SEC Emphasizes the Need to File Suspicious Activity Reports in Response to Cyber Fraud

May 18, 2021 Tim Newman, Kit Addleman

PRACTICES Litigation, Privacy and Cybersecurity

Last week, the U.S. Securities and Exchange Commission charged a broker-dealer with failing to file Suspicious Activity Reports ("SARs") in accordance with the federal Bank Secrecy Act ("BSA"). While charges for failures to file SARs aren't new, this action was unique because the suspicious activity related to successful and attempted takeovers of retirement accounts by cybercriminals and other bad actors. The SEC's action is a reminder that cyber fraud is everywhere and can have far-reaching impacts on an organization's compliance obligations.

GWFS Equities, Inc. ("GWFS") is a registered broker-dealer that provides services to employer-sponsored retirement plans. According to the SEC's order, between 2015 and 2018, GWFS experienced an increase in attempted account takeovers, or instances in which bad actors attempted to gain unauthorized access to an account, often by leveraging improperly obtained personal information belonging to the account holders, similar to the experiences of other retirement plan service providers.

Securities Exchange Act Section 17(a) and Rule 17a-8 require broker-dealers to comply with the reporting requirements of the BSA. When account takeovers involve more than $5,000, a SAR must be filed, and those SARs must include "the five essential elements of information—**who? what? when? where? and why?**—of the suspicious activity being reported."[1] In 2011, the U.S. Treasury Department's Financial Crimes Enforcement Network ("FinCEN") issued an advisory alerting financial institutions to the increased risk of account takeovers and advising firms to "provide a detailed description of the activity" in the SARs they file in connection with account takeovers.[2] More recently, FinCEN has addressed the need to provide data such as IP addresses, timestamps, device identifiers, and methodologies used in SARs when suspicious activity relates to suspected cybercrime.[3]

In its order, the SEC alleged that GWFS violated its obligations to file SARs following attempted or successful account takeovers impacting retirement plan participants. Specifically, the SEC alleged that GWFS failed to file required SARs in approximately 130 instances. In one instance, GWFS allegedly discovered that a bad actor had fraudulently impersonated a plan participant, called GWFS's customer service center, authenticated the participant's personal identifying information, and requested a distribution. An investigation uncovered the bank accounts and phone number the bad actor used to perpetrate the attack, and they were used in at least two other account takeovers.

In another instance, a plan participant allegedly reported to GWFS that the participant had received a check he did not request. An internal investigation purportedly revealed that the participant's personal information had been changed, the participant's account had been accessed using an IP address that GWFS had identified in connection with another account takeover, and the bad actor planned to request and then intercept distribution checks as part of a fraudulent scheme. Eight

other plan participants with the same employer were targets of similar activity around the same time.

Approximately 130 such incidents were allegedly reported to GWFS's BSA officer, and in some instances, it was determined that SARs should be filed. However, GWFS allegedly failed to file the required SARs.

The SEC also alleged that when GWFS did file SARs following actual or attempted account takeovers, it failed to provide sufficient detail to satisfy the requirements of the BSA in nearly 300 instances. Specifically, the SEC alleged that GWFS filed generic reports of account takeovers with no additional detail, despite the fact that GWFS was often in possession of information identifying persons, phone numbers, bank accounts, email accounts, and IP addresses associated with the takeovers and identifying when and how the bad actors took control or attempted to take control of accounts. According to the SEC, this detail was provided to GWFS's BSA officer and its SAR committee, but GWFS failed to include this information in the SARs it filed.

The SEC acknowledged that in many cases GWFS detected account takeovers before any improper distributions occurred, and the Commission did not allege that the personal information used in attempted takeovers had been obtained through any breach of GWFS's systems. The SEC also recognized GWFS's cooperation with the SEC's investigation and the firm's extensive remediation of the alleged filing deficiencies. Among other things, GWFS added to its anti-money laundering team, retained an outside consultant to review and recommend enhancements to its SARs policies and procedures, and implemented a new case management system to track suspicious activity.

Nonetheless, the SEC alleged that GWFS's conduct violated the financial recordkeeping and reporting provisions of Section 17(a) of the Exchange Act and Rule 17a-8. The SEC ordered GWFS to cease and desist from any future violations, censured GWFS, and imposed a $1.5 million civil penalty. GWFS neither admitted nor denied the SEC's allegations in the order.

The SEC's order is a reminder that cybercrime is ever-increasing and ever-changing, and its effects can be felt not only in the direct losses that may result from a cyber-attack, but also in the impact it has on compliance policies and procedures. This order makes it clear that even when GWFS and others in the industry successfully thwart account takeovers, for example, they must still ensure they comply with reporting obligations under the BSA.

But it is not just broker-dealers that must focus on controls and reporting in response to cyber-crime. In a recent Section 21(a) report, the SEC's Division of Enforcement highlighted the risk faced by public companies that fall victim to business email compromises or related cyber scams; they may not only suffer the financial losses associated with those attacks but may also find themselves facing charges of internal accounting controls violations under Section 13(b)(2)(B) of the Securities Exchange Act of 1934. Organizations must remain vigilant and stay informed of the evolving nature of cybercrime and how it could affect their ongoing business and compliance practices.

---

[1] *See* FinCEN, *Guidance on Preparing a Complete & Sufficient Suspicious Activity Report Narrative* (Nov. 2003), at pg. 3, *available at* https://www.fincen.gov/sites/default/files/shared/sarnarrcompletguidfinal_112003.pdf.

[2] *See* FinCEN, *Account Takeover Activity*, FIN-2011-A016 (Dec. 19, 2011), *available at* https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2011-a016.

[3] *See* FinCEN, *Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime*, FIN-2016-A005 (Oct. 25, 2016), *available at* https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005.

The SEC's order involving GWFS Equities, Inc. is available here. If you have questions about how to combat cybercrime in your organization or how cybercrime may impact your organization's compliance policies and practices, contact one of the attorneys listed below.