# Recent SEC Enforcement Actions Signal Key Lessons for Reg S-ID Compliance

**August 3, 2022**

On July 27, 2022, the Securities and Exchange Commission ("SEC") separately charged three financial institutions with violations of Rule 201 of Regulation S-ID ("Reg S-ID"), also known as the Identity Theft Red Flags Rule ("Red Flags Rule"). The announcement of multiple Reg S-ID enforcement settlements (all of which were investigated by the SEC's recently-expanded Crypto Assets and Cyber Unit and originated from referrals from the Division of Examinations) highlights the SEC's agency-wide focus on Reg S-ID compliance. Notably, these are the first Reg S-ID cases the SEC has brought since 2018, when the Commission brought its first-ever Reg S-ID action.

The SEC's orders detail numerous deficiencies in each firm's Identity Theft Prevention Program ("ITPP"), provide registrants with an outline of the Commission's expectations for compliance with Reg S-ID, and underscore the Commission's increasing scrutiny of cybersecurity deficiencies in the securities marketplace.

The orders establish that registrants must craft ITPPs that are particularized to each individual firm and updated to cover new risks. Given the evolving identity theft threat landscape, firms should consider building cross-functional teams drawing resources from the business, compliance, legal, privacy, and cyber areas to address these cybersecurity risks.

## Overview of Reg S-ID's Requirements

Rule 201 of Reg S-ID requires financial institutions and creditors to periodically determine whether they offer or maintain "covered accounts," which are defined as (i) accounts that are offered or maintained primarily for personal, family, or household purposes and involve or are designed to permit multiple payments or transactions, and (ii) any other account for which there is a reasonably foreseeable risk of identity theft.

A financial institution or creditor that offers or maintains covered accounts must develop and implement a written identity theft prevention program. The program must:

- Be designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account;
- Be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities;
- Include reasonable policies and procedures to identify red flags for covered accounts, incorporate those red flags into the program, detect red flags that have been incorporated, and respond appropriately to any red flags that are detected; and
- Include reasonable policies and procedures to ensure the program and any red flags determined to be relevant are updated periodically to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

The financial institution or creditor must also:

- Provide for the continued administration of the program;
- Obtain approval of the initial written program from its board of directors (or an appropriate committee thereof);
- Involve the board (or an appropriate committee of the board or designee from senior management) in the oversight, development, implementation, and administration of the program;
- Train staff, as necessary, to effectively implement the identity theft prevention program; and
- Exercise appropriate and effective oversight of service provider arrangements.

Appendix A to Reg S-ID contains criteria that each financial institution or creditor should consider including in its program, as appropriate, such as categories and examples of red flags, factors to consider in updating a program, and guidelines for oversight of service providers.

## The July 27, 2022 Orders

The three July 27, 2022 orders stem from similar findings by the SEC. Two of the charged firms are global financial services institutions with dually-registered broker-

dealers and investment advisers. The third is a broker-dealer that offers online brokerage services to retail customers.

The orders relate to violations between 2017 and 2019. None of the orders detail any actual loss or identity theft to customers attributable to the violations. Instead, the orders find that each company failed to maintain an adequate program, as required by the regulations. Without admitting or denying the SEC's findings, the firms agreed to cease and desist from future violations; censures; and to pay penalties ranging from $425,000 to $1.2 million. The settlements are also notable because they originated in referrals from the Division of Examinations to the Division of Enforcement, illustrating that cybersecurity remains a priority across the entire Commission.

## SEC's Focus on Reg S-ID and Cybersecurity Enforcement

The SEC settlements noted that although all three companies had ITPPs, they failed to tailor their programs to their respective businesses and to update the programs in a timely manner. Consequently, each firm, according the SEC, failed to satisfy several requirements of Reg S-ID.

All three charged firms had programs that the SEC views as failing to include reasonable policies and procedures to (1) identify, incorporate, detect, and respond appropriately to red flags, and (2) ensure their programs were updated periodically to reflect changing risks. The SEC faulted the firms' respective ITPPs for simply restating the general legal requirements of Reg S-ID without providing particularized guidance for identifying, detecting, and responding to red flags, which was tailored to the firms' specific business models. The SEC also found failures in: the oversight of service providers; training of staff to implement ITPPs; reporting to the board of directors (when the board was charged with supervising the ITPP); the periodic review of new or existing types of customer accounts to ascertain whether they were "covered accounts"; and ITPP updates to reflect emerging cybersecurity risks.

The July 2022 actions mark only the second time that the SEC has brought charges for violating Reg S-ID. In September 2018, the SEC charged a dually registered broker-dealer and investment adviser with violating Reg S-ID and the Safeguards Rule of Regulation S-P in connection with a cyber intrusion that compromised customers' personal information. Similar to the July 2022 Reg S-ID settlements, the SEC found that the firm did not review and update its ITPP in response to changes in risks, did not provide adequate training to staff, did not ensure adequate board oversight of the program, and did not have reasonable policies and procedures to respond to red flags. However, it is noteworthy that in the 2018 matter, there was an underlying identity

theft that highlighted the deficiencies to the SEC, whereas in the present matters, no instances of identity theft were discussed in the orders—demonstrating that the Commission will not hesitate to charge cybersecurity violations, even in the absence of actual harm to investors.

## Key Takeaways from SEC Enforcement for Reg S-ID Compliance

The trio of Reg S-ID settlements underscores that SEC registrants should regularly review their written ITPPs for compliance with Reg S-ID. Important considerations include:

- **Identifying and Incorporating Red Flags in the ITPP Tailored to Each Firm's Risks:** Firms should re-examine their ITPPs to ensure they contain reasonable policies and procedures to identify and incorporate particularized red flags relevant to their institutions or their own experiences with identity theft risks. For example, although Appendix A to Reg S-ID contains a lengthy list of potential identity theft red flags, a firm should not unthinkingly adopt this list wholesale, but could instead identify and incorporate only those red flags that the firm considers relevant to its business model. Additionally, where a firm does not obtain and review consumer reports in connection with opening covered accounts, its ITPP should not reference red flags related to information received from consumer reporting agencies. On the other hand, where a firm encounters specific forms of social engineering or account-takeover fraud, the policies could be updated to reflect and address those risks. In turn, in determining relevant categories of red flags, a firm should look to factors applicable to its own business, such as the types of covered accounts it offers or maintains, methods to open and access accounts, and prior experiences with identity theft.

- **Detecting and Responding to Red Flags:** Firms should consider whether their ITPPs contain reasonable policies and procedures to detect and respond appropriately to red flags. For example, potentially appropriate responses to red flags include declining to open a new account and notifying law enforcement. Firms should consider providing specific steps for employees to undertake in addressing red flags.

- **Periodic Updates Based on Changing Risks:** Firms should consider whether their ITPPs contain reasonable policies and procedures to ensure periodic updates to reflect changing risks. The SEC settlements emphasized the "significant changes in external cybersecurity risks related to identity theft" in recent years. Firms that have not regularly made material changes to ITPPs to reflect the emerging cybersecurity

risk landscape should consider assessing evolving identity theft-related risks and updating their programs accordingly. Further, if a firm's ITPP states that the firm will review and update it periodically, the policy could also describe the frequency of review and the mechanics of policy updates.

- **Evaluating "Covered Accounts":** Firms should consider developing, maintaining, and implementing policies and procedures for determining whether they maintain or offer "covered accounts" and for identifying new types of covered accounts offered. The SEC settlements suggest that firms should identity red flags based on the types of covered accounts that the firm specifically offers or maintains, and should conduct risk assessments or other evaluations to determine the types of accounts it offers or maintains.

- **Cross-Functional Compliance:** The process of creating and updating an ITPP in order to meet the particularized risks of a firm benefits from input from a cross-functional team of stakeholders. For example: customer service representatives can share the experiences they have with customers (and fraudsters); cybersecurity teams can identify new methods of account takeover fraud; privacy teams can share experiences from breach notifications; and the law and compliance teams can bring together updates. A cross-functional team can help facilitate ongoing compliance, particularly at global financial institutions where relevant responsibilities and duties may be shared across multiple groups.

- **Board Involvement:** ITPPs should address involvement from the board of directors (or a committee thereof or a designee from senior management, as appropriate). Specifically, the firm should consider providing the board with reports specific to the program and compliance with Reg S-ID. Such reports could include sufficient information about the program's effectiveness, significant identity theft-related incidents and management's responses, and metrics related to identity theft at the firm. Moreover, the firm should consider documenting any board-level discussions about compliance with Reg S-ID.

- **Staff Training:** Firms should consider providing training to staff on effective implementation of the ITPP, including training on identifying, detecting, monitoring, and responding to red flags.

- **Oversight of Service Providers:** Firms should consider evaluating whether they exercise appropriate and effective oversight of service providers, including whether their activities comply with reasonable policies and procedures to detect, prevent, and mitigate identity theft.

Finally, even if a firm takes actions to respond to actual incidents of identity theft, its written ITPP should include those actions in its policies and procedures. And importantly, where a firm has reasonable policies and procedures in place, it should make sure to follow them.

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 Lily Coad for her work on this Debevoise Data Blog.*

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
cachandrasekhar@debevoise.com

Noah L. Schwartz
nlschwartz@debevoise.com

Michael R. Roberts
mrroberts@debevoise.com

**SAN FRANCISCO**

Kristin A. Snyder
kasnyder@debevoise.com