Lowenstein Sandler

Client Alert

Investment Management

December 19, 2025

SEC Brings Cybersecurity and Identity Theft Controls Case Against Registered Investment Adviser and Broker-Dealer

By Hannah Pastore, Jeremy Cantor, and Scott H. Moss

Introduction

On Nov. 25, the Securities and Exchange Commission (SEC) announced a settlement with a registered investment adviser (RIA) and broker-dealer (the Adviser) for violations of Regulation S-P and Regulation S-ID.[1]

Regulation S-P (17 CFR § 248.30) requires broker-dealers and RIAs to adopt written policies and procedures with administrative, technical, and physical controls to protect customer information. These policies must reasonably (1) ensure the security and confidentiality of customer information, (2) protect against anticipated threats or hazards, and (3) prevent unauthorized access or use that could cause substantial harm or inconvenience.[2]

Regulation S-ID (17 CFR § 248.201) requires broker-dealers and RIAs to implement a written identity theft prevention program tailored to their size, complexity, and activities. The program must reasonably (1) identify relevant red flags for covered accounts, (2) detect those red flags, (3) respond appropriately to prevent and mitigate identity theft, and (4) update the program periodically to address evolving risks. Firms must also determine periodically whether they offer or maintain covered accounts and incorporate red flags informed by past incidents and known identity theft methods.[3]

The subject activity of the Adviser in the SEC's order occurred ahead of the first of two compliance dates under the 2024 amendments to Regulation S-P, which took effect on Dec. 3 for larger advisers. The second deadline of the recent Regulation S-P amendments for smaller advisers will take effect on June 3, 2026. We previously wrote about these amendments here. These amendments introduce a mandatory incident response program, timely customer breach notifications, enhanced service-provider oversight, expanded definitions of protected information, strengthened recordkeeping, a revised privacy notice framework, and a national security/public safety delay mechanism. Similarly, the SEC's 2026 examination priorities focus on, among other things, Regulation S-P and Regulation S-ID.[4] With these amended Regulation S-P requirements now in effect for larger advisers, and given the SEC's 2026 examination priorities, RIAs should expect heightened SEC scrutiny in the coming months on Regulation S-P and Regulation S-ID compliance.

SEC Settlement Order

The Adviser is a dual RIA and broker-dealer, serving its customers through a nationwide network of representatives at branch offices known as member firms. According to the SEC's order, the Adviser violated Regulation S-P by failing to adopt and implement reasonably designed enterprise-level policies to protect customer records and information. The SEC also found violations of Regulation S-ID for failing to maintain and periodically update an identity theft prevention program.

Between July 2019 and March 2024, the Adviser faced several email account takeovers affecting 17 accounts across 13 member firms. Unauthorized actors accessed business email accounts and disseminated credential-harvesting emails to roughly 8,500 individuals, including a significant number of customers; four firms experienced repeat compromises, with the second incident alone affecting approximately 2,952 individuals. At least one incident resulted in an unauthorized wire transfer. The takeovers exposed customer records and personally identifiable information contained in the compromised accounts and, according to the SEC, occurred at firms that lacked basic controls required by the Adviser's own 2020 information security policy, including multifactor authentication (MFA), a written incident response framework, and annual security awareness training.

The order also faults the Adviser's enterprise governance. Prior to September 2020, the Adviser lacked a written enterprise wide information security policy for member firms. Although the Adviser adopted an information security policy in September 2020 covering 17 control categories, including MFA, incident response, and training, the SEC found the policy was not reasonably designed or effectively implemented. Adviser-collected data in 2021 and 2023 showed continuing control gaps at member firms; nevertheless, the Adviser did not enforce compliance, impose consequences, or strengthen its oversight in response.

Separately, the SEC took issue with the Adviser's failure to develop and implement an identity theft prevention program that was periodically updated to reflect changes in risk, despite ongoing cybersecurity incidents affecting customers. Specifically, the program had had no material updates since at least 2015, and it omitted cybersecurity related red flags even as the Adviser experienced email account takeovers at member firms during the relevant period. The SEC also found that the program lacked reasonable policies and procedures to detect and respond to red flags arising from cybersecurity breaches, and the procedures in place did not specify steps member firms should take in response to incidents like email account takeovers to prevent and mitigate identity theft. In addition, the Adviser failed to periodically determine whether it offered or maintained "covered accounts," had no policies or procedures for identifying covered accounts, and did not conduct required periodic risk assessments considering how accounts are opened and accessed and the Adviser's prior identity theft experiences.

Legal Violations

The SEC found willful violations of:

- Regulation S-P: failure to adopt written policies and procedures reasonably designed to protect customer records and information.
- Regulation S-ID: failure to develop and implement a written program designed to detect, prevent, and mitigate identity theft and to periodically determine covered accounts and update the program.

Sanctions and Remedial Measures

Without admitting or denying the findings, the Adviser consented to a cease-and-desist order, a censure, and a $325,000 civil penalty.

The SEC credited several remedial steps by the Adviser, including hiring a chief information security officer and a chief privacy officer, plans to update the information security policy, new accountability mechanisms for member firm noncompliance, formal risk assessments, mandatory cybersecurity onboarding, annual policy attestations, expanded training, the deployment of data loss prevention and monitoring tools, and the implementation of a vendor risk management program.

Practical Implications for Broker-Dealers and RIAs

This action highlights persistent supervisory and control expectations for firms with distributed office structures, independent contractor models, or a significant reliance on branch or member firms. This action also serves as a warning for all RIAs with respect to Regulation S-P and Regulation S-ID compliance. The SEC's focus extends beyond "paper compliance" to whether controls operate effectively in practice and whether firms enforce compliance where gaps persist. Key expectations include ensuring enterprise policies reflect actual risk, enforcing the adoption of controls at the branch or member firm level, and regularly refreshing programs to address current threats and incident trends.

The case also reinforces the need for dynamic Regulation S-ID programs. Identity theft red flags must incorporate contemporary threat patterns such as email account takeovers, phishing, credential harvesting, unauthorized transfers, and compromised vendor accounts. Programs should explicitly detail detection and response procedures for cyber-driven identity theft scenarios and document periodic determinations of covered accounts, considering account-opening methods, access channels, and recent incidents.

Strategic Guidance: Next Steps for Covered Institutions

Covered institutions should consider taking the following actions:

- Enterprisewide security baseline. Ensure written policies and procedures are reasonably designed for the firm's structure and are reliably implemented across all offices or member firms, with clear accountability for noncompliance. Emphasize MFA, incident response planning, security awareness training, and branch-level information security policies.
- Control effectiveness and monitoring. Confirm adoption and operation of required controls through attestations, testing, and remediation tracking. Use incident and audit data to identify systemic weaknesses and drive updates.
- Incident-driven program updates. Following cybersecurity breaches, update Regulation S-P and Regulation S-ID programs to reflect new threat vectors, detection mechanisms, and mitigation protocols. Include explicit red flags and response playbooks for threats such as email account takeovers and business email compromise.
- Covered accounts analysis. Conduct and document periodic assessments of whether the firm offers or maintains covered accounts, considering access channels and recent identity theft experiences as required under Regulation S-ID.
- Training, culture, and accountability. Provide role-based training, particularly for branch personnel, on phishing, credential harvesting, wire verification, and incident escalation. Establish disciplinary or contractual mechanisms to ensure timely remediation.
- Vendor and technology risk. Maintain a robust third-party risk management framework and deploy monitoring and data-loss prevention tools to reduce exposure through email and collaboration platforms.

Conclusion

Given this enforcement action and upcoming examination priorities, the SEC will likely continue to enforce core cybersecurity, privacy, and identity theft safeguards, particularly where policies are poorly tailored or inconsistently applied across branches. Broker-dealers and RIAs should expect strict scrutiny of control effectiveness and firm enforcement of noncompliance, and they should conduct prompt program reviews and updates under Regulation S-P and Regulation S-ID.

For more information, guidance, and clarity on implementing Regulation S-P, recent amendments to which have already gone into effect, or Regulation S-ID programs, please reach out directly to the authors of this article, our Privacy team, or your regular Lowenstein Sandler contact.

---

[1] https://www.sec.gov/files/litigation/admin/2025/34-104255.pdf
[2] https://www.ecfr.gov/current/title-17/chapter-II/part-248/subpart-A
[3] https://www.ecfr.gov/current/title-17/chapter-II/part-248/subpart-C
[4] https://www.sec.gov/files/2026-exam-priorities.pdf

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

HANNAH PASTORE
Associate
T: 212.419.5854
hpastore@lowenstein.com

JEREMY CANTOR
Counsel
T: 212.419.5986
jcantor@lowenstein.com

SCOTT H. MOSS
Partner
Chair, Fund Regulatory & Compliance
Co-chair, Investment Management Group
T: 646.414.6874
smoss@lowenstein.com