Evaluating Identity Theft Red Flags Programs and Compliance with Regulation S-ID

MAKING AN IMPACT THAT MATTERS since 1845

Securities and Exchange Commission's (SEC) renewed focus on Identity Theft Red Flags Programs

On December 5, 2022, the staff of the Securities Exchange Commission ("SEC") issued a Risk Alert highlighting observations and compliance issues during recent examinations related to Prevention of Identity Theft under Regulation S-ID ("Reg S-ID"). As a result of these examinations, firms were fined a collective total of $2.5 million for failure to adopt and implement a reasonably designed identity theft prevention and red flags program ("Program"). In another instance, the CEO was fined personally and required to undertake expedited enhancements to the related financial institution's Program and its interrelated cybersecurity functions.

Many of the observations outlined in recent SEC enforcement actions and the Risk Alert were attributed to firms' inability to develop and implement a Program that's consistent with the objectives of Reg S-ID. If left unaddressed, the SEC believes that these compliance issues could leave retail investors increasingly vulnerable to threats of identity theft and financial loss.

To underscore this point, the SEC staff highlighted the following commonly identified Reg S-ID program weaknesses:

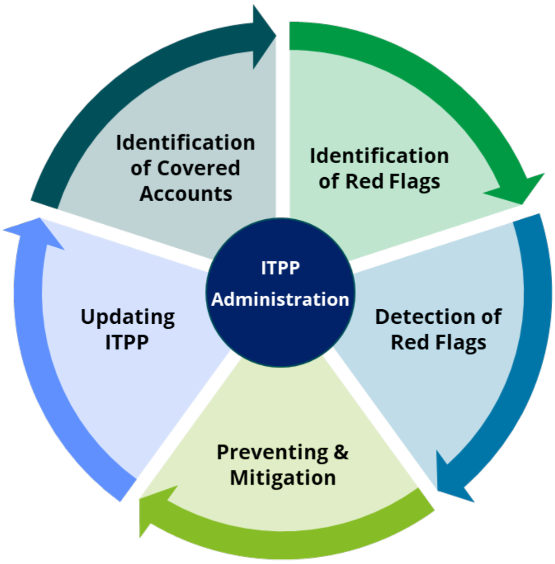
1. **Covered accounts not properly identified:** SEC staff observed that firms failed to: (1) identify if they offer and maintain covered accounts as defined by Reg S-ID; (2) periodically assess and identify if new covered accounts were being offered to customers; and (3) conduct risk assessments to evaluate how the methods provided to open, access, maintain and close accounts exposed the firm to additional identity theft risk.
2. **Programs not tailored to business activity:** SEC staff observed that: (1) programs were not tailored to the size and complexity of a firm's business activities; and (2) Program did not cover all of the required elements of Reg S-ID.
3. **Lack of procedures to identify, detect, and respond to Red Flags:** SEC staff observed that firms failed to include reasonable policies and procedures to identify, detect, and respond to relevant red flags for covered accounts, specifically firms:
    - Failed to identify red flags specific to their covered accounts;
    - Listed red flags which did not apply to their firm;
    - Did not have a process or did not follow existing procedures to evaluate actual experiences with identity theft;
    - Did not include any self-identified red flags in their Program;
    - Relied on pre-existing policies and procedures to satisfy this requirement of its Program, despite those policies and / or procedures not being designed with the intention of detecting and identifying red flags; and
    - Failed to include reasonable policies and procedures to reasonably ensure the Program is updated periodically to reflect any material changes to firm's business (i.e., new red flags, mergers or acquisitions, new products, features, and methods to onboard customers).
4. **Lack of program administration:** The SEC staff identified that firms failed to establish an adequately design administration process for their Program, which included the following: (1) firms did not appear to

provide sufficient information to the board or designated senior management through periodic reports; (2) firms did not have robust processes in place to assess which employees need to be trained, as well as firm training often falling short of SEC expectations; and (3) firms failed to evaluate controls of third-party service providers, including reviewing service provider controls.

The recent enforcement actions and Risk Alert underscore the SEC's commitment to ensuring the prevention of identity theft and demonstrating the SEC staff is diligently examining firms to determine if Programs are reasonably designed to achieve compliance with Reg S-ID. Given the regulatory guidance and enforcement focus within Reg S-ID, information security professionals and compliance officers should assess the design and operational effectiveness of their firm's Program. The following sections serve as a framework to assist firms in evaluating and assessing their Programs based on our understanding of industry leading practices and regulatory expectations.

Overview of the Reg S-ID Assessment Framework

Given the increased regulatory prioritization and scrutiny, it is imperative that each firm evaluate whether its Program meets regulatory expectations and industry best practices based on its business model and structure. When evaluating the Program, a firm should consider its size and complexity and evaluate the Program based upon the size, scope, and nature of its activities. Additionally, firms should assess whether the Program includes reasonable policies and procedures to: (1) identify red flags and covered accounts; (2) detect red flags that have been identified as relevant to the firm's covered accounts; (3) respond appropriately to those detected red flags; and; (4) validate the Program is periodically updated to reflect changes to the risks to customers and safety and soundness of the financial institution. This often requires a firm to integrate various aspects of its existing risk and control framework into its Program policies and vice versa; thereby, creating a Program designed to protect both customers and the firm from identity theft. Lastly, firms should reasonably ensure that these processes have clear escalation channels to senior leadership and that the Program and red flags are routinely evaluated based on identity theft incidents at the firm.



Below is a list of focus areas and high-level questions that a firm should consider while conducting an evaluation of its Program:

Identification of Covered Accounts

- Does the firm's Program include all covered accounts?
- Does the firm's Program include a documented process for periodic assessing the types of covered accounts offered to customers?

Establishment of the Program

- Is the Program integrated with your firm's policies and procedures?

- Are the firm's procedures for detecting and mitigating identity theft red flags adequately documented in the Program?
- Are the escalation channels reasonably designed to prevent and mitigate identity theft incidents?

Required Elements of the Program

- Does the firm adequately capture all red flags from identity theft sources?
- Are the firm's escalation channels effectively communicating issues to necessary stakeholders?

Administration of the Program

- Does the Program have a documented administration process?
- Is the Program updated at least annually?

The topical areas and questions listed above will help establish a framework to assist the firm in evaluating its Program and how it compares to the regulatory requirements of Reg S-ID. However, one-time evaluations of the Program are not sufficient to comply with Regulation S-ID and each firm should periodically conduct an end-to-end review and assessment of its Program, at least annually, to understand and update policies, procedures, and processes.

Does your firm's Program include all covered accounts?

The general (or likely) starting point for any evaluation is whether all covered accounts are included within the Program, and whether any accounts have been added or changed since the prior evaluation. Reg S-ID is applicable to all accounts that the firm offers or maintains primarily for personal, family, or household purposes, and involves or is designed to permit multiple payments or transactions, including: (1) Brokerage accounts; (2) Accounts maintained by a mutual fund (or its agent) that permits wire transfers or other payments to third parties; and (3) Any other account that the firm or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the firm or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

With this broad regulatory applicability, brokers, dealers, investment companies, and investment advisors should create policies and processes to regularly evaluate whether they offer or maintain covered accounts. This is both an initial and ongoing exercise required to reasonably ensure the firm identifies all covered accounts that it has experienced and should be clearly described within its Program policies.

Is the Program adequately integrated with existing policies and procedures?

In addition to assessing a firm's covered accounts, each firm should identify red flags across all business lines and support functions while considering the risk factors, sources, and categories of each red flag. The Firm should also be able to evidence the development and maintenance of a written Program designed to detect, prevent, and mitigate identity theft in connection with the opening or maintenance of a covered account.

Historically, firms have created standalone red flags or identity theft policies that do not properly integrate with their red flags and existing fraud, third-party risk, complaints, or cyber programs, and in some instances, firms have failed to create policies altogether based on an inaccurate understanding of the requirement of Reg S-ID.

To create a cohesive Program, a firm should map all the relevant process areas, stakeholders, and policies to its Program to understand the interactions and integrations between identity theft and red flag systems and the teams that identify, triage, and disposition identified red flags and identity theft incidents. The firm can then socialize the integrations across all business functions, groups, and departments. The purpose of this mapping is to clearly delineate and assign roles and responsibilities across the firm that are pertinent to identifying, detecting, preventing, and mitigating identity theft red flags. This approach will require the firm to implement a cross-functional workflow that allows stakeholders to corroborate and communicate across business lines.

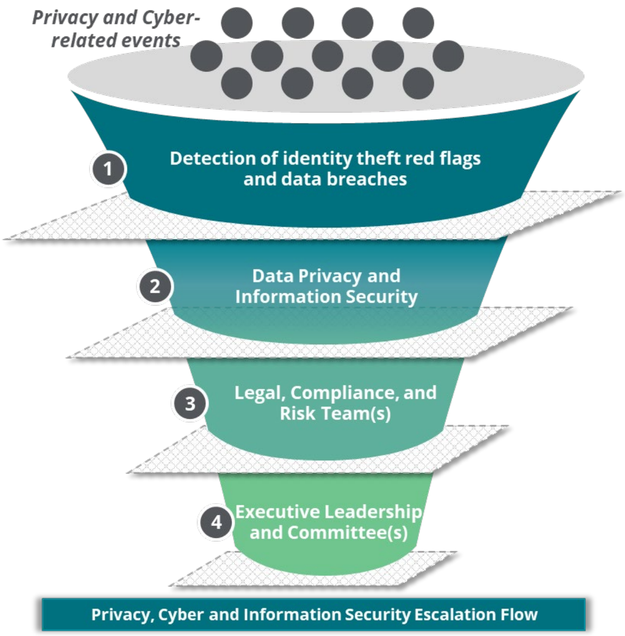
The purpose of this mapping is to clearly delineate and assign roles and responsibilities across the firm that are pertinent to identifying, detecting, preventing, and mitigating identity theft red flags.

Does the firm adequately capture all red flags from identity theft sources?

To properly assess identity theft red flags and risks, each firm should evaluate all of the areas where it could receive identity theft-related escalations. The evaluation should consider existing teams and departments that handle identity theft related incidents, as well as those that could potentially be notified of any identity theft incidents.

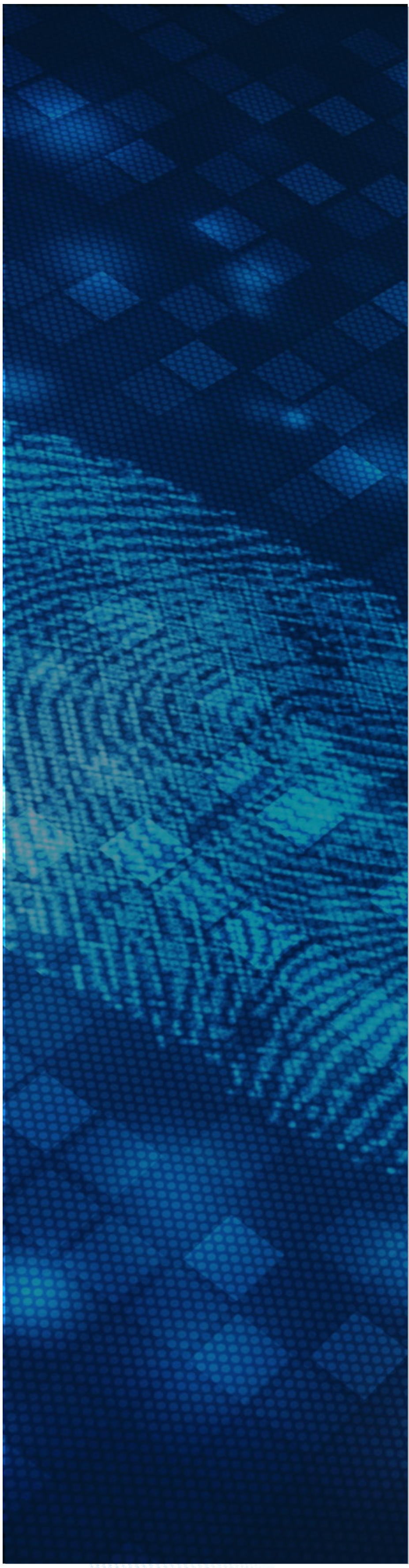
There are four broad areas that should be reviewed and incorporated as part of the Program, including:

- Front Office and Customer Support Team(s): Front office sales and sales support, call centers and technology support centers, social media response, customer inquiry and complaint, or customer validation and onboarding teams. These teams play a critical role in the detection and escalation of and response to identity theft red flags.
- Third-Party Risk / Vendor Management Team(s): These teams conduct risk-based reviews of third party's compliance with data protection requirements
- Cybersecurity / Technology Team(s): These teams monitor and detect cyber threats from internal and external sources, as well as manage access rights and controls
- AML / Fraud Team(s): These teams review and detect red flags related to fraudulent, suspicious, or unusual activity


Privacy and Cyber-related events
1
Detection of identity theft red flags and data breaches
2
Data Privacy and Information Security
3
Legal, Compliance, and Risk Team(s)
4
Executive Leadership and Committee(s)
Privacy, Cyber and Information Security Escalation Flow

These teams are all potential recipients of red flags and identity theft related incidents; however, there could be many more teams or functional areas that should be included in this evaluation depending on the size and complexity of the firm. After being evaluated, each firm should document tailored red flags within the identity theft prevention policy or equivalent and highlight the proper escalation channels and procedures for each red flag.

Are the firm's escalation channels sufficiently documented?



Each firm should evaluate what communication and escalation channels will be used to send and receive information related to identity theft red flags and incidents. Many firms utilize a centralized hub or shared site to facilitate the escalation of potential identity theft red flags. These centralized information hubs are designed to make it more efficient for firms to evaluate and consolidate the identity theft incidents that they receive, triage, and disposition.

A firm should consider having a well-documented and clear point of contact within their information security or data privacy team that serves as an escalation point for potential identity theft incidents, depending on the size and complexity of the firm. These information security or data privacy teams are typically responsible for reviewing information related to identity theft red flags and incidents to order to determine the appropriate response and whether additional escalations are required.

Additionally, the firm should clearly detail the appropriate escalation channel, response processes, and applicable procedures for each red flag. Escalation channels may include compliance, legal, and risk teams depending upon the structure and complexity of the firm. Although the standard 26 red flags should be considered as part of minimum requirements pursuant to FINRA's FTC FACT Act Red Flags Rule Template, the firm should also evaluate and include additional red flags based on the size and complexity of their specific business and operations.

The Program's Detection Grid, which is typically a table or appendix to its Program policy, is meant to be a usable guidance document for any employees within the firm to quickly find and understand the response processes required for each red flag. Specifically, it should include enough information for the user to understand who to escalate to and the steps required to start the escalation process.
Firm employees should be able to obtain the below information from the Detection Grid:

- **What:** What constitutes an identity theft red flag
- **Who:** Who is(are) the team(s) that receive and escalate red flags
- **How:** How is(are) a team(s) responding to red flags
- **Where:** Where should employees find information and additional guidance regarding responses to red flags (i.e., procedures on freezing accounts)

While most firms have a Detection Grid that provides generic red flags and detection mechanisms, many lack the specificity and processes required based on regulatory expectations. Additional issues with the Detection Grid often include:

- Red flags are not customized for specific business lines and risk exposure;
- The firm's experiences are not included or are inconsistent with firm's identity theft logs and guidelines;

- Not providing enough details for employees to be able to respond to red flags;
- Not including related policies and procedures that detail additional process steps; and,
- Not including red flag escalation channels, including centralized reporting hubs or online portals.

The obligation to escalate these red flags and incidents is not only a requirement of Reg S-ID, but also reasonably ensures a timely response to material incidents and breaches that could potentially impact a firm's reputation, regulatory scrutiny, and legal liability.

Does the Program have a documented administration process?

Each firm should establish a governance structure that provides for ongoing program administration, starting with initial written approval of the covered accounts and Program by the board of directors or senior management. The board of directors or executive committee should also be included in the oversight, development, implementation, and administration of the Program.

Additionally, identity theft incidents and breaches should be escalated to senior management, including executive committees, when material incidents occur or when there is a significant impact to the firm's business or stakeholders. This includes detailed processes for data privacy and information security team members to quickly escalate to chief information security officer or equivalent executive leader(s) upon identification of a material or significant event. Similarly, legal and/or compliance officers that become aware of a material or significant event may be required to escalate to their chief legal officer/general counsel or chief compliance officer.

Senior leadership should also reasonably ensure that the Program has the proper support and infrastructure to implement a training program for employees and cross-team and business line support for the Program including collaboration with front office, fraud, third-party risk management, cyber, and other applicable business lines and teams.

Is the firm updating its Program at least annually?

A firm should review its Program at least annually to evaluate the sufficiency and update it, as necessary, based on the firm's experiences. As part of the review, a firm should review all covered accounts, red flags, and identify whether any new product offerings impacted red flags or covered accounts since its last review. The analysis and determination of whether additional red flags need to be added should include a holistic look at the risks associated with each covered account type and based on the experiences with identity theft incidents. To conduct an evaluation or assessment, a firm should review its Program, covered accounts, communication and escalation channels, trainings, impacted teams, reporting cadence and structure, Detection Grid, and documentation of these areas within its policies and procedures.

Next steps

Firms of all sizes should expect more regulatory scrutiny around their Identity Theft Red Flags Programs and be closely evaluating their ability to achieve compliance with Reg S-ID. In most cases, this will require firms to assess their policies, procedures, and processes in place to support their Program to assist in determining if it's adequately designed to meet the SEC's regulatory expectations and industry best practices.

Deloitte has been one of the leading advisors with respect to Reg S-ID and has experience with guiding firms to address regulatory compliance and operational risk-related challenges. Deloitte also has a breadth of knowledge and experience with assisting firms with their Programs, including assessing covered accounts, communication and escalation channels, trainings, impacted teams, reporting cadence and structure, Detection Grid, and documentation of these areas within firm's policies and procedures against the requirements of Reg S-ID. Utilizing our experienced team, while leveraging accelerators and our understanding of industry leading practices and regulatory expectation, Deloitte can assist in evaluating a Program and providing tailored recommendations to a firm's information security and compliance teams.

Please contact one of our professionals listed below for more information.

Contacts

Josh Uhl
Managing Director | Deloitte & Touche LLP
juhl@deloitte.com

Andrew Kisz
Manager | Deloitte & Touche LLP
akisz@deloitte.com

Additional Contributors:

Taariq Phillips
Senior Consultant

Thomas Mayo
Consultant

[1] Risk Alert: Observations From Broker-Dealer and Investment Adviser Compliance Examinations Related to Prevention of Identity Theft Under Regulation S-ID (sec.gov)
[1] Regulation S-ID: Statute (17 CFR part 248 Subpart C (Regulation S-ID: Identity Theft Red Flags)
[1] FTC FACT Act Red Flags Rule Template

Formatted by CoRe Creative Services. RITM1256193