CARLTON FIELDS

Regulation S-ID: Financial Institutions Take Note

October 07, 2022

The SEC enacted "Regulation S-ID: Identity Theft Red Flags Rules" in 2013. The regulation's purpose is to help protect investors from theft, loss, and abuse of their personal information. Broker-dealers, investment advisers, investment companies, and other financial institutions, big and small, must develop and implement an identity theft prevention program appropriately tailored to their businesses and update the program in response to the increased threat and changing nature of identity theft. Regulation S-ID also covers creditors, as defined by the Fair Credit Reporting Act.

The SEC brought its first Regulation S-ID enforcement action in 2018. FINRA followed with its first enforcement action in December 2020. Although the two regulators tasked with enforcing the regulation brought only one enforcement action each between 2018 and 2020, enforcement in this area is quickly heating up. In July 2022, the SEC announced charges against three financial institutions for deficiencies in their programs designed to prevent identity theft. The most recent actions brought by the SEC indicate that enforcement of the regulation has become a much higher priority for the SEC. This article will discuss: (1) what Regulation S-ID requires; (2) where financial institutions have faced problems; and (3) how financial institutions can mitigate risk.

What Does Regulation S-ID Require?

Regulation S-ID requires financial institutions that offer or maintain one or more covered accounts to develop and implement a written 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. The program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities. Regulation S-ID is proscriptive in its requirements; however, developing and implementing a system that is "appropriately tailored" raises many questions, leaving regulated entities without clear guidance.

Regulation S-ID has a specific definition of a covered account. Simply put, this means all accounts at a financial institution or creditor where multiple transactions, payments, and wires to and from third parties take place. Covered accounts also are any other accounts that a financial institution or

creditor maintains where there is a reasonably foreseeable risk of identity theft, including other operational risks. Essentially, Regulation S-ID applies to any financial institution or creditor with customer accounts, such as brokerage accounts and accounts maintained by a mutual fund.

Regulation S-ID requires that each program include reasonable policies and procedures to: identify relevant red flags for the covered accounts, and incorporate those red flags into the program; detect red flags that have been incorporated into the program; respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and ensure the program (including the red flags determined to be relevant) is updated periodically to reflect changes in risks to customers and to the safety and soundness of the financial institution.

Importantly, each financial institution must provide for the continued administration of the program and must: obtain approval of the initial written program from either its board of directors or an appropriate committee of the board; involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation, and administration of the program; train staff, as necessary, to effectively implement the program; and exercise appropriate and effective oversight of service provider arrangements.

Where Financial Institutions Have Faced Problems

With the proscriptive nature of Regulation S-ID, where have financial institutions faced problems? As referenced above, the SEC brought the first Regulation S-ID enforcement action in 2018 against a financial institution where, over a six-day period in 2016, intruders posed as independent contractor representatives when calling the financial institution's technical support line to request a password reset for three registered representatives. According to SEC releases, in two instances, the fraudulent requests came from phone numbers the financial institution had previously identified as associated with fraudulent activity. The prior activity also involved attempts to impersonate the financial institution's independent contractor representatives. During these attempts, the technical support staff reset the independent contractor representatives' passwords and provided the individuals posing as "representatives" with temporary passwords over the phone. In two of those prior instances, technical support also provided the usernames. Three hours after the first fraudulent request, one of the three registered representatives targeted by intruders notified technical support that he had received an email notifying him of the password change but had not initiated a request to change his password.

Although the financial institution took certain steps to respond to the intrusion, according to the SEC those steps did not prevent two additional account intrusions using the same technique over the next several days. Further, the financial institution did not immediately terminate the intruders' access to the three registered representatives' accounts. As a result, the intruders gained access to

the personally identifiable information (PII) of at least 5,600 customers and subsequently obtained account documents containing PII for at least one customer. The intruders also used customer information to create new online profiles, which gave them access to two additional customers' account information and PII. The SEC ultimately fined the financial institution $1 million.

Two years after the SEC's action, FINRA brought an enforcement action against a financial institution for violating Regulation S-ID and FINRA Rule 2010. There, FINRA alleged that the financial institution's program failed to include reasonable policies and procedures to identify or detect red flags of identity theft and that its procedures for responding were not tailored to its business. For example, the program provided that the financial institution's legal department would take an active role in investigating incidents of suspected identity theft, but the financial institution did not have a legal department. More fundamentally, the program did not address the identification and detection of red flags of identity theft and did not provide any guidance regarding steps to take in the event of an incident. The deficiencies in the financial institution's program were spotlighted when its systems were breached.

According to FINRA releases, beginning in April 2018, the financial institution's dual CEO and CCO began receiving hundreds of notifications in his financial institution email inbox that messages sent from his account could not be delivered to an external email address. Despite not recognizing the external email address, the CEO and CCO ignored the undeliverable notifications for approximately four months, at which time he contacted the email vendor that informed him that an automated rule was established that blind-copied all emails he received to the unknown external email address. Due to the financial institution's alleged inaction, approximately 17,000 emails were blind-copied to the unauthorized external email. Perhaps most troubling, from FINRA's perspective, was that the financial institution made no effort to notify any of the customers affected by the breach as of the date of the FINRA Acceptance, Waiver, and Consent, which occurred more than two years after the breach. FINRA censured the financial institution, fined it $65,000, and imposed a number of undertakings.

Most recently, the SEC announced an enforcement action it took against three major financial institutions. Unlike the previous actions brought by the SEC and FINRA, both of which had actual breaches into their systems on which the enforcement actions were predicated, the SEC's latest tranche of cases involved deficient policies and procedures, with no identified, underlying harm. Nevertheless, the SEC fined the financial institutions $1.2 million, $925,000, and $425,000, respectively.

Although the SEC's orders against the three financial institutions were somewhat similar, each financial institution's conduct revealed the various land mines financial institutions can find themselves confronting when thinking about their own programs. For example, the SEC accused one financial institution of failing to incorporate policies and procedures that described how identity

theft red flags were to be identified or responded to once they were detected. According to the SEC, the financial institution also did not incorporate reasonable policies or procedures to ensure that the program was updated periodically and did not provide training to staff to implement the program.

Against the second financial institution, the SEC found that the financial institution made no material changes to its program after Regulation S-ID went into effect, instead relying on its 2008 identity theft red flags program. Despite the ever-changing landscape of cybersecurity risks related to identity theft, the financial institution did not update its program to incorporate new red flags or procedures for detection and response. According to the SEC, the financial institution did not provide enough details to its board of directors for it to be sufficiently involved in the oversight, development, and implementation of its program. This financial institution also did not provide identity theft red flag training to its staff.

Last, the SEC found that the third financial institution did not consider factors applicable to it to identify relevant red flags tailored to its particular business. For example, the financial institution's program provided that it would be a red flag if the photograph or physical description of a client was inconsistent with the client's appearance; however, nearly all of the financial institution's accounts were opened online, preventing the financial institution from comparing physical appearance to the identification presented. The SEC also found the financial institution did not have reasonable policies and procedures for when an employee identified a red flag beyond directing the employee to conduct additional due diligence. Like the two other financial institutions, this one also did not have policies or procedures for periodic updates to its program.

How to Mitigate Risk

As explained above, the SEC has now taken actions against financial institutions that did not suffer actual intrusions but merely had, in the SEC's view, deficient policies and procedures in the absence of a specific customer loss. As such, the risk of enforcement is much higher than in the past few years, and it would be prudent for all financial institutions to evaluate and, if necessary, update their existing programs. There are a number of ways financial institutions can mitigate risk for their customers and, accordingly, reduce their risk of an examination finding or enforcement matter:

- **Maintain current policies and procedures that are tailored to the financial institution**. For example, if a financial institution does not accept physical stock certificates, then it may not need to address red flags associated with stock certificates in the program. The financial institution also should review the policies and procedures annually to ensure that no updates are needed or update as necessary. Financial institutions also should document who conducted the annual reviews, even if they chose not to make updates.

- **Refer to Appendix A of Regulation S-ID – Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation**. This appendix provides non-exhaustive guidelines intended to assist financial institutions in developing and implementing a reasonable program. But as with the first tip, make sure the guidelines selected are appropriate to the financial institution. For instance, Appendix A provides a category of red flags related to suspicious documents. If the financial institution opens all accounts online and does not intake physical documents, then this portion should be omitted.
- **Review and, as needed, update the program anytime the financial institution suffers a breach** to incorporate policies and procedures that will prevent, detect, and mitigate that same breach to decrease the likelihood that it would happen again.
- **Learn from other data breaches**. If the financial institution becomes aware of another major breach in the industry, it should ensure that its program is prepared to confront such a breach.
- **Involve the board of directors in developing and maintaining the program**, leveraging the members' individual experience and expertise, and include a summary of the discussion in the meeting minutes.
- **Regularly train employees on identity theft red flags**. Every employee who handles accounts or data should receive periodic training on identifying and escalating red flags of identity theft. In addition to periodic training, if a breach occurs that causes the financial institution to update its policies and procedures to prevent, detect, and respond to that breach, the financial institution should provide timely training on those updates.
- **Make and preserve reasonable documentation of program reviews**. Financial institutions should document each review of their program, regardless of whether changes were made. Financial institutions will have a much easier time defending an imperfect program if they can demonstrate to regulators, with written evidence, that they gave thoughtful and timely consideration to it.
- **Be proactive**. If the financial institution does not have a reasonable program that is consistent with the requirements of Regulation S-ID, fix it. The key here is to fix the program before a regulatory inquiry. Then, even if a regulator asks about an earlier time period, financial institutions can acknowledge that their program was not perfect but that they have since updated it to ensure compliance. This is a much more effective strategy than waiting until a regulator inquires about the program to fix it, at which point the financial institution would have to scramble to mitigate the damage.

Authored By

Tino M. Lisella

Related Practices

Securities Litigation and Enforcement
Cybersecurity and Privacy
Financial Services Regulatory
Digital and E-Commerce Engagement and Innovation

Related Industries

Securities & Investment Companies