017).

In September 2017, the SEC also announced the creation of a Cyber Unit. The Cyber Unit was formed to consolidate the expertise of the SEC's Division of Enforcement and enhance its ability to identify and investigate a wide-range of cyber-related threats, including (1) market manipulation schemes involving false information communicated electronically; (2) hacking to obtain material nonpublic information; (3) fraud involving blockchain technology and "initial coin offerings"; (4) hacking into retail brokerage accounts; and (5) cyber threats to trading platforms and market infrastructure. In commenting on the Cyber Unit's launch, Stephanie Avakian, co-director of the SEC's Enforcement Division, identified cyber-related threats as "among the greatest risks facing investors and the securities industry." SEC Press Release 2017-176, *SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors* (Sept. 25, 2017).

Since its creation, the Cyber Unit has wasted little time in bringing cases. According to the Enforcement Division's 2018 Annual Report, during 2018, the SEC brought 20 stand-alone cases related to cybersecurity and has 225 cyber-related investigations that it deems "ongoing." See SEC

Annual Report, Division of Enforcement (Nov. 2, 2018). In several cases, the enforcement actions were first-of-their-kind, as discussed below.

The SEC's focus on cybersecurity also appears to be driven by its own experience with cybersecurity issues. The same month that the SEC announced the creation of its Cyber Unit, the SEC announced that it, too, has experienced data breaches. In an extended Statement on Cybersecurity that likely is also intended to serve as a model for public companies in discussing their own material cybersecurity risks and incidents, Clayton announced a number of cybersecurity risks and data incidents effecting the SEC, the most significant of which involved hackers gaining access to the SEC's EDGAR filing database in 2016 to steal unreleased corporate filings that potentially contained material nonpublic information. See SEC Public Statement, *Statement on Cybersecurity* (Sept. 20, 2017).

Public Company Cybersecurity Disclosures

Cyber Disclosure Guidance. One of the centerpieces of the SEC's enhanced cybersecurity strategy is in encouraging public companies and issuers to be transparent with the investing public about their material cyber risks and incidents. In September 2017, Clayton said that he is "not comfortable that the American investing public understands the substantial risks that we face systemically for cyber issues, and I'd like to see better disclosure around that." C. Germaine, *Clayton Says No Shift in Enforcement Priorities at SEC*, Law360 (Sept. 6, 2017). Perhaps exemplifying the SEC's concerns, that same month, credit reporting agency Equifax disclosed that an unknown attacker had stolen personally identifiable information of approximately 145 million consumers. K. Coen, *Populist Pitchforks Come Out: Insider Trading and Equifax,* Law360 (Nov. 6, 2017). Equifax faced immediate public criticism over the timeliness and adequacy of its disclosure, which came approximately six weeks after it discovered the breach. Further, questions were raised about potential insider trading by four Equifax executives, including the Chief Financial Officer, all of whom collectively sold $1.8 million of Equifax shares between the time the breach was discovered and when it was disclosed to the public. Id. An internal review ultimately cleared those executives of any wrongdoing.

> Firms that have yet to dedicate sustained attention to their cyber threats and risks may find that the SEC is far more willing to use a stick rather than a carrot to obtain compliance.

In February 2018, and consistent with the SEC's focus on disclosure—and perhaps in response to the Equifax breach—the SEC published revised guidance regarding public company disclosures about material cyber risks and incidents (2018 Guidance). See SEC Release Nos. 33-10459 & 34-82746, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* (Feb. 26, 2018). The 2018 Guidance consolidated and built upon the SEC's prior guidance on disclosure obligations relating to cybersecurity, particularly the Division of Corporation Finance's guidance from 2011. Among other things, the 2018 Guidance addresses topics such as: (1) the criteria for determining whether a cyber risk or incident is "material"; (2) how promptly companies must disclose material cyber incidents; (3) the level of specificity required when disclosing material cyber risks; and (4) the need to adopt policies and procedures to prevent insider trading on as-yet undisclosed cyber incidents.

Disclosure-Related Enforcement Actions. At the time the 2018 Guidance was released, it was still unclear whether the SEC would bring an enforcement action against an issuer that failed to disclose material cyber risks or incidents to the investing public. Previously, Stephanie Avakian said that she could "absolutely" envision a situation in which the SEC would bring an enforcement action for inadequate cyber disclosures. J. Hoover, *SEC Suits Over Cyber Reporting Could Be on the Horizon*, Law360 (April 20, 2017).

That uncertainty was resolved in April 2018, when the SEC announced its first-ever enforcement action against a public company for failing to disclose a breach. The enforcement action involved Yahoo, which the SEC alleged had misled shareholders by not disclosing in its public filings for nearly two years a data breach that affected hundreds of millions of its internet email subscribers. See SEC Press Release 2018-71, *Altaba, Formerly Known as Yahoo!, Charged with Failing to Disclose Massive Cybersecurity Breach; Agrees to Pay $35 Million* (April 24, 2018). The Yahoo breach only came to light as a result of merger discussions with Verizon, which sought to purchase the company. According to the SEC, Yahoo's senior management and legal staff allegedly "did not properly assess the scope, business

impact, or legal implications of the breach, including how and where the breach should have been disclosed in [its] public filings or whether the breach rendered, or would render, any statements made by [it] in its public filings misleading."

The SEC further noted that the company's disclosures in its public filings were misleading to the extent they omitted known trends or uncertainties presented by the data breach. In addition, the SEC alleged the risk factor disclosures in the company's public filings were misleading in that they claimed the company only faced the risk of potential future data breaches without disclosing that a data breach had in fact already occurred. The SEC noted that while immediate disclosure (such as in a Form 8-K) is not always necessary in the event of a data breach, the breach should have been disclosed in the company's regular periodic reports. The company ultimately agreed to pay a $35 million fine.

In the case of Yahoo, the failure to disclose the breach had a clear effect on the company's shareholders, who saw Verizon reduce its purchase price for Yahoo by $350 million after the breach was disclosed. In announcing the Yahoo enforcement action, Steven Peikin, co-director of Enforcement, observed that "[w]e do not second-guess good faith exercises of judgment about cyber-incident disclosure. But we have also cautioned that a company's response to such an event could be so lacking that an enforcement action would be warranted. This is clearly such a case." Id.

It remains to be seen whether the SEC will take any actions with respect to Equifax for its six-week delay in disclosure of its 2017 breach. However, in March and June of 2018, the SEC charged two former Equifax employees with trading on material nonpublic information related to the Equifax breach. See SEC Press Release 2018-40, *Former Equifax Executive Charged With Insider Trading* (March 14, 2018) and SEC Press Release 2018-115, *Former Equifax Manager Charged With Insider Trading* (June 28, 2018). The U.S. Department of Justice also brought parallel criminal insider trading charges against these individuals. Notably, the two individuals charged were not included among the four Equifax executives who were initially suspected of engaging in potential insider trading.

> Public companies and entities registered with the SEC would do well to heed the SEC's admonitions and take a close and careful look at their cybersecurity-related policies and procedures to ensure full compliance.

The charges against these individuals highlight the challenge public companies face in managing information related to a breach among their employees prior to public disclosure. In Equifax's case, neither defendant was told about the breach directly. Instead, Equifax provided them with a false cover story to explain the breach mitigation work they were asked to perform. Because the defendants were not told about the breach, they were not also expressly instructed that a blackout had been imposed on Equifax share sales. The defendants eventually pieced together the clues about the breach and sold their shares prior to the company's public disclosure of the breach.

Data Security Safeguards

In addition to cybersecurity disclosures, the SEC has also reaffirmed its commitment to seeing registered entities such as broker-dealers and investment advisers implement appropriate data security programs to protect their systems and customer data.

For example, the 2019 examination priorities of the SEC's Office of Compliance Inspections and Examinations (OCIE) again feature *cybersecurity* as a top priority. See SEC 2019 Examination Priorities, Office of Compliance Inspections and Examinations (Dec. 20, 2018). Among other things, OCIE continues to stress the importance of cyber risk assessments, access rights, vendor management, training, and data loss prevention for firms. The scope of focus, however, has sharpened over the last year to include the configuration of network storage devices, policies and procedures related to retail trading information security, and practices at investment advisers with multiple branch offices or that have recently merged with other investment advisers. Further, for entities that maintain critical market infrastructure, OCIE will examine compliance with SEC Regulation SCI, which requires such entities to maintain policies to protect their systems' capacity, integrity, resiliency, availability, and security.

Given the SEC's sharp focus on cybersecurity compliance issues for broker-dealers and investment advisers, one would expect to see a corresponding focus by Enforcement Division on these issues as well. And, in fact, in September

2018, the SEC brought another first-of-its-kind enforcement action that, notably, was based on a referral from an OCIE examination. See SEC Press Release 2018-213, *SEC Charges Firm With Deficient Cybersecurity Procedures* (Sept. 26, 2018). In that action, a mid-sized broker-dealer and investment adviser was fined $1 million for alleged cybersecurity lapses that allowed hackers to access client Social Security Numbers, account balances and details of client investment accounts. In additional to finding a violation of the Regulation S-P—the SEC's Safeguards Rule—the SEC dusted off its "Identity Theft Red Flags Rule" to censure the firm. The Identity Theft Red Flags Rule—also called "Regulation S-ID"—requires designated financial firms to develop and implement a written identity theft prevention program "designed to detect, prevent, and mitigate identity theft" for investment accounts. The rule also requires board oversight of the identity theft program. Although the SEC had adopted the red flags rule five years ago, it has not been used in an enforcement action until now.

The SEC outlined a phishing scheme in which attackers impersonated the firm's contractors over a six-day period in 2016 and convinced employees on the firm's support line to reset certain contractor passwords and, in some cases, provide them to the hackers over the phone. The hackers then used the new passwords to gain access to the personal information of 5,600 customers. Even though the firm did have some protections in place, the SEC found them inadequate, in part because in some instances, the malevolent actors called from phone numbers the firm had previously associated with fraudulent activity and, in other instances, the helpdesk staff did not sufficiently understand the firm's system settings such that they could effectively mitigate the attack. The SEC ultimately found the firm's conduct to be so alarming that it deemed the violation "willful." The firm agreed to pay a $1 million settlement even though no customers were found to have suffered a financial loss as a result of the attack.

Accounting Controls and Business Email Compromises

Opening up yet another area of focus regarding cybersecurity, on October 16, 2018, the SEC issued a Report of Investigation (the Report) detailing an investigation by the SEC's Enforcement Division into the internal accounting controls of nine public companies that were victims of "business email compromises," a form of cyber fraud. See Securities Exchange Act of 1934 Release No. 84429, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements* (Oct. 16, 2018). Business email compromises occur when attackers send phishing emails that typically impersonate senior executives or outside vendors in an attempt to trick company employees to transfer funds to the attackers. These email spoofs—also sometimes called "CEO scams" or "vendor scams"—do not require technologically sophisticated hacks, but instead exploit common policies and procedures concerning wire transfers and other payments. Perpetrators often target corporate finance departments in an effort to reroute planned wire payments or generate new transfers to offshore accounts. The SEC noted business email compromises affect public companies across all industries and that these attacks have caused over $5 billion in loses since 2013, which was the "highest estimated out-of-pocket losses from any class of cyber-facilitated crime during this period."

The SEC issued the Report pursuant to Section 21(a) of the Securities Exchange Act, forgoing traditional enforcement actions against any of the companies involved, to communicate the SEC's view that this issue is problematic and to put issuers and individuals on notice that the SEC intends to pursue enforcement actions where companies have failed to maintain internal accounting controls that reasonably safeguard company assets. In releasing the Report, the SEC is sending a clear message that it expects issuers to not only act responsibly in the event of a cybersecurity incident but also to institute appropriate controls to mitigate the risks of cyber-related threats and safeguard company assets from those risks.

Conclusion

The SEC has, in the past, largely taken a softer approach to encouraging compliance in the cyber-security arena, but the agency now appears ready to bring significant enforcement actions for cyber-related missteps. Public companies and entities registered with the SEC would do well to heed the SEC's admonitions and take a close and careful look at their cybersecurity-related policies and procedures to ensure full compliance.