Deloitte.

Center *for* **Regulatory Strategy US**

# SEC finalizes amendments to Regulation S-P

**The amendments expand the scope of customer information covered by the rule.**

On May 15, 2024, the Securities and Exchange Commission (SEC) finalized amendments to Reg S-P that modernize the agency's customer information protection rule, which was initially adopted in 2000. The amendments enhance the protection of customer information by expanding the scope of information covered by the rule, requiring impacted institutions to adopt incident response programs and establishing a notification requirement when data breaches or potential data breaches put customers at risk of harm.

## *5 insights you should know*

**Impacted entities:** Reg S-P applies to broker-dealers, investment companies (ICs), registered investment advisers (RIAs), and transfer agents. While Reg S-P has long covered broker-dealers, ICs and RIAs, transfer agents are a new addition to the types of entities scoped into the rule.

**Scope of information:** The final amendments expand the scope of customer information required by the rule to include nonpublic personal information that the financial institution receives from or shares with service providers as well as information it collects directly from its customers. This is a critical change in how the rule is constructed, and firms will need to update their programs to account for this expanded scope.

**Incident response program:** Firms are required to establish an incident response program that is "reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information."

**Other requirements:** The final rule also includes a customer notification requirement whereby affected individuals must be notified "as soon as practicable" and not later than 30 days after the institution becomes aware that an incident of unauthorized access or use of customer information likely occurred. There is an exception to this requirement if it is determined that the customer information most likely was not used in a manner that would cause "substantial harm or inconvenience."

**Compliance period:** Large entities have until December 2025 to comply with the amendments while small entities have until June 2026. While firms have considerable time to implement the rule's amendments, they likely also have parallel regulatory implementation efforts competing for budget and attention. *For a definition of large and small entities, please see the next page.*

## *5 considerations to evaluate*

1 **Degree of impact:** All firms implicated by Reg S-P should review their existing processes for alignment with the rule's expanded requirements. Transfer agents that are newly scoped into the rule may need to establish new compliance processes associated with the rule. Broker-dealers, ICs and RIAs will need to evaluate their existing programs for alignment with the rule's expanded requirements.

2 **Assess data sources:** Firms should inventory their dataflows for nonpublic personal information to reasonably ensure that they are appropriately monitoring for and responding to all data breaches implicated by the rule. The customer notification requirement includes customer information shared with a third party as well as any data breaches that originate at that source.

3 **Assess or establish a program:** If a firm does not have an existing incident response program it will need to establish one. Otherwise, firms may need to assess their existing programs to reasonably ensure they align with the rule's expectations. If the SEC publishes future guidance on its expectations for firms' incident response programs, further modification may need to be made.

4 **Apply a narrow reading of exceptions:** To safeguard against scrutiny in future examinations, firms should take a cautious approach to the more lenient aspects of the customer notification requirement. For example, firms should determine an internal standard for "as soon as practicable" notification, rather than defaulting to a 30-day time horizon. Similarly, firms may be well served by taking a generous approach to "substantial harm or inconvenience" or alternatively disclosing all data breaches to customers without seeking to make such determinations.

5 **Make a plan:** Firms with existing incident response programs may want to begin by mapping (or locating documentation of) dataflows for customer information, especially with respect to service provider data. Firms without incident response programs likely will want to begin by establishing an incident response program that is robust and designed to meet each of the rule's requirements.

## Definitions

The following entities will be designated "**Larger Entities**:" 1) Investment companies together with other investment companies in the same group of related investment companies with net assets of $1 billion or more as of the end of the most recent fiscal year; 2) RIAs with $1.5 billion or more in assets under management; and 3) All broker-dealers and transfer agents that not are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act.

A **broker or dealer is a small entity** if it: (i) had total capital of less than $500,000 on the date in its prior fiscal year as of which its audited financial statements were prepared or, if not required to file audited financial statements, on the last business day of its prior fiscal year; and (ii) is not affiliated with any person that is not a small entity.

A **transfer agent is a small entity** if it: (i) received less than 500 items for transfer and less than 500 items for processing during the preceding six months; (ii) transferred items only of issuers that are small entities; (iii) maintained master shareholder files that in the aggregate contained less than 1,000 shareholder accounts or was the named transfer agent for less than 1,000 shareholder accounts at all times during the preceding fiscal year; and (iv) is not affiliated with any person that is not a small entity.

## Endnotes

1. Securities and Exchange Commission (SEC), "Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information," May 15, 2024.

## Connect with us:

**Josh Uhl**
Managing Director | Risk & Financial Advisory
Deloitte & Touche LLP
**juhl@deloitte.com**

**Meghan Burns**
Manager | Center for Regulatory Strategy
Deloitte Services LP
megburns@deloitte.com

Deloitte.