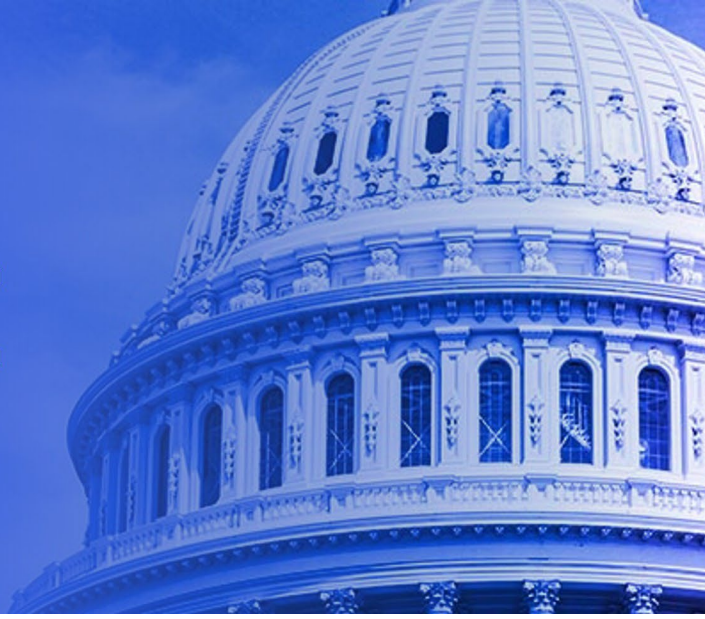
KPMG

Regulatory Alert

Regulatory Insights for Financial Services



May 2024

Regulation S-P: SEC Final Amendments

KPMG Insights:

- ***Data Security:*** *In addition to customer data breach notifications, rulemaking expands expectations around broader data risk management governance and controls (e.g. TPRM, monitoring/detection, disposal, cybersecurity, and privacy).*
- ***Aligning Rulemaking:*** *To align with other regulatory actions such as SEC cyber proposals/rules, national security reporting, GLBA.*
- ***Perimeter Expansion:*** *Expansion of "covered institutions" (including transfer agents); recognition of the increased use of technology and service providers and the corresponding increase in data security and privacy risks.*

The Securities and Exchange Commission (SEC) adopts final amendments to Regulation S-P, which governs the treatment of nonpublic personal information about consumers by certain financial institutions. The amendments apply to broker-dealers (including funding portals), investment companies, registered investment advisers, and transfer agents (collectively defined as "covered institutions"), and are intended to modernize and enhance the privacy protections provided to consumer financial information by requiring the adoption of incident response programs that:

- Address unauthorized access to or use of customer information.
- Require service providers to adhere to policies and procedures to protect customer information and provide notification of an incident.
- Provide timely notification to individuals affected by an incident.
- Establish and maintain records documenting compliance with the Safeguards and Disposal Rules under Regulation S-P.

The final amendments are adopted largely consistent with the SEC March 2023 proposal, with certain modifications based on comments received and to align with requirements in other rulemakings, such as notification requirements in the SEC's Public Company Cybersecurity Rule.

Details, including definitions, are highlighted below.

Incident Response Program. The amendments will require covered institutions to develop, implement, and maintain written policies and procedures for an incident response program that are "reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information)." The program must include policies and procedures to assess, contain and control, as well as notify certain "affected individuals" (discussed below).

Service Providers. As part of an incident response program, the amendments require covered institutions to establish, maintain, and enforce written policies and procedures reasonably designed to require oversight, including through due diligence on and monitoring of

service providers, to ensure service providers take appropriate measures to:

- Protect against incidents related to customer information.
- Provide notification to the covered institution as soon as possible, but no later than 72 hours after becoming aware of a breach in security has occurred (an increase from the proposed 48 hours), resulting in unauthorized access to a customer information system maintained by the service provider.

Customer Notification. The incident response programs will be required to include policies and procedures to provide "clear and conspicuous notice" to affected individuals "by a means designed to ensure that the individual can reasonably be expected to receive actual notice in writing" as soon as practicable, but no later than thirty (30) days after becoming aware of the incident. The notice requirement applies to each affected individual whose sensitive customer information was, or was reasonably likely to have been, accessed or used without authorization. However, the notice is not required if the covered institution has determined, after a reasonable investigation of the incident, that sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience.

Note: In a modification from the proposal, the final amendments will permit a delayed notice of up to thirty (30) days (with provisions for additional delays) if requested by the U.S. Attorney General due to a finding that the required notice would pose a substantial risk to public safety, in addition to national security (as proposed).

Recordkeeping. Covered institutions are required to establish and maintain written records documenting compliance with the Safeguards Rule and the Disposal Rule under Regulation S-P as outlined in the table below.

Covered Institution	Retention Period
Registered Investment Companies	*Policies and Procedures.* A copy of policies and procedures in effect, or that at any time in the past six (6) years were in effect, in an easily accessible place. *Other Records.* Six (6) years, the first two (2) in an easily accessible place.
Unregistered Investment Companies	*Policies and Procedures.* A copy of policies and procedures in effect, or that at any time in the past six (6) years were in effect, in an easily accessible place. *Other Records.* Six (6) years, the first two (2) in an easily accessible place.
Registered Investment Advisers	All records for five (5) years, the first two (2) in an easily accessible place.
Broker-Dealers	All records for three (3) years, in an easily accessible place.
Transfer Agents	All records for three (3) years, in an easily accessible place.

Additional Amendments. The final amendments to Regulation S-P also include provisions to:

- Conform the annual privacy notice delivery provisions to the terms of an exception provided by the Gramm-Leach-Bliley Act (GLBA – as amended), provided certain conditions are met.
- Extend the requirements of the Safeguards and Disposal Rules to all transfer agents registered with the SEC or another appropriate regulatory agency.

Definitions. Terms used throughout the final amendments include:

- *Customer information* means "any record containing non-public personal information about a customer of a financial institution, whether paper, electronic, or other form." *Note:* The final amendment extends the requirements of both the Safeguards Rule and the Disposal Rule to non-public personal information collected by a covered institution about its own customers and non-public personal information that is received from a third-party financial institution about that institution's customers.

- *Sensitive customer information* means "any component of customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information."
- *Service provider* means "any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution." *Note:* The final definition removed proposed language regarding "third parties" to clarify that covered institutions' affiliates are included.

Effective Date and Compliance Period. The final amendments become effective sixty (60) days after publication in the Federal Register, and provide the following periods to comply:

- Larger entities (as defined in the table below) will have eighteen (18) months after the date of publication in the Federal Register to comply with the amendments.
- Smaller entities (those that are not large entities) will have twenty-four (24) months after the date of publication in the Federal Register to comply.

Entity	Qualification to be Considered a "Large Entity"
Investment Companies (together with other investment companies in the same group of related investment companies)	Net assets of $1 billion or more as of the end of the most recent fiscal year.
Registered Investment Advisers	$1.5 billion or more in assets under management.
Broker-Dealers	All broker-dealers that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act.
Transfer Agents	All transfer agents that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act.

For more information, contact Mike Sullivan or Steve Stein.

Contact the author:

Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com