Cyber attack victims face one-two punch as SEC ramps up enforcement actions

By Daniel L. Stein, Esq., Michele Cerezo-Natal, Esq., and Maura K. McDevitt, Esq., Mayer Brown

OCTOBER 12, 2021

The Securities and Exchange Commission (SEC) established its Cyber Unit in 2017 to combat a variety of cyber-related misconduct, including market manipulation, unauthorized access to non-public information and financial accounts, threats to financial market infrastructure, and other misconduct.

In the SEC's Sept. 25, 2017, press release announcing the creation of its Cyber Unit, the SEC described cyber-related threats and misconduct as among the "greatest risks facing investors and the securities industry," and an area of "critical national importance." In recent years, the SEC has ramped up its enforcement actions related to violations connected to cybersecurity incidents, particularly in matters where customers' personally identifiable information (PII) has been compromised.

A series of actions over the last several weeks underscores the SEC's determination to bring enforcement actions against the financial firms that fall victim to cyber-fraud — not simply the bad actors who engage in cyber-related misconduct.

Recent SEC cyber unit cybersecurity enforcement actions

Safeguards Rule and client communications. The SEC's settlement with Cetera Advisor Networks LLC, Cetera Investment Services LLC, Cetera Financial Specialists LLC, Cetera Advisors LLC, and Cetera Investment Advisers LLC (the "Cetera Entities"), announced in August 2021, is particularly illustrative of the SEC's push to punish firms that failed to protect themselves (and their customers) from cyberattacks.

The SEC determined that the Cetera Entities violated the "Safeguards Rule" (17 C.F.R. § 248.30(a)), which requires all SEC registrants to adopt and implement written policies and procedures to protect customers' PII. From 2017 through 2019, the email accounts of more than 60 Cetera Entities' personnel were taken over by unauthorized parties through various methods of cyberattacks, including phishing attacks, which resulted in the exposure of customers' PII.

In recent years, the SEC has ramped up its enforcement actions related to violations connected to cybersecurity incidents, particularly in matters where customers' personally identifiable information (PII) has been compromised.

The SEC concluded that the Cetera Entities did not have reasonable policies and procedures in effect to prevent such unauthorized access to customers' PII. In particular, the SEC focused on the Cetera Entities' imperfect implementation of its written policies, including the inconsistent use of multifactor authentication (MFA) and failure to apply security measures to independent contractors with email addresses associated with the Cetera Entities.

SEC Cybersecurity Enforcement Actions 2017-2021 (as of October 4, 2021)
via https://www.sec.gov/spotlight/cybersecurity-enforcement-actions

Year	Digital Assets / Initial Coin Offerings	Account Intrusions	Hacking / Insider Trading	Market Manipulation / False Tweets / Fake Websites / Dark Web	Regulated Entities – Cybersecurity Controls and Safeguarding Customer Information	Public Company Disclosure and Controls	Trading Suspensions	Total
2017	5	1	0	1	0	0	7	14
2018	19	0	0	1	1	2	9	32
2019	17	0	1	0	2	0	1	21
2020	23	0	0	2	0	0	0	25
2021 (as of 10/4)	16	0	1	4	2	2	1	26

The SEC also charged Cetera Advisors LLC and Cetera Investment Advisers LLC with violations in connection with the data breach notices they issued to their customers. In light of the data breaches, Cetera Advisors LLC and Cetera Investment Advisers LLC issued notifications through their outside counsel that suggested the breaches were discovered recently, and that, therefore, the notifications were issued promptly after the discovery of the breach.

Failure to mitigate the risks of cyberattacks via widely available security tools is tantamount to an unreasonable risk in the eyes of the SEC — and a clear violation of the Safeguards Rule.

The SEC stated that those notices were "misleading" because the notifications were not delivered until over six months after discovery of the breach. Accordingly, the SEC concluded that the companies had violated 17 C.F.R. § 275.206(4)-7, which requires the implementation of reasonably designed policies and procedures to prevent the dissemination of misleading or inaccurate customer communications.

Failure to correct deficient procedures. The SEC has also doubled down on companies that fail to implement enhanced security measures after the discovery of initial lapses in security for customers' PII. For example, on Aug. 30, 2021, the SEC announced a settlement with Cambridge Investment Research, Inc. and Cambridge Investment Research Advisors, Inc. (the "Cambridge Entities") for violations of the Safeguards Rule arising out of unauthorized access to email accounts of independent contractors via phishing and other cyberattacks.

Beginning in 2018, various cyberattacks compromised cloud-based email accounts held by independent contractors affiliated with the Cambridge Entities, exposing the PII of certain customers. Although the Cambridge Entities alerted the affected customers to the exposure or potential exposure of their PII as a result of the cyberattacks, the Cambridge Entities did not take any further steps to secure customers' PII from cyberattacks and prevent exposure via enhanced security measures until 2021, years after the unauthorized access was first discovered. As a result, the SEC fined the Cambridge Entities $250,000 for failing to revise their procedures to address the deficiencies.

SEC guidance. The SEC has noted its concerns surrounding increased risks of cyber incidents as many companies moved to operate remotely during the pandemic. The SEC's Office of Compliance Inspections and Examinations (OCIE) issued guidance regarding the heightened cybersecurity risks present due to COVID-19. In its Aug. 20, 2020 risk alert, OCIE exhorted SEC registrants to, among other things,

- enhance identification and encryption technologies to protect customer communications and data, including across personally owned devices;
- conduct heightened reviews of personnel access rights and controls;
- enhance system access security, including requiring the usage of MFA where possible;
- address any cyber-related issues related to third-party access to company systems; and
- provide periodic training and reminders to personnel regarding cybersecurity issues, including phishing and other targeted cyberattacks, in order to protect customers' PII.

Conclusion

Given the dual-pronged risks associated with cyber-attacks — from both hackers and regulatory agencies — companies should closely review their cybersecurity compliance measures for vulnerabilities in both their systems and protocols. In light of the increasing prevalence of phishing attacks, and other cyber hacking attacks designed to collect PII, companies should be on high alert. Failure to mitigate the risks of cyberattacks via widely available security tools is tantamount to an unreasonable risk in the eyes of the SEC — and a clear violation of the Safeguards Rule.

Companies registered with the SEC should make every effort to design and implement effective policies and procedures to safeguard customers' PII, not only as part of their obligations to protect their customers, but also to stave off scrutiny from regulators. In the face of ongoing cyber threats, companies should strive to maintain the confidentiality, integrity, and availability of their systems and data through the implementation of written policies and procedures designed to integrate industry-standard security measures.

As the Cetera Entities' settlement agreement illustrates, companies must also ensure that these policies and procedures are applied uniformly to all affiliated parties, including independent contractors. Further, once a cybersecurity breach is detected, companies must ensure that impacted parties are notified promptly and adequately of the breach with specifically tailored communications, in compliance with statutory, regulatory, and contractual requirements, as well as internal written procedures and policies governing customer communications.

Marcus A. Christian, a partner with the firm, contributed to this article.

About the authors



Daniel L. Stein (L), a partner in **Mayer Brown**'s New York office, leads the firm's global Regulatory & Investigations group and is a co-leader of the White Collar Defense & Compliance group. A former federal prosecutor, he has extensive experience in regulatory enforcement, government and internal investigations, white collar criminal defense and complex civil litigation. He counsels clients in a range of complex issues, including U.S. Securities and Exchange Commission and Financial Industry Regulatory Authority investigations and enforcement actions. He can be reached at dstein@mayerbrown.com. **Michele Cerezo-Natal** (C) is counsel in the firm's New York office and a member of the Litigation & Dispute Resolution and White Collar Defense & Compliance practices. Her practice, which leverages her extensive in-house experience, focuses on global internal investigations and enforcement matters, responding to federal and state regulators and enforcement authorities and providing proactive compliance counseling. She can be reached at mnatal@mayerbrown.com. **Maura K. McDevitt** (R) is an associate in the firm's New York office and a member of the Litigation & Dispute Resolution group. Her practice focuses on complex commercial and financial services litigation and investigations. She can be reached at mmcdevitt@mayerbrown.com.

This article was first published on Reuters Legal News and Westlaw Today on October 12, 2021.