The Investment Lawyer
Covering Legal and Regulatory Issues of Asset Management
VOL. 30, NO. 5 • MAY 2023

REGULATORY MONITOR

SEC Update

By Adam Aderton, Aliceson (Kristy) Littman, Marc J. Lederer, and Michael James

SEC's EXAMS Observations of Investment Advisers' and Broker-Dealers' Compliance with Red Flags Identity Theft Regulation S-ID

On December 5, 2022, the Securities and Exchange Commission (SEC) Division of Examinations published a Risk Alert providing observations from recent examinations of, and enforcement actions against, SEC-registered investment advisers and broker-dealers (together, firms) related to compliance with Regulation S-ID.[1] According to the SEC, the purpose of the Risk Alert is to assist firms with implementing effective policies and procedures under Regulation S-ID, which requires the development and implementation of an identity theft prevention program for firms that offer or maintain covered accounts.

Most Frequently Observed Regulation S-ID Compliance Issues

The Division of Examinations Staff (EXAMS) identified practices they deemed inconsistent with the objectives of Regulation S-ID. A number of common deficiencies identified by EXAMS are listed below.

Identification of Covered Accounts

Under Regulation S-ID, firms that meet the definition of "financial institution" or "creditor" (Covered Firms)[2] must determine and then periodically reassess whether they offer or maintain covered accounts.[3] Covered accounts typically include any retail accounts that allow multiple payments and transactions, or customer accounts for which there is a risk of identity theft.[4] Accordingly, Covered Firms must conduct a risk assessment to determine whether they offer or maintain covered accounts, taking into consideration the methods they provide for opening and accessing accounts, as well as their previous experiences with identity theft. EXAMS provided a number of observations related to the periodic identification of covered accounts from recent examinations.[5]

Failure to Identify Covered Accounts. EXAMS observed Covered Firms that failed to conduct an assessment of whether any of their accounts were covered accounts. As a result of this failure, EXAMS observed that some Covered Firms did not identify covered accounts at the firm and failed to implement a program as required under Regulation S-ID.

Failure to Identify New and Additional Covered Accounts. EXAMS observed that some Covered Firms did initially identify one category of covered accounts, but either failed to conduct periodic assessments or conducted periodic assessments that did not identify all categories or new types of covered accounts. EXAMS also observed examples of Covered Firms omitting online accounts, retirement

accounts, and other special purpose accounts from their determination and reassessment of covered accounts. Additionally observed were instances where Covered Firms did not maintain any documentation of their analysis of covered accounts. EXAMS noted that while not required by Regulation S-ID, such documentation can assist the firm in identifying the basis for its determination to auditors and regulators.

Failure to Conduct Risk Assessments. EXAMS observed that while some Covered Firms periodically identified covered accounts, the process did not include a risk assessment taking into consideration the methods provided to open, maintain, and close accounts, methods to access different types of covered accounts, or previous experiences with identity theft. In not periodically conducting a risk assessment of new methods to access accounts, some Covered Firms that historically maintained customer accounts at branch locations did not identify online accounts as covered under their programs. This impacted Covered Firms' abilities to develop controls for detecting and responding to red flags.

Establishment of the Program

Regulation S-ID requires Covered Firms to develop and implement a written program that is appropriate to the size and complexity of the firm and the nature and scope of its activities.[6] EXAMS observed the following issues with respect to the establishment of written programs.

Programs Not Tailored to the Business. EXAMS observed Covered Firms that established a generic program that was not tailored to or appropriate for their business model. Some of these Covered Firms relied on a template with fill-in-the-blanks that were not completed. Other Covered Firms adopted programs that simply restated the requirements of Regulation S-ID without including processes for complying with the regulation.

Program Did Not Cover all Elements of Regulation S-ID. Covered Firms represented to EXAMS that other policies and procedures outside of a written program constituted the firm's process for detecting, preventing, and mitigating identity theft, even though such procedures had not been incorporated into the program. In many cases, these procedures did not cover all of the required elements of Regulation S-ID.

Required Elements of the Program

Programs under Regulation S-ID must include reasonable policies and procedures to identify, detect, and respond to red flags that are relevant to identity theft. These programs must also include reasonable policies and procedures to ensure that they are updated periodically to reflect changes in risks to customers and to the safety of the Covered Firm from identity theft.[7]

Identification of Red Flags. Programs must include reasonable policies and procedures to identify relevant red flags for covered accounts offered by the firm and incorporate those red flags into the program. Red flags are patterns, practices, or specific activities that indicate potential identity theft. EXAMS observed Covered Firms that failed to identify red flags specific to their covered accounts, and instead listed examples from Regulation S-ID regardless of the flags' relevance to the firm's covered accounts. EXAMS also observed Covered Firms that only offered online accounts listing red flags related to the physical appearance of a customer. Some Covered Firms included red flags related to consumer reports even though those Covered Firms did not obtain consumer reports for customers. Other Covered Firms did not have a process or did not follow existing procedures to evaluate actual experiences with identity theft so that they could determine if additional red flags should be added to their programs. Some Covered Firms did not include any identified red flags in their program.

Detect and Respond to Red Flags. Programs must incorporate reasonable policies and procedures to detect and respond appropriately to any red flags that are detected. EXAMS observed Covered Firms that relied on preexisting policies and procedures to satisfy this requirement of the program, when such

procedures were not designed to detect and respond to identity theft red flags. EXAMS also observed Covered Firms that identified procedures for detecting and responding to specific red flags, when the actual procedures did not exist or failed to contain any relevant process related to the red flag.

Periodic Program Updates

Regulation S-ID requires that programs include reasonable policies and procedures to ensure the program is updated periodically to reflect changes in risks to customers and the firm from identity theft.[8] EXAMS observed Covered Firms that did not update their identified red flags after making significant changes to the ways in which their customers open and access their accounts, such as providing account access not only through local branch offices, but also through online customer portals. Additionally, EXAMS observed Covered Firms that had gone through business changes or reorganizations but had failed either to incorporate these new business lines into their existing program or to amend their programs for these new business lines.

Administration of the Program

Covered Firms must provide for the continued administration of the program through: (1) obtaining approval of the initial written program from either its board of directors, an appropriate committee of the board, or from a designated senior management employee if the firm does not have a board; (2) involving the board or senior management in the oversight and administration of the program; (3) training staff as necessary; and (4) exercising appropriate oversight of service provider arrangements.[9] EXAMS observed Covered Firms that did not appear to provide sufficient information to the board or designated senior management through periodic reports. These Covered Firms either failed to submit any reports, or submitted reports that did not appear to contain sufficient information for the board or senior management to evaluate the effectiveness of the program.

Inadequate Training. EXAMS observed Covered Firms that did not have robust processes to assess which employees should be trained, with some trainings appearing to be insufficient because the trainings were limited to a single sentence telling employees to be aware of identity theft.

Failure to Evaluate Controls of Service Providers. Some Covered Firms that relied on service providers to perform activities in connection with covered accounts did not evaluate the controls in place at the service provider to monitor for identity theft.

Conclusion

In light of the observations detailed in the Risk Alert and issues highlighted in recent Enforcement actions,[10] registered broker-dealers and investment advisers should be proactive in reviewing their policies and procedures relating to Regulation S-ID. In doing so, Covered Firms should pay particular attention to their procedures for identifying covered accounts and conducting periodic risk assessments of such accounts. Regulation S-ID requires Covered Firms to develop and implement a written program that is appropriate to the size and complexity of the firm.

In developing such a program, Covered Firms should ensure their programs are appropriately tailored to their business and cover all of the required elements of Regulation S-ID, such as identification, detection and responses to red flags. Merely restating the requirements of Regulation S-ID in a Covered Firm's policy and using generic language not relevant to its actual business may cause the SEC to question a Covered Firm's program. Covered Firms should also ensure that their programs provide for periodic updates to reflect changes in risk to customers and the firm. Finally, Covered Firms should review and update as necessary their processes for program evaluation, employee training and service provider oversight.

Mr. Aderton and **Ms. Littman** are partners at Willkie Farr & Gallagher LLP in Washington, DC. **Mr. Lederer** is a staff attorney at Willkie Farr & Gallagher LLP in New York, NY and **Mr. James** is an associate at Willkie Farr & Gallagher LLP in Washington, DC.

NOTES

1 *See* Risk Alert, Observations from Broker-Dealer and Investment Adviser Compliance Examinations Related to Prevention of Identity Theft Under Regulation S-ID, Securities Exchange Commission Division of Examinations (Dec. 5, 2022) (Risk Alert), available at *https://www.sec.gov/files/risk-alert-reg-s-id-120522.pdf*.

2 For a discussion on how a firm may be considered a "financial institution" or "creditor" under Regulation S-ID, please *see* Willkie Farr & Gallagher LLP, Client Memorandum: SEC and CFTC Adopt Identity Theft Red Flag Rules, available at *https://www.willkie.com/~/media/Files/Publications/2013/05/SEC%20and%20CFTC%20Adopt%20Identity%20Theft%20Red%20Flag%20Rules/Files/SECandCFTCAdoptIdentityTheft1pdf/FileAttachment/SEC_and_CFTC_Adopt_Identity_Theft1.pdf*.

3 *See id; see also* 17 CFR 248.201(c).

4 Covered account means: (i) an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a brokerage account with a broker-dealer or an account maintained by a mutual fund (or its agent) that permits wire transfers or other payments to third parties; and (ii) any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks. *See* 17 CFR 248.201(b)(3).

5 *See* Risk Alert at 2-3.

6 *See* Risk Alert at 3; *see also* 17 CFR 248.201(d)(1).

7 *See* Risk Alert at 4; *see also* 17 CFR 248.201(d)(2).

8 *See* Risk Alert at 6; *see also* 17 CFR 248.201(d)(2)(iv).

9 *See* 17 CFR 248.201(e).

10 *See* SEC Charges Firms for Deficiencies Relating to the Prevention of Customer Identity Theft, Securities and Exchange Commission (July 27, 2022), available at *https://www.sec.gov/news/press-release/2022-131*.