Recent SEC EXAMS Risk Alert Highlights Key Considerations for Reg S-ID Compliance

December 15, 2022

On December 5, 2022, the Securities and Exchange Commission (the "SEC") Division of Examinations ("EXAMS") published a Risk Alert providing observations from recent examinations relating to investment adviser and broker-dealers' compliance with Regulation S-ID ("Reg S-ID"), also known as the Identity Theft Red Flags Rule (the "Red Flags Rule"). We previously wrote about the SEC's July 2022 charges against three financial institutions for violations of Rule 201 of Reg S-ID.

This week's Risk Alert underscores the SEC's continued focus on Reg S-ID compliance and view that registrants continue to demonstrate deficiencies in this area, and provides a useful roadmap for Reg S-ID compliance. EXAMS expects firms to establish and regularly update Reg S-ID policies and procedures that reflect the business model and particularized risks faced by each registrant and to engage in regular reevaluation of the Identity Theft Prevention Program (the "Program") in response to new and emerging identity theft risks.

MOST FREQUENTLY OBSERVED REG S-ID COMPLIANCE ISSUES

The Risk Alert covers the following three areas of Reg S-ID compliance where EXAMS identified deficiencies:

- Identification of covered accounts;
- Development and implementation of a written Program that meets all required elements; and
- Administration of a Program.

Identifying Covered Accounts

Firms have a continuing obligation to determine whether they offer accounts covered under Reg S-ID. EXAMS identified several areas where firms did not comply with their identification obligations:

- **Failure to identify covered accounts**. EXAMS observed some firms' failure to conduct required assessments to determine which, if any, accounts qualified as "covered accounts." Consequently, these firms failed to properly implement Programs.

- **Failure to identify new and additional covered accounts**. EXAMS observed that some firms initially identified covered accounts as one category of accounts that they offered. However, they ultimately failed to conduct periodic assessments—either at all or in a manner that sufficiently identified all categories of new accounts that were also "covered accounts." EXAMS observed that firms merging with other entities should conduct a reassessment to determine whether to include new accounts in the Program. Additionally, the determination and reassessment of covered accounts should include online accounts, retirement accounts and other special purpose accounts. EXAMS also underscored that firms should maintain documentation of their analysis of covered accounts and noted that while such documentation is not required by Reg S-ID, EXAMS can assist firms in identifying the basis for their determination to auditors and regulators.

- **Failure to conduct risk assessments**. Even where firms periodically identified covered accounts, firms sometimes failed to conduct a risk assessment in which they assess the methods for opening, maintaining, accessing and closing accounts, as well as the firm's prior experiences with identity theft. EXAMS flagged that the absence of risk assessments prevented some firms from identifying certain covered accounts, which limited firms' ability to develop controls relevant to their red flags. As required by Reg S-ID, firms should conduct such risk assessments periodically to determine whether they need to include additional accounts in the scope of "covered accounts" as a result of changes to account types or features. Such risk assessments should in turn identify particular red flags based on such changes.

Developing and Implementing a Written Program That Meets All Required Elements

Regulation S-ID requires that firms create a written Program appropriate for that specific firm that is based on the firm's size, activities and complexity of transactions. The Program must cover all required elements of the regulation, enumerating policies and procedures to identify, detect and respond to red flags of identity theft. The Program should include reasonable policies and procedures to ensure that it is updated regularly to be consistent with changes in the threat landscape in terms of risks to

customers and the safety and soundness of the registrant. EXAMS highlighted several issues related to Program implementation:

- **Failure to tailor a Program to the business**. Using a Reg S-ID template with fill-in-the-blanks is insufficient, as is restating the Regulation as the firm's policy. Firms must design a Program that is tailored to their particular business model.

- **Failure to identify red flags**. EXAMS found that firms lacked reasonable policies and procedures to spot red flags, which are patterns, practices or specific activities that indicate possible identity theft. Some firms did not include any specific identified red flags for their Programs, while other firms identified red flags that were not relevant to their business models. Firms should take care to assess relevant red flags for their covered accounts and add additional red flags to their Programs as appropriate (for example, identifying new identities or services being used for identity theft).

- **Failure to detect and respond to red flags**. Firms relied too heavily on preexisting policies and procedures, such as anti-money laundering procedures, which were not designed to combat identity theft. EXAMS found that firms either did not detect or did not adequately respond to instances of identity theft because they did not have policies and procedures tailored to relevant red flags. While a firm might maintain other policies related to identity theft prevention, firms should incorporate these procedures directly or by reference into their Programs—and to the extent that other policies and procedures are incorporated by reference into the Program, they should cover all of the required elements of Reg S-ID.

- **Failure to periodically update Programs**. The Regulation requires that firms update their Programs to reflect developments in the firm and identity theft risks. When undergoing business changes or reorganizations, firms should take care to make relevant Program changes or to approve a new Program for new lines of business.

Administering a Program

Firms are required to take four steps to provide for the continued administration of Reg S-ID. *First*, firms should obtain approval of their initial written Program from either an appropriate committee of the Board of Directors (or senior management if the firm lacks a Board). *Second*, the Board or senior management needs to be involved in administering the Program. *Third*, the appropriate staff should be trained on the Program. *Fourth*, the firm should conduct oversight of service provider arrangements for compliance. EXAMS noticed several areas where firms failed to meet these obligations:

- **Failure to provide sufficient information to the Board or senior management**. Some firms were not providing the Board or senior management with any reports or with insufficient reports. Reports should be sufficiently detailed to allow the Board or senior management to evaluate the effectiveness of the Program.

- **Failure to provide adequate training**. Firms sometimes failed to assess which employees need training on identity theft prevention and/or provided insufficient training. Firms should conduct comprehensive training as well as periodically determine which employees should be trained.

- **Failure to evaluate controls of service providers**. When a firm relies on an outside service provider to perform activities related to covered accounts, that outside service provider should also have adequate identity theft prevention controls. EXAMS underscored that firms should evaluate the identity theft controls in place at third-party service providers.

You can find our previous coverage of SEC enforcement actions in data- and cybersecurity-related matters (here, here, here, here, and here).

To subscribe to the Data Blog, please click here.

The authors would like to thank Debevoise Law Clerk Charlotte Blatt for her work on this Debevoise Data Blog post.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Avi Gesser
agesser@debevoise.com

Erez Liebermann
eliebermann@debevoise.com

Charu A. Chandrasekhar
cchandrasekhar@debevoise.com

Michael R. Roberts
mrroberts@debevoise.com

Noah L. Schwartz
nlschwartz@debevoise.com

SAN FRANCISCO

Kristin A. Snyder
kasnyder@debevoise.com