Lowenstein Sandler

Client Alert

Data, Privacy & Cybersecurity
Investment Management

August 4, 2025

Compliance Deadlines to Implement Significant Amendments to Regulation S-P Are Fast Approaching: Key Implications for Covered Institutions (Including Brokers and Investment Advisers) and Recommended Considerations

By Scott H. Moss, Kathleen A. McGee, and Hannah Pastore

Executive Summary

On May 16, 2024, the Securities and Exchange Commission (SEC) adopted sweeping amendments to Regulation S-P, which governs the privacy of nonpublic consumer personal and financial information for a broad range of financial institutions by implementing policies and procedures to safeguard this data and by providing customers with clear privacy notices. The amendments, effective August 2, 2024, introduced new requirements for incident response, customer notification, service provider oversight, and recordkeeping, and they expanded the scope of covered institutions and protected information. Compliance with the amendments will be implemented in phases based on entity size–larger entities are required to comply by December 3, 2025, while smaller entities have until June 3, 2026.

Who Is Covered?

The amendments apply to Regulation S-P's "covered institutions," including broker-dealers, funding portals, investment advisers, registered investment companies, employee securities companies, and notably, all transfer agents registered with the SEC or other appropriate agencies.

For purposes of the compliance date, entities that are considered "larger entities" are (1) investment companies that, together with other investment companies in the same group of related investment companies, have net assets of $1 billion or more as of the end of the most recent fiscal year, (2) SEC-registered investment advisers that have $1.5 billion or more in assets under management, (3) all broker-dealers that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act, and (4) all transfer agents that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act. "Smaller entities" are those covered institutions that do not meet these standards.

Key Changes and Requirements

1. Mandatory Incident Response Program

Covered institutions must implement written policies and procedures for an incident response program that addresses unauthorized access to or use of customer information. The program must enable detection, response, and recovery from such incidents and include procedures for customer notification.

2. Timely Customer Notification of Data Breaches

If sensitive customer information is compromised, covered institutions must notify affected individuals as soon as practicable but no later than 30 days after becoming aware of the incident. The notification must include a description of the incident, the type of information breached, the date of the breach, contact information, recommended actions for the customer, and guidance from the Federal Trade Commission (FTC).

3. Expanded Scope of Protected Information

The definition of "customer information" is broadened to include any record containing sensitive customer information, or otherwise known as nonpublic personal information, about a customer, whether in paper, electronic, or other form. This now explicitly covers:

- Information about a financial institution's own customers
- Information about customers of other financial institutions provided to the covered institution
- Information handled or maintained on behalf of a covered institution, not just information in its direct possession

"Sensitive customer information" is defined as any component of customer information, alone or in conjunction with other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual (e.g., Social Security numbers, driver's license numbers, biometric data, account numbers, and login credentials).

4. Service Provider Oversight

Covered institutions must exercise due diligence and ongoing monitoring of service providers. Policies and procedures must require service providers to notify the covered institution within 72 hours of any breach involving customer information.

5. Enhanced Recordkeeping

Institutions must maintain written records documenting compliance with the amended rules, including policies and procedures, incident documentation, investigation records, notifications, and service provider records.

6. Annual Privacy Notice Exception

The amendments align annual privacy notice delivery requirements with the statutory exception under the Fixing America's Surface Transportation Act (FAST Act). Institutions are exempt from providing annual privacy notices if they have not changed their privacy policies and share nonpublic personal information with third parties only in accordance with certain regulatory exceptions.

7. National Security/Public Safety Delay

Customer notification may be delayed if the Attorney General determines that notice poses a substantial risk to national security or public safety. The delay can be up to 30 days, with possible extensions in extraordinary circumstances. This, however, will likely be rare.

Strategic Guidance: Next Steps for Covered Institutions

With the first of two compliance deadlines fast approaching, covered institutions should begin addressing several critical considerations without delay. Our recommendations are as follows.

1. Assess and Update Policies and Procedures

Review and update existing written information security programs to ensure they meet the new requirements for incident response, customer notification, and service provider oversight. Ensure that policies specifically address the expanded definitions of customer and sensitive customer information.

2. Review and Enhance Service Provider Contracts

Amend contracts with service providers to require prompt notification–within 72 hours–of any breach involving customer information. Implement due diligence and monitoring processes to ensure ongoing compliance.

3. Prepare for Customer Notification Obligations

Develop or update customer notification templates and procedures to ensure compliance with the new 30-day notification deadline and content requirements. Establish internal protocols for rapid incident assessment and response.

4. Strengthen Recordkeeping Practices
Implement systems to document all aspects of compliance, including incident response activities, notifications, and service provider oversight. Ensure records are maintained in accordance with the new requirements.

5. Evaluate Applicability of Annual Privacy Notice Exception
Determine whether your institution qualifies for the annual privacy notice exception and, if it does, document the basis for relying on the exception.

6. Plan for Compliance Deadlines
Identify whether your institution is a "larger entity" (compliance by December 3, 2025) or a smaller entity (compliance by June 3, 2026) and develop a project plan to achieve timely compliance.

7. Train Staff and Raise Awareness
Conduct training on the new requirements for relevant personnel, especially those involved in information security, incident response, and customer communications.

Conclusion

The SEC's amendments to Regulation S-P represent a significant expansion of privacy and data security obligations for financial institutions. Early action is critical to ensure compliance by the applicable deadlines and to mitigate the risk of regulatory enforcement and reputational harm in the event of a data breach. Institutions should begin reviewing and updating their policies, procedures, contracts, and training programs as soon as possible.

For further information, guidance, and clarity on the amendments or our recommended next steps, please reach out directly to the authors of this article or your regular Lowenstein Sandler contact.

Contacts

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

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

KATHLEEN A. MCGEE
Partner
T: 646.414.6831
kmcgee@lowenstein.com

HANNAH PASTORE
Associate
T: 212.419.5854
hpastore@lowenstein.com