SEC Issues Statement on Cybersecurity

Katz, Marshall & Banks Partner **Alexis Ronickher** published an article in Corporate Compliance Insights on October 10, 2017 entitled "SEC Issues Statement on Cybersecurity." **Click here** to view the article on the CCI website, or read the full text of the article below.

High-profile data breaches seem to come fast and frequently these days. Last month, the Securities and Exchange Commission revealed it was the target of a cyberattack through which the criminals gained access to nonpublic information. With the announcement, the SEC declared its renewed focus on cybersecurity and reminded the public of the important role whistleblowers play in enforcement efforts.

On September 20, the U.S. Securities and Exchange Commission (SEC) announced that it had suffered a cyber breach that potentially allowed intruders to make an illegal profit from nonpublic information they had accessed.**[1]** The announcement rattled Wall Street and investors and brought the SEC under congressional scrutiny. The SEC, however, seized the opportunity and used the announcement to reinforce its commitment to taking cybersecurity risks seriously and to emphasize that a company's failure to similarly do so could result in an enforcement action.

This is not an empty warning. Over the last five years, the SEC has taken several enforcement actions related to cybersecurity. Most have involved market manipulation through hacking, but the SEC also has taken action against certain SEC-regulated participants in the financial markets for failure to safeguard customer data. In its most high-profile action of that type, in June 2016 the SEC announced a $1 million penalty against Morgan Stanley Smith Barney LLC for failure to safeguard customer data. To date, the SEC has not taken any enforcement action against a public company for inadequately disclosing cyberattacks or cybersecurity threats in its public filings. Media reports, however, indicate that the SEC is investigating Yahoo's untimely disclosure to the public of two mega-breaches.

In a September 20 statement issued in conjunction with the cyber-breach announcement, SEC Chairman Jay Clayton specifically identified three areas of focus for the Commission related to cybersecurity: the adequacy of disclosures to shareholders by public companies, strong protection of securities market infrastructure (e.g., stock exchanges) and proper information-security practices on the part of market participants (e.g., broker-dealers, investment advisors). Chairman Clayton specifically warned public companies that the failure to "take their periodic and current disclosure obligations regarding cybersecurity risks seriously… may result in an enforcement action."**[2]**

In the wake of this month's Equifax mega-breach that jeopardizes the financial security of 143 million Americans, the SEC's restatement of its commitment to pursuing enforcement actions related to cybersecurity is good news for whistleblowers. Both the SEC and the Equifax breaches demonstrate that even entities that purportedly take cybersecurity seriously are vulnerable to catastrophic breaches. While no entity can be 100 percent secure from cyberattacks, conscientious employees who raise alarms when they discover cyber vulnerabilities are a critical means for combating cyber breaches and protecting their employers and the public.

Employees who are legally protected from retaliation are more willing to blow the whistle when they observe illegal conduct. And while no federal law explicitly protects cybersecurity whistleblowers, the SEC's several cybersecurity enforcement actions and the Commission's cybersecurity guidance, including Chairman Clayton's statement, create a strong basis for arguing that the anti-retaliation provisions of the Sarbanes-Oxley Act of 2002 (SOX) and the Dodd-Frank Act Wall Street Reform and Consumer Protection Act (Dodd-Frank) protect a wide range of potential cybersecurity whistleblowers, including not just employees of market participants, but also employees of public companies.

The SEC's enhanced focus on cybersecurity also means that an insider who has information about his or her employer's failure to meet its public disclosure requirements or its failure to comply with the SEC's information security requirements should consider providing the information to the SEC Office of the Whistleblower. The SEC Whistleblower Program incentivizes such reporting by issuing awards of 10 to 30 percent of the monetary sanctions the SEC recovers in enforcement action based on the whistleblower's information and provides incentives to whistleblowers who first report their information to company management. To be eligible for an award, the cumulative amount of the sanctions and penalties has to be over $1 million. This means that a viable SEC tip must provide information about a significant potential violation, such as Yahoo's failure to publicly disclose the two mega-breaches for years or Morgan Stanley's decade-long failure to protect confidential customer data, which allowed hackers to steal the data and use in schemes that could have caused serious harm to customers on a large scale.

The SEC's focus on cybersecurity, coupled with related whistleblowers protections and incentives, is good not just for the whistleblowers, but for the public overall. We live in a time when our most private information — health history, financial records — is under siege, and for most of us, every few months we learn that our information has again been compromised. Because data-breach litigation by consumers has been met with mixed results, however, companies may feel less compelled to take the necessary steps to shore up their cybersecurity, particularly given the high costs associated with achieving a robust cybersecurity posture. Government regulators like the SEC may end up being the primary enforcers that will force companies to protect the valuable information with which they are entrusted. Whistleblowers with inside information will be critical to government enforcement efforts, and their willingness to come forward is best assured with adequate incentives and protections.

[1] SEC Chairman Clayton Issues Statement on Cybersecurity (Sept. 20, 2017), *available at*: **https://www.sec.gov/news/press-release/2017-170**.

[2] Clayton, Jay, Statement on Cybersecurity, U.S. Securities and Exchange Commission (Sept. 20, 2017), *available at*: **https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20**

Washington DC Office
202.299.1140
1718 Connecticut Avenue, NW
Sixth Floor
Washington, DC 20009
202.299.1148 fax

Philadelphia Office
215.735.2171
1845 Walnut Street
25th Floor
Philadelphia, PA 19103