Lowenstein Sandler

Investment Management

December 13, 2022

SEC Releases Risk Alert Regarding Compliance Issues with Identity Theft Prevention Programs Under Regulation S-ID

By Scott H. Moss and Vincent R. Scala

On December 5, 2022, the Division of Examinations (EXAMS) of the Securities and Exchange Commission (SEC) issued a Risk Alert[1] regarding recently observed compliance issues with respect to Regulation S-ID.[2] Under Regulation S-ID, certain registered investment advisers, broker-dealers, and investment companies are required to develop and implement an identity theft prevention program. EXAMS noted four primary compliance issues related to identifying covered accounts, establishing an appropriate identity theft prevention program, implementing all required elements of a program, and administering a program.

Background

Regulation S-ID requires SEC-regulated entities that qualify as financial institutions or creditors under the Fair Credit Reporting Act to determine whether they offer or maintain covered accounts.[3] The Regulation applies to certain registered investment advisers, broker-dealers, and investment companies. For example, Regulation S-ID applies to qualifying entities that offer margin or custodial accounts, permit individuals to wire transfers to other parties, offer check writing privileges, or direct transfers or payments from individual accounts to third parties based on instructions from individuals or their agents. The Regulation typically applies to accounts that are primarily for personal, family, or household purposes. Qualifying entities must establish a written program to detect, prevent, and mitigate identity theft related to opening covered accounts and maintaining pre-existing covered accounts.

Compliance Issues

Through examinations of SEC-registered investment advisers and broker-dealers (collectively, Firms), EXAMS identified four primary compliance issues that may leave customers vulnerable to identity theft and financial loss.

1. Failing to Identify Covered Accounts

Regulation S-ID requires Firms to determine and periodically reassess whether they offer or maintain covered accounts. EXAMS found that some Firms failed to identify covered accounts, failed to identify new and additional covered accounts, and failed to conduct risk assessments. Since some Firms failed to perform an assessment of whether they have covered accounts, they failed to implement an identity theft prevention program in violation of Regulation S-ID. Although some Firms initially did identify covered accounts, they either failed to conduct any periodic assessments or they did conduct periodic assessments but did not properly identify all or new types of accounts. Such accounts included online accounts, retirement accounts, and other special purpose accounts. Further, EXAMS found that while some firms did perform periodic assessments, they failed to consider (a) the methods used to open, maintain, and close accounts, (b) the methods used to access

---

[1] The Risk Alert can be found here.
[2] *See* 17 CFR 248.201.
[3] Under 17 CFR 248.201(b)(3), a covered account is "(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; 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."

different types of covered accounts, and (c) previous experiences with identity theft.

2. Failing to Establish an Appropriate Identity Theft Program

Regulation S-ID requires Firms to develop and implement a program that is appropriate given their size, complexity, and activities. EXAMS found that some Firms failed to properly tailor their programs to their business model. For example, some Firms relied on fill-in-the-blank templates but failed to fully complete the forms. Meanwhile, other Firms merely restated the requirements of Regulation S-ID without including policies and procedures to comply with the Regulation. EXAMS also noted that some Firms failed to include all necessary policies and procedures in their written program. For example, EXAMS found that some Firms pointed to other policies and procedures used to detect, prevent, and mitigate identity theft that were outside of their written program, even though such policies and procedures were not incorporated directly or referenced in their written program.

3. Lacking Required Elements of an Identity Theft Program

Regulation S-ID requires programs to have reasonable policies and procedures (a) to identify, detect, and respond to red flags[4] that are relevant to identity theft and (b) to ensure there are periodic updates to adapt to changes in theft-related risks to customers, financial institutions, and creditors.

EXAMS found that some Firms failed to identify, detect, and respond to red flags. Notably, EXAMS found that some Firms either failed to list any red flags or failed to identify red flags that were specific to their covered accounts, and instead, merely listed examples from Regulation S-ID.[5] Moreover, EXAMS noted that some Firms only had red flags related to physically meeting with customers, despite only offering online accounts. As another example, EXAMS found that some Firms included red flags related to consumer reports, despite not obtaining consumer reports for their customers. EXAMS also noted that some Firms did not establish procedures, or did not follow existing procedures, to determine whether additional red flags should be added to their written programs. Additionally, EXAMS found that some Firms relied on pre-existing policies and procedures, such as anti-money laundering procedures, to meet the requirements of Regulation S-ID, despite not being designed to detect and respond to red flags for identity theft.

Moreover, EXAMS observed that some Firms failed to periodically update their program to address changes to theft-related risks. Notably, some Firms did not update their red flags, despite making significant changes to the method in which their customers open and access their accounts, such as now providing account access through online portals. Meanwhile, other Firms that underwent either a merger or an acquisition failed to incorporate new business lines into their existing program.

4. Improperly Administering an Identity Theft Program

Regulation S-ID requires Firms to continuously administer their program by (a) obtaining approval of the initial written program by the board or senior management if there is no board, (b) having board or senior management oversight, (c) adequately training staff as needed, and (d) properly overseeing service provider arrangements. EXAMS found that some Firms provided insufficient information to their board or senior management to evaluate the effectiveness of their program, offered inadequate training to staff, and did not evaluate the controls of service providers used to monitor identity theft.

Our Thoughts

Considering these recent findings, new and existing registered investment advisers, broker-dealers, and investment companies should make initial assessments to determine whether they offer covered accounts. If so, these entities must have a written program to detect, prevent, and mitigate identity theft in compliance with Regulation S-ID. If a program is already established, qualifying entities should ensure policies and procedures are tailored for their business model and to address specific red flags. Moreover, qualifying entities should continuously monitor their program for changes to their business model and changes to theft-related risks for customers, financial institutions, and creditors. At a minimum, entities should include these assessments as part of their annual review. This should not be a onetime event. Qualifying entities should also ensure board or senior management involvement, offer adequate training for staff, and assess the controls of service providers. Given that EXAMS recently identified these concerns, qualifying entities should act now to implement or

---

[4] Under 17 CFR 248.201(b)(10), a red flag means "a pattern, practice, or specific activity that indicates the possible existence of identity theft."
[5] *See Regulation S-ID, Appendix A, Supplement A.*

revise programs as needed, especially as part of any upcoming or ongoing reviews.

Regulation S-ID should also be considered in connection with Regulation S-P,[6] Regulation S-AM,[7] and similar state and non-US laws that simultaneously apply. Collectively, these rules and regulations provide a legal framework for safeguarding consumers. Regulation S-ID is merely one piece of a bigger puzzle that should be part of all annual or other periodic reviews.

Next Steps

Lowenstein Sandler will monitor additional Risk Alerts and provide further updates and analysis in future Client Alerts so qualifying entities can determine whether changes are required to their policies and procedures. Please contact one of the listed authors of this Client Alert or your regular Lowenstein Sandler contact if you have any questions regarding the Risk Alert.

---

[6] Regulation S-P mandates registered investment advisers, broker dealers, and investment companies to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information." *See* 17 C.F.R. 248.30.
[7] Regulation S-AM "regulates the use of consumer information received from an affiliate to make marketing solicitations." *See* 17 CFR § 248.101.

Contact

Please contact the listed attorneys for further information on the matters discussed herein.

SCOTT H. MOSS
Partner
Chair, Fund Regulatory & Compliance
T: 646.414.6874
smoss@lowenstein.com