RISK ALERT
DIVISION OF EXAMINATIONS

December 5, 2022

OBSERVATIONS FROM BROKER-DEALER AND INVESTMENT ADVISER COMPLIANCE EXAMINATIONS RELATED TO PREVENTION OF IDENTITY THEFT UNDER REGULATION S-ID[1]

I. Introduction

This Risk Alert provides observations from recent examinations of SEC-registered investment advisers ("advisers") and broker-dealers (together with advisers, "firms") related to compliance with Regulation S-ID.[2] The Division of Examinations ("EXAMS") is issuing this Risk Alert in order 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 ("Program") for firms that offer or maintain covered accounts.[3]

Regulation S-ID applies to SEC-regulated entities that qualify as financial institutions or creditors under the Fair Credit Reporting Act ("FCRA")[4] and requires SEC-regulated financial institutions and creditors to determine whether they offer or maintain covered accounts. SEC-regulated entities that are likely to qualify as financial institutions or creditors and maintain

1 The views expressed herein are those of the staff of the Division of Examinations, formerly known as the Office of Compliance Inspections and Examinations or OCIE (the "Division"). This Risk Alert is not a rule, regulation, or statement of the Securities and Exchange Commission (the "SEC" or the "Commission"). The Commission has neither approved nor disapproved the content of this Risk Alert. This Risk Alert has no legal force or effect: it does not alter or amend applicable law, and it creates no new or additional obligations for any person. This document was prepared by Division staff and is not legal advice.

2 Regulation S-ID is set forth at 17 CFR 248.201 et. seq. Identity Theft Red Flags Rule, Joint Final Rules and Guidelines, Securities Exchange Act Release No. 34-69359, Investment Advisers Act Release 3582, Investment Company Act Release 30456 (Apr. 10, 2013), 78 FR 23637 (April 19, 2013) ("Identity Theft Red Flags Rule"), available at: https://www.sec.gov/rules/final/2013/34-69359.pdf.

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. *See* 17 CFR 248.201(b)(3).

4 Fair Credit Reporting Act, 15 U.S.C. 1681.

covered accounts include most registered broker-dealers (e.g., broker-dealers offering margin or custodial accounts) and registered investment companies (e.g., registered investment companies that allow individuals to wire transfers to other parties or that offer check writing privileges),[5] and some registered investment advisers (e.g., registered investment advisers who can direct transfers or payments from individual accounts to third parties based on the individual's instructions or who act as agents on behalf of individuals) if the accounts are primarily for personal, family, or household purposes.[6] If a firm determines that it has such accounts, it must establish a Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

II. Most Frequently Observed Regulation S-ID Compliance Issues

Through its examinations, EXAMS staff identified practices that are inconsistent with the objectives of Regulation S-ID, which may leave retail customers vulnerable to identity theft and financial loss. Below are examples of the most common deficiencies identified by EXAMS staff in connection with the elements of Regulation S-ID.

A. Identification of Covered Accounts

Under Regulation S-ID, firms must determine and then periodically reassess whether they offer or maintain covered accounts.[7] Accordingly, 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. Below are examples of observations related to the periodic identification of covered accounts from recent examinations.

- ***Failure to identify covered accounts.*** EXAMS staff observed firms that failed to conduct an assessment of whether any of their accounts were "covered accounts" and as a result

---

5 Regulation S-ID applies to any investment company that is registered or required to be registered under the Investment Company Act of 1940, that has elected to be regulated as a business development company under that Act, or that operates as an employees' securities company under that Act, if such investment company otherwise meets the definition of financial institution or creditor and offers or maintains covered accounts.

6 *See* Identity Theft Red Flags Rule for additional examples of SEC-registered entities that may qualify as creditors or financial institution under FCRA. *See also* SEC Small Business Compliance Guide: Identity Theft Red Flags Rule, available at: https://www.sec.gov/info/smallbus/secg/identity-theft-red-flag-secg.htm.

7 17 CFR 248.201(c).

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.*** Some firms did initially identify, as covered accounts, one category of accounts that they offered, but they failed to conduct periodic assessments, either at all, or those periodic assessments did not identify all categories or new types of accounts that were "covered accounts." For example, firms may have merged with other entities but then never conducted a reassessment to see whether any new accounts should be included in the Program. EXAMS staff observed examples of firms omitting online accounts, retirement accounts, and other special purpose accounts from firms' determination and reassessment of covered accounts. EXAMS staff also observed instances where a firm did not maintain any documentation of their analysis of covered accounts. While not required by Regulation S-ID, such documentation can assist the firm in identifying the basis for their determination to auditors and regulators.
- ***Failure to conduct risk assessments.*** EXAMS staff also observed that while some firms periodically identified covered accounts, the process did not include a risk assessment taking into consideration the methods provided to open, maintain, and closed accounts; methods to access different types of covered accounts; or previous experiences with identity theft.[8] For example, in not periodically conducting a risk assessment of new methods to access accounts, some firms that historically maintained customer accounts at branch locations did not identify online accounts as covered under their Programs. This impacted firms' abilities to develop controls relevant to their red flags.

B. Establishment of the Program

Regulation S-ID requires 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.[9] Through recent examinations, EXAMS staff observed the following issues with respect to the establishment of written Programs.

---

8 *See* Identity Theft Red Flags Rule at 27 (stating that "each financial institution or creditor must periodically determine whether it offers or maintains covered accounts")..

9 17 CFR 248.201(d)(1).

- ***Programs not tailored to the business***. EXAMS staff observed firms that established a generic Program that was not tailored to or appropriate for their business model. In some cases, firms relied on a template with fill-in-the-blanks that had not been completed. Other firms adopted Programs that simply restated the requirements of the regulation without including processes for complying with the regulation.
- ***Program did not cover all required elements of Regulation S-ID***. Firms represented to staff 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 directly or by reference into the Program and in many cases did not cover all of the required elements of Regulation S-ID.

C. 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. Additionally, the Program must include reasonable policies and procedures to ensure that it is updated periodically to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.[10] EXAMS staff observed the following instances in which Programs lacked required elements.

***Identification of Red Flags*:** Red flags are patterns, practices, or specific activities that indicate the possible existence of identity theft.[11] 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. Supplement A to Regulation S-ID's Appendix A provides illustrative examples of red flags for a firm to consider. EXAMS staff observed firms that did not appear to have reasonable policies and procedures to identify relevant red flags. Specifically, EXAMS staff observed:

[10] 17 CFR 248.201(d)(2).

[11] 17 CFR 248.201(b)(10).

- Firms that failed to identify red flags specific to their covered accounts, and instead listed examples from Appendix A of Regulation S-ID regardless of the flags' relevance to the firm's covered accounts.
- Firms that only offered online accounts listed red flags related to the physical appearance of a customer; and some firms included red flags related to consumer reports even though those firms did not obtain consumer reports for customers.
- Firms that did not have a process or did not follow existing procedures to evaluate actual experiences with identity theft in order to determine if additional red flags should be added to their Programs. For example, EXAMS staff observed firms that experienced ongoing account takeovers over several years and did not consider any red flags related to account takeovers.
- Firms that did not include any identified red flags in their Program. For example, some firms created written Programs that had generic language for identifying, detecting and responding to, and updating red flags but the Programs did not include any actual red flags identified by the firms. As such, the written Programs were merely policy statements without any actionable procedures.

***Detect and Respond to Red Flags*:** Programs must have reasonable policies and procedures incorporated into the Program to detect and to respond appropriately to any red flags that are detected.[12] EXAMS staff observed firms that did not appear to have reasonable policies and procedures to detect and respond to relevant red flags. Specifically, EXAMS staff observed:

- Firms that relied on pre-existing policies and procedures (e.g., anti-money laundering procedures) to satisfy this requirement of its Program, when such procedures were not designed to detect and respond to identity theft red flags. For example, such procedures did not include processes to detect whether the fraud was related to identity theft, such as the use of forged or false credentials.
- 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 that

[12] 17 CFR 248.201(d)(2)(ii) and (iii).

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.[13] In recent examinations, EXAMS staff observed:

- Some firms 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.
- Firms that had gone through business changes or reorganizations, such as mergers or acquisitions of other financial firms, but had failed either to incorporate these new business lines into their existing Program or to approve a new Program for these new business lines.

D. Administration of the Program

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 of directors, 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.[14] EXAMS staff observed firms that did not provide for the continued administration of their Programs as required by Regulation S-ID. For example:

- ***Did not appear to provide sufficient information to the board or designated senior management.*** EXAMS staff observed firms that did not appear to provide sufficient information to the board or designated senior management through periodic reports, either by failing to submit any reports or by submitting reports that did not appear to

[13] 17 CFR 248.201(d)(2)(iv).

[14] 17 CFR 248.201(e).

contain sufficient information for the board or senior management to evaluate the effectiveness of the Program.

- ***Inadequate Training***. EXAMS staff observed firms that did not have robust processes to assess which employees should be trained, and some trainings appeared to be insufficient because the training was limited to a single sentence telling employees to be aware of identity theft.[15]
- ***Failure to evaluate controls of service providers***. Some 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.

III. Conclusion

In sharing these observations, EXAMS encourages registered broker-dealers and investment advisers to review their practices, policies, and procedures with respect to their Programs and to consider whether any improvements are necessary.

This Risk Alert is intended to highlight for firms risks and issues that the Division's staff has identified. In addition, this Risk Alert describes risks that firms may consider to (1) assess their supervisory, compliance, and/or other risk management systems related to these risks, and (2) make any changes, as may be appropriate, to address or strengthen such systems. Other risks besides those described in this Risk Alert may be appropriate to consider, and some issues discussed in this Risk Alert may not be relevant to a particular firm's business. The adequacy of supervisory, compliance and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.

[15] 17 CFR 248.201(e)(3) (requiring firms to train staff to effectively implement the Program).