SEC ANNOUNCES CREATION OF CYBER UNIT

Following the announcement of its own data breach, on September 25, 2017, the SEC announced a new enforcement initiative that will target cyber-related threats. SEC Chair Jay Clayton has made it clear that he views the SEC's mission as focused on "Main Street investor[s],"[i] and he has indicated that he is "not confident that the Main Street investor has received a sufficient package of information . . . to understand the substantial risks resulting from cybersecurity and related issues."[ii] Accordingly, this new unit will focus on targeting cyber-related misconduct.

THE SEC CYBER UNIT

The new Cyber Unit will be part of the SEC's Enforcement Division and will focus on conduct including: (i) spreading false information through electronic and social media to manipulate the market; (ii) hacking to obtain material nonpublic information; (iii) violations involving distributed ledger technology and initial coin offerings; (iv) intrusions into retail brokerage accounts; and (v) cyber-related threats to trading platforms and other critical market infrastructure. Robert A. Cohen, former co-chief of the Market Abuse Unit, was appointed chief of the new Cyber Unit which, according to Stephanie Avakian, Co-Director of the SEC's Enforcement Division, "will enhance [the SEC's] ability to detect and investigate cyber threats through increasing expertise in an area of critical national importance."

Many of the kinds of matters that the new unit will address have already been the subject of enforcement actions. For example, the SEC has brought a number of cases related to market manipulation based on spreading false information. One such case, filed in May 2016, alleged that Nauman Aly, a Pakistani trader, electronically filed a false Schedule 13D – a form that individuals who hold more than 5% of any class of publicly traded securities in a public company must file – to increase the price of a technology stock. According to the complaint in that case, Aly purchased out-of-the-money call options on the stock shortly before filing the Schedule 13D, which alleged that he and a group of Chinese citizens owned over 5% of the company and had written to the board of directors offering to buy the company at a 65% premium. The SEC also brought suit in November 2015 against Scottish trader James Alan Craig, who allegedly made false statements about two companies on Twitter accounts that he deceptively created to look like the real Twitter accounts of well-known securities research firms. These tweets, which claimed that two public companies were under investigation, caused significant drops in their share prices.

The SEC has also previously prosecuted individuals who allegedly hacked entities to obtain material nonpublic information. For example, in December 2016, the SEC charged and obtained a default judgment against three Chinese traders who conspired to hack two New York-based law firms to steal confidential M&A deal information to fuel fraudulent trading. The defendants allegedly installed malware on the law firms' networks and used the access gained to copy and transmit dozens of gigabytes of emails to remote internet locations. The traders used the nonpublic information in those emails to purchase shares in at least three public companies ahead of public announcements about entering into merger agreements.

Similarly, the SEC has prosecuted individuals who made intrusions into brokerage accounts. In June 2016, the SEC filed for and obtained an emergency court order to freeze the assets of Idris Dayo Mustapha. Mustapha, a UK resident, allegedly hacked into the online brokerage accounts of US customers of broker dealers. Mustapha

allegedly made unauthorized trades through these accounts in conjunction with trades through his own accounts – leading to profits of at least $68,000 for him while leaving losses of at least $289,000 for his victims.

Despite the fact that there have been related cases in the past, the creation of this new unit signals that these areas will be a specific focus in the future. This action was likely spurred, in part, by the SEC's recent revelation of its own data breach.

IMPLICATIONS FOR REGISTERED ENTITIES AND PUBLICLY TRADED COMPANIES

Registered investment advisers and broker-dealers are obligated to protect their customers from cyber threats by Regulation S-P, which requires that they adopt policies that are reasonably designed to safeguard customers' nonpublic personal information, protect that information against anticipated threats, and prevent unauthorized access and use of nonpublic material information that could result in significant harm to the customer.
cash flows.

Regulation S-P has already been used to bring two enforcement actions against registered entities that suffered data breaches. In 2015, the SEC settled an investigation with R.T. Jones Capital Equities Management, Inc., related to a hack that rendered the PII of more than 100,000 individuals vulnerable to theft. After *R.T. Jones,* the SEC subsequently brought another case in 2016 against a registered investment adviser and broker-dealer whose customer data was released as a result of a hack.

In addition, issuers should pay heed to recent public statements regarding the importance of adequate disclosure of cybersecurity risks and material events. While the SEC has yet to bring a disclosure-based cybersecurity enforcement action, the controversy surrounding the recent Equifax hack raises the likelihood of increased SEC enforcement activity in the coming months. In addition, the SEC could seek to establish books and records violations, supported by the SEC's statement in its cybersecurity guidance that breaches may require recognition of impaired assets and reductions in projected future earnings.

CONTACTS

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Benjamin Berringer
Associate

T +1 212 878 3372
E benjamin.berringer
@cliffordchance.com

Laurence Hull
Associate

T +1 202 912 5560
E laurence.hull
@cliffordchance.com

[i] https://www.sec.gov/news/testimony/testimony-clayton-2017-09-26
[ii] *Id.*