KPMG

Regulatory Alert

Regulatory Insights for Financial Services

March 2023

SEC proposed amendments to Regulation S-P

***KPMG Regulatory Insights**:*

- *The SEC is currently considering multiple rule proposals that seek to strengthen "cyber hygiene", improve incident notification and disclosure, and enhance data privacy protection across a broad array of supervised entities.*
- *In addition to Regulation S-P proposed amendments and Regulation SCI proposals, the SEC also announced (on the same day) reopening of the comment period to its February 2022 proposal for cyber risk management of investment advisers and funds. Collective actions in this area indicate the SEC is looking to consider the implications of its rulemakings, potential differences in state and federal requirements, and the importance of national security concerns.*
- *Key features of the Regulation S-P proposal specifically highlight requirements for: i) notification of a customer data breach, ii) monitoring and detection of unauthorized access to sensitive data, iii) proper disposal of customer information, and iv) expansion of coverage to transfer agents.*

The Securities and Exchange Commission (SEC or Commission) proposed amendments to Regulation S-P are intended to enhance the privacy protections provided to consumer financial information by requiring the adoption of an incident response program to address unauthorized access to or use of customer information and expanding the scope of institutions and information subject to the regulation.

The proposal would apply to broker-dealers, investment companies, registered investment advisers, and transfer agents, defined collectively as "covered institutions," and would require them to address the following:

- **Incident Response**. Develop, implement, and maintain written policies and procedures for an incident response program that is "reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information." The program must include procedures to assess, contain, and control incidents of unauthorized access or use of customer information, including notifications to certain "affected individuals".
- **Service Providers**. Include as part of the incident response program, written policies and procedures that require service providers to a covered institution to take appropriate measures that are designed to protect against unauthorized access or use of customer information, including the obligation to notify the covered institution as soon as possible but no later than 48 hours after becoming aware of a breach.
- **Incident Notification.** Notify affected individuals of incidents relating to unauthorized access or use of their sensitive customer information (as defined in the rule – see below) as soon as practicable but no later than thirty days after becoming aware of the occurrence of such an incident. A delayed notice would be permissible if requested by the U.S. Attorney General due to a finding that the required notice would pose a substantial risk to national security.
  - Covered institutions would not need to provide this notification if they determine "after reasonable investigation of the facts and circumstances" that sensitive customer information has not been and is not reasonably likely to be used in manner that would result in "substantial harm or inconvenience" (as defined in the rule – see below).

— **Recordkeeping.** Establish and maintain written records documenting compliance with the Safeguards Rule and the Disposal Rule under Regulation S-P.

Definitions. Definitions of terms used throughout the proposal include:

— "Customer information" to mean any record containing non-public personal information about a customer of a financial institution, for purposes of the Safeguards Rule and the Disposal Rule.

— "Sensitive customer information" to mean "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.

— "Substantial harm or inconvenience" to mean "personal injury, or financial loss, expenditure of effort or loss of time that is more than trivial." The definition is intended to cover "a broad range of financial and non-financial harms and inconveniences that may result from failure to safeguard sensitive customer information."

— "Service provider" to mean "any person or entity that is a third party and receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution.

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

— Conforming 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.

— Extending the Safeguards Rule to transfer agents registered with the Commission or another appropriate regulatory agency.

— Extending the Disposal Rule to all transfer agents, including those registered with another regulatory agency.

— Extending the requirements of both the Safeguards Rule and the Disposal Rule to all customer information (as defined under the proposal) in the possession of a covered institution, and all consumer information that a covered institution maintains or otherwise possesses for a business purpose, as applicable, regardless of whether such information pertains to individuals with whom the covered institution has a customer relationship, or pertains to the customers of other financial institutions and has been provided to the covered institution.

State laws and regulations. The SEC notes that broker-dealers, investment companies, and registered investment advisers currently respond to data breaches, including customer notifications, according to applicable state laws. SEC suggests, "as a result, a firm's notification obligations arising from a single data breach may vary such that customers in one state may receive notice while customers of the same institution in another state may not receive notice or may receive less information." The proposed amendments would establish a Federal minimum standard for providing notification to all customers of a covered institution affected by a data breach (regardless of state residency) and providing consistent disclosure of "important information" to help affected customers respond to a data breach.

Compliance. The proposal provides that compliance with the rule would be required "twelve months after the effective date of any adoption of the proposed amendments."

Other rule proposals. The SEC acknowledges that the entities covered by this Regulation S-P rule proposal may also be impacted by its rule proposals to amend Regulation SCI and to establish Cybersecurity Risk Management frameworks (separately for "Market Entities" and for Investment Advisers and Funds), which contain policy, procedure, and disclosure requirements. The SEC notes that, although related, each of the proposals has a different scope and purpose and has included questions and requests for comment regarding implementation of the multiple requirements and obligations.

Comment Period. The SEC requests comment on the proposed rule (and many questions contained within it) to be submitted no later than 60 days after the date of publication in the Federal Register.

For more information, please contact Mike Sullivan or Steve Stein.

Contact the author:

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