Davis Polk

SEC expands cybersecurity requirements of Regulation S-P, the "Safeguards Rule"

May 22, 2024 | Client Update | 4-minute read

The SEC expanded the scope of the Safeguards Rule, which already required broker-dealers, investment advisers and investment companies to have reasonably designed policies and procedures to protect customer information. The SEC amended the rule to add requirements for incident response programs, customer notifications, and regulatory obligations.

The SEC adopted amendments to Regulation S-P, known as the "Safeguards Rule," on May 16, 2024. The amendments apply to transfer agents in addition to broker-dealers, investment companies, and registered investment advisers (Covered Institutions). The existing rule has required Covered Institutions to adopt reasonably designed written policies and procedures to protect customer information from threats such as data breaches. The amendments impose the following additional requirements:

- **Incident response program:** Covered Institutions must adopt written policies and procedures establishing an incident response program. The incident response program must identify how the institution will (1) assess the nature and scope of a data breach, (2) determine which customer information systems and customer information may have been affected, (3) contain and control the breach, and (4) provide notice of the breach to customers. The incident response program takes effect any time that customer information is accessed or used without authorization, including upon notification from a service provider of a data breach.
  - **Service providers:** Covered Institutions using service providers do not need to have a written contract requiring service providers to notify customers of a data breach. The institutions only need to establish written policies and procedures reasonably designed to establish oversight of their service providers' compliance with the rule. A service provider must be required to notify the institution of a data breach within 72 hours of its awareness of the incident.
- **Customer notification:** Covered Institutions must provide "clear and conspicuous notice" in writing to customers whose sensitive information was or was reasonably likely to have been subject to unauthorized access or use. The notice must be issued within 30 days of when the Covered Institution becomes aware of the incident unless an exception applies. Individuals covered under the rule include customers of a Covered Institution or other entities that have given their customer information to the Covered Institution.
  - **Exception for delays:** An initial delay in customer notification of up to 30 days is permissible if the United States Attorney General finds that notification would create a "substantial" national security or public safety risk and requests a delay in writing to the SEC. The SEC may grant a second delay of up to 30 days if the security risk continues and it receives another written request from the Attorney General. Extraordinary circumstances may warrant an additional delay of up to 60 days upon the Attorney General's written request, with prolonged security risks eligible for additional delays. Covered institutions may ask the Attorney General to issue a request for a delay to the SEC.
  - **Entity providing notices:** Covered Institutions are ultimately responsible for complying with the notification requirements, even if they have a written contract requiring their service providers to issue customer notifications.

    - **Contents and format of notices:** Customer notices must explain details of the incident, the breached data, and steps that affected individuals can take to protect themselves from the breach.

- **Recordkeeping:** Covered Institutions must keep records of written policies and procedures about the incident response program; written policies, procedures, or contracts with service providers adopted under this rule; and documents regarding data breaches and subsequent notification processes, including Attorney General requests for delays in notice.
- **Compliance date:** Larger entities must comply with the amended rule within 18 months of its publication in the Federal Register. Smaller entities must do so within 24 months.

The final rule substantially reflects the SEC's original proposal, with some modifications that slightly reduce the burden of compliance. The SEC proposed these changes last year as part of a sweeping package of cybersecurity-related reforms (discussed in this client update). This amendment of the Safeguards Rule is the first part of the proposed reforms to be adopted.

Commissioner Hester Peirce expressed concerns in a public statement that the rule could result in "over-notification," where individuals receive so many notices that they become commonplace and potentially ignored. She also indicated that customer notification remains a complex issue, with more work to be done to streamline notification procedures.

The SEC periodically brings enforcement cases against broker-dealers and investment advisers for breaching the Safeguards Rule following cybersecurity events that involve customer data (see our prior client update as discussed in this earlier client update). The new requirements increase the landscape for possible enforcement action, including claims for inadequate incident response plans following a cybersecurity incident.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres
+1 212 450 4724
greg.andres@davispolk.com

Matthew J. Bacal
+1 212 450 4790
matthew.bacal@davispolk.com

Martine M. Beamon
+1 212 450 4262
martine.beamon@davispolk.com

Micah G. Block
+1 650 752 2023
micah.block@davispolk.com

Robert A. Cohen
+1 202 962 7047
robert.cohen@davispolk.com

James W. Haldin
+1 212 450 4059
james.haldin@davispolk.com

Stefani Johnson Myrick
+1 202 962 7165
stefani.myrick@davispolk.com

Fuad Rana
+1 202 962 7053
fuad.rana@davispolk.com

Gabriel D. Rosenberg
+1 212 450 4537
gabriel.rosenberg@davispolk.com

Zachary J. Zweihorn
+1 202 962 7136
zachary.zweihorn@davispolk.com