Broker-Dealer Assessed $1.5 Million Penalty for Suspicious Activity Reporting Violations Relating to Cyber Intrusions

May 17, 2021

The Securities and Exchange Commission's recent case against a registered broker-dealer for not filing Suspicious Activity Reports (SARs) reinforces the SEC's focus on anti-money laundering (AML) and Bank Secrecy Act (BSA) compliance. The case also highlights the intersection of AML compliance and cybersecurity.

The Order

According to the SEC's **order**, over the course of three years, the broker-dealer was aware that bad actors attempted and, in some cases, successfully gained unauthorized access to the accounts of individual retirement plan participants. The broker-dealer was also aware that the bad actors improperly obtained certain personal identifying information of the plan participants, plus login information (i.e., user names, email addresses and passwords). The order cites the broker-dealer for not filing SARs for nearly 130 instances when it detected unauthorized account access. The order also finds that the broker-dealer failed to include all necessary details, such as URL and IP addresses, in 300 SARs that it filed.

The broker-dealer did not admit or deny the charges in agreeing to pay a $1.5 million penalty. In accepting the offer of settlement, the SEC said that it considered the broker-dealer's cooperation and significant remedial measures. These included new policies, procedures and training; retaining a consultant to enhance its SAR processes; increasing the size and experience of its AML team; restructuring its SAR process to ensure greater accountability and quality controls; and implementing a new case management system.

Background

The Financial Crimes Enforcement Network adopted the "**AML Program Rule**" and the "**SAR Rule**" to require broker-dealers to implement AML programs and suspicious activity monitoring and reporting. Securities Exchange Act Rule 17a-8 requires broker-dealers to comply with the reporting, recordkeeping and record retention requirements of the BSA, including those related to SARs. On March 29, 2021, the SEC's Division of Examinations (the **Staff**) issued a **Risk Alert** reminding broker-dealers of their obligations under AML rules and regulations, in particular requirements related to monitoring for and reporting of suspicious activity. The Risk Alert identified the Staff's key areas of concern, which include:

1. **Inadequate Policies and Procedures**. The Staff noted that some broker-dealers have not established adequate AML policies, procedures and internal controls to address the type of activity in which their customers regularly engage. Accordingly, broker-dealers should include appropriately tailored red flags in AML policies and procedures to assist with identifying activity for further due diligence.

2. **Failure to Respond to Suspicious Activity**. The Staff reminded broker-dealers to conduct and document adequate due diligence in response to red flags, especially with respect to activity in low-priced securities, consistent with firm policies and procedures and the red flags identified in prior guidance, such as the **2014 SEC examination risk alert** and **FINRA Notice to Members 19-18**.

3. **Filing Inaccurate or Incomplete SARs.** The Staff cautioned broker-dealers against filing SARs containing generic boilerplate language, which renders SARs less valuable to law enforcement and regulators. The Staff found that the use of boilerplate language led a number of broker-dealers to file SARs that contained inaccurate information or lacked sufficient detail to make clear the true nature of the suspicious activity.

Looking Forward

The case and the Risk Alert underscore the importance for broker-dealers to maintain reasonably designed AML compliance programs to protect against facilitating illicit activity, and to ensure full compliance with SAR reporting obligations when necessary. The case also highlights the prevalence of account intrusions in the securities industry, and the importance of implementing policies and procedures to protect customer information and detect instances of identity theft.[1]

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.

Greg D. Andres	+1 212 540 4724	greg.andres@davispolk.com
Robert A. Cohen	+1 202 962 7047	robert.cohen@davispolk.com
Tatiana R. Martins	+1 212-450-4085	tatiana.martins@davispolk.com
Paul J. Nathanson	+1 202-962-7055	paul.nathanson@davispolk.com
Gabriel D. Rosenberg	+1 212 450 4537	gabriel.rosenberg@davispolk.com
Daniel P. Stipano	+1 202 962 7012	dan.stipano@davispolk.com
Zachary J. Zweihorn	+1 202 962 7136	zachary.zweihorn@davispolk.com
Kendall Howell	+1 202 962 7068	kendall.howell@davispolk.com

[1] *See, e.g., In the Matter of Voya Financial Advisors, Inc.*, Exch. Act Rel. No. 90745 (Dec. 21, 2020) (settled action) (finding a violation of Section 206(2) of the Advisers Act, which prohibits an investment adviser, directly or indirectly, from engaging "in any transaction, practice, or course of business which operates as a fraud or deceit upon any client or prospective client."). *See also,* 17 C.F.R. 248.30 (requiring registered broker-dealers, investment companies, and investment advisers to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information"); 17 C.F.R. 248.201 (requiring regulated entities to adopt written policies and procedures to identify, detect and respond to identify theft).