SEC Amendments to Regulation S-P: What Broker-Dealers and Registered Investment Advisors Need to Know

By Robert Gaines, Director and Thomas DeMayo, Partner

The Securities and Exchange Commission (SEC) recently announced significant amendments to Regulation S-P aimed at modernizing and strengthening the regulations governing the handling of consumers' nonpublic personal information by specific financial institutions. Regulation S-P was introduced almost 25 years ago in 2000 pursuant to the Gramm-Leach-Bliley Act and was intended to provide customers and consumers with protections against threat actors who commit identity theft and other crimes using personally identifiable information such as social security numbers, names, phone numbers and addresses.

The new amendments consist of two primary components: the **safeguard rule** and the **disposal rule**. The safeguard rule mandates covered financial institutions to establish written policies and procedures to safeguard customer information against unauthorized access and usage. The disposal rule necessitates proper disposal of consumer report information by financial institutions and transfer agents.

Regulation S-P Covered Institutions

The amended Regulation S-P applies to various covered institutions, including:

- Registered Investment Advisors (RIAs)
- Broker-Dealers
- Investment Companies
- Transfer Agents

Key Requirements

The amended safeguard rule imposes several key requirements on covered institutions:

- *Incident Response Program* - Covered institutions must develop and maintain a written incident response program aimed at promptly detecting, responding to and recovering from unauthorized access or usage of customer information. Additionally, provisions for oversight of service providers are mandated within this program.
- *Service Providers* - Formalized programs, including due diligence and monitoring, must exist to ensure that service providers have implemented reasonable controls to protect consumer information. Further, in the event of a breach of the service provider, the service provider must notify the covered institution as soon as possible but no later than 72 hours after becoming aware that the breach resulted in unauthorized access to consumer information. Upon such notification, the covered institution is to activate its incident response program.

- *Notification Protocol* - In the event of unauthorized access or usage of sensitive customer information, covered institutions must notify affected individuals without delay but no later than 30 days after becoming aware of the breach. The notification should include comprehensive details of the incident, the breached data and guidance on protective measures for affected individuals. The covered institution can elect to enter into a written agreement with the service provider to give the notifications on their behalf.

- *Privacy Notices* - Covered institutions are obligated to provide initial and annual privacy notices to customers, outlining information-sharing policies and customer rights. They must also create and maintain documentation showing the steps taken to comply with the Safeguards and Disposal Rules.

- *Customer Information* - With the amendment, the SEC expanded the scope of information covered by the Safeguards and Disposal Rules. The definition of "customer information" was adjusted to include "information in the possession of a covered institution or information that is handled or maintained by the covered institution or on its behalf, regardless of whether such information pertains to (a) individuals with whom the covered institution has a customer relationship or (b) the customers of other financial institutions where such information has been provided to the covered institution." These new rules also now cover customer information received by covered institutions from third-party financial institutions, as well as customer information, even when an individual no longer has a customer relationship with the covered institution.

- *Record Keeping* - Covered institutions are now required to maintain written records regarding the following:

    - Incident response policies and procedures.

    - Documentation of any detected unauthorized access to, or use of, customer information, as well as any response to and recovery from such unauthorized access to or use of customer information.

    - Documentation of any investigation and determination on whether notification is required, notice transmitted or United States Attorney General communications delayed.

    - Documentation of any contract or agreement with service providers.

Timeline to Enforcement

The amendments will come into effect 60 days after publication in the Federal Register. Larger entities, those with assets under management greater than $1.5 Billion, will have 18 months, while smaller entities will have 24 months from the date of publication to ensure compliance.

Key Takeaways

The SEC's amendments to Regulation S-P mark a significant stride toward fortifying consumer financial data protection measures. Covered institutions must promptly adapt to the revised requirements to ensure compliance and mitigate risks associated with unauthorized access or usage of customer information.

Covered institutions should:

- Review and update policies and procedures to include updates to existing safeguards and disposal policies to comply with the newly expanded definition of "customer information."

- Review and update vendor risk management policies and procedures.

- Evaluate contracts with service providers to identify any in which agreements exist with notification requirements in excess of 72 hours. Amend, as necessary, to ensure the service providers can comply with the new requirements.
- Revise incident response plans so that notification requirements are within scope or work with vendors to provide the notifications.
- Ensure that log and auditing tools are sufficient to provide protections and visibility into controls surrounding protected data that is covered by the amendments.
- Perform annual tabletop exercises that include scenarios in which consumer data is impacted.

To learn more about the new amendments, click here.

How We Can Help

We have a team of Cybersecurity and IT Privacy professionals who specialize in helping financial service firms manage the ever-evolving cyber and regulatory landscape. We can provide assistance with vendor management program design and management, incident response plan development and testing through table-top exercises, cybersecurity program review or penetration testing.

Contact Us

If your business is impacted by Regulation S-P and you need assistance, please contact your client service team or either of the following:

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Partner
Cybersecurity and Privacy Advisory
tdemayo@pkfod.com | 646.449.6353

Robert Gaines, CISSP, CECI, CCFI, CIPP/US
Director
Cybersecurity and Privacy Advisory
rgaines@pkfod.com | 425.518.1974