Investigations, Compliance, and Defense

Recent SEC Settlement Underscores Focus on Financial Institutions Facing Cyber Intrusions

By: Charles D. Riely, Sarah F. Weiss, Rachel C. Foster, and E.K. McWilliams

The SEC last week announced a settlement with a Colorado-based registered broker-dealer for allegedly failing to file Suspicious Activity Reports (SARs) and filing incomplete SARs on attempted cyber intrusions into its customers' electronic retirement accounts. The settlement is in the wake of the SEC's 2021 examination priorities and a March 2021 SEC risk alert emphasizing that broker-dealers must file complete SARs when bad actors attempt to gain access to customers' online accounts or electronically stored personal data. The SEC's order also follows guidance issued from the Financial Crimes Enforcement Network (FinCEN) to banks, casinos, broker-dealers, and other entities that are required to file SARs (Reporting Entities) emphasizing that FinCEN expects Reporting Entities to file complete SARs on all cyber-intrusions.[1]

This client alert examines the SEC's recent settlement with a broker-dealer for failing to file SARs—including for failure to file adequately detailed SARs—on cyber-intrusion events, summarizes recent guidance by the SEC and other federal regulators on SAR filings on cyber-intrusions, and discusses the key takeaways from the SEC's recent action and agency guidance on cyber-events.

The SEC's Settlement with Broker-Dealer for Failing to File SARs and Filing Incomplete SARs

The SEC faulted the broker-dealer for allegedly both failing to file SARs and omitting important information from the SARS it did file. According to the SEC's order, from September 2015 through October 2018, the broker-dealer, which services employer sponsored retirement plans, knew of at least 130 attempts by external bad actors to gain access to individuals' retirement accounts but failed to file SARs on these attempted or actual data intrusion incidents. The order provides that the broker-dealer "detected most of [the 130] attempts before the bad actors could request a distribution from a plan participant's account, but some incidents involved successful distributions." Like the SEC has done in at least one previous action, it also focused on information that was missing from SARs that were filed. In particular, the order notes that the filed SARs were deficient in the "five essential elements"—the "who, what, when, where, and why" of the suspicious activity being reported—and omitted other key facts, including cyber-related data such as URL addresses and IP addresses.

The Colorado broker-dealer agreed to pay a $1.5 million fine for its failure to file SARs and its filing of incomplete SARs. The SEC's order also notes that the broker-dealer undertook "significant remedial measures," including: implementing new SAR drafting procedures; retaining an outside AML consulting firm to review SAR processes; increasing both the size and experience of its AML compliance team; restructuring its SAR process to ensure greater accountability and quality control; implementing new SAR-related policies and procedures; and implementing a new case management system to better track unusual reports.

Recent Guidance from the SEC and Other Regulators on Filing SARs on Data Intrusions

The SEC's action follows recent efforts from the agency to emphasize the importance of filing appropriately detailed SARs on cyber-intrusion events. The SEC referenced safeguarding customer accounts against intrusions in its 2021 Examination Priorities. Additionally, on March 29, 2021, the SEC's Division of Examinations (EXAMS) released a risk alert reminding broker-dealers that they must

file SARs on cyber-intrusion events that include all details about the method and manner of the intrusion known at the time of reporting.

FinCEN also emphasized reporting such events in SARs in a 2016 Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime. The advisory reiterated that a financial institution must file a SAR if it "knows, suspects, or has any reason to suspect that a cyber-event was intended, in whole or in part, to conduct, facilitate, or affect a transaction or a series of transactions." The advisory said SARs must include available cyber-related information, including IP addresses with timestamps, virtual-wallet information, and device identifiers. FinCEN also provided an FAQ to help financial institutions determine whether and how to file a SAR after a cyber-event.

Finally, the Financial Industry Regulatory Authority (FINRA) has also announced that it will focus on broker-dealer filings of SARs related to cyber-intrusions this year. In an April 6, 2021 podcast, a FINRA senior vice president explained that there is an "intersection" between cyber-events and AML compliance and that the agency will "pay quite a bit of attention to" this area.

Key Takeaways

The SEC's recent settlement, as well as its 2021 examination priorities, and FinCEN's guidance on cyber intrusions, affirms that the filing of prompt and complete SARs on data intrusions is a vital part of broker-dealers' AML obligations. Indeed, broker-dealers who fail to file SARs on the heels of data intrusion events, including those that file SARs missing critical data about the method and means of the intrusion, may have exposure for failing to file SARs with a clear, complete, and concise disclosure of the nature of the suspicious activity.

The SEC's action also serves as a reminder to all entities that are obligated to file SARs that, when confronted with cyber intrusions, filing SARs is an important part of the required response. Like the SEC, FinCEN has stressed that Reporting Entities must disclose the "who, what, when, where, and why" of the event. For cyber intrusions in particular, FinCEN is looking for cyber-related data such as the method of the intrusion, URL addresses, IP addresses, and bank account information.

---

[1] The settlement was announced on the same day the Biden administration issued an Executive Order expanding the obligation of federal government and information technology (IT) and operational technology (OT) providers to report cyber breaches to designated government agencies. This indicates that the federal government is focused on collecting information related to cyber-threats and incidents from Reporting Entities, as well as from entities that contract with the government but are not obliged to file SARs.

Contact Us

Charles D. Riely

criely@jenner.com | Download V-Card

Sarah F. Weiss

sweiss@jenner.com | Download V-Card

Rachel C. Foster

rfoster@jenner.com | Download V-Card

E.K. McWilliams

emcwilliams@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

Anthony S. Barkow
Co-Chair
abarkow@jenner.com
Download V-Card

David Bitkower
Co-Chair
dbitkower@jenner.com
Download V-Card

Christine Braamskamp
Co-Chair
cbraamskamp@jenner.com
Download V-Card

Erin R. Schrantz
Co-Chair
eschrantz@jenner.com
Download V-Card

Andrew Weissmann
Co-Chair
aweissmann@jenner.com
Download V-Card