JENNER & BLOCK

# The SEC Expands Its Cybersecurity Oversight by Adopting Regulation S-P Amendments

**Client Alerts**

May 30, 2024
By: Charles D. Riely, Gina Shabana

Earlier this month, approximately one year after releasing its proposed amendments to Regulation S-P, the SEC announced the adoption of final amendments to Regulation S-P, expanding the information protected, the policies and procedures required, and the entities covered by the rules. Covered financial institutions—including any broker-dealer, investment company, registered investment adviser, or transfer agent—will now be required to establish and implement a reasonable incident response program and notify impacted customers of certain security breaches. The final amendments further codify the SEC's expectations of the financial institutions' oversight of third-party service providers, and they expand the reach of the Safeguards and Disposal Rules to transfer agents. This alert covers the new components of Regulation S-P, along with our key takeaways.

## Incident Response Program

The final amendments require covered institutions to develop, implement, and maintain written policies and procedures for an incident response program "reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information." 17 CFR § 248.30(a). While the SEC does not dictate the exact procedures expected of financial institutions, it does set the expectation that the institutions "tailor their policies and procedures to their individual facts and circumstances."[1] The final rule requires that the incident response program:

1. Assess the nature and the scope of the incident;
2. Contain and control the unauthorized access to customer information; and
3. Notify impacted customers.

## Notification Requirement

The final amendments do not detail precisely what constitutes a reasonable incident response program. But they do codify certain specific requirements relating to the customer notice element of the final rule, including (1) who must receive the notice, (2) when notice must be sent, and (3) exceptions to the notice obligations.

**1) Who must receive notice**? The rule requires covered financial institutions to provide written notification to "affected individuals" whose "sensitive customer information" was or is reasonably likely to have been compromised.

**a. *Affected individuals*.** The final amendments broadly expanded the scope of "customer information" subject to Regulation S-P, which now includes "any record containing 'nonpublic personal information' (as defined in Regulation S-P) about 'a customer of a financial institution,' whether in paper, electronic or other form that is handled or maintained by the covered institution or on its behalf." What this means for financial institutions is that Regulation S-P, including the notice requirement, will now apply not only to its customers, but to "customer information in a covered institution's possession or that is handled or maintained on the covered institution's behalf, regardless of whether such information pertains to" its customers or customers of *other* financial institutions.[3]

**b. *Sensitive customer information***. The rule defines "sensitive customer information" as information that, if compromised, "could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information." 17 CFR § 248.30(d)(9). The rule provides examples of two different types of sensitive information:

i. Unique identifying customer information (*e.g.*, social security number, driver's license, passport number, biometric record, among others); and

ii. Customer information that in combination with other similar identifying information can be used to access a customer's account (*e.g.*, access code, credit card expiration date, partial social security number, place of birth, among others).

**2) When must notice be provided?** The rule requires that clear and conspicuous notice be provided in an accessible manner as soon as reasonably practicable, but not later than 30 days, after the covered institution becomes aware that a breach has or is reasonably likely to have occurred.

**3) What are the exceptions to the notice requirement?** The rule provides two exceptions:

**a. *Risk of Harm*.** Notice is not required if, "after a reasonable investigation of the facts and circumstances of the incident, [a covered financial institution] has determined 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.[4]

**b. *National Security & Public Safety Delay*.** The final rule also permits delaying customer notifications for up to 30 days (with possible extensions for extraordinary

circumstances) for substantial public safety or national security risk upon determination by the Attorney General.

**Annual Notice Exception**

The final amendments now include an exception to the annual notice requirement. The exception to the requirement of delivering annual privacy notices applies "if the institution (1) only provides non-public personal information to non-affiliated third parties when an exception to third-party opt-out applies and (2) the institution has not changed its policies and practices with regard to disclosing non-public personal information from its most recent disclosure sent to customers."[5]

**Transfer Agents**

Another significant change was to extend the Safeguards Rule and the Disposal Rule to apply to transfer agents registered with the SEC or another appropriate regulatory agency. As the SEC explained in its Proposing Release, transfer agents are subject to many of the same risks of data system breach or failure that other market participants face, and the scope and volume of funds and securities processed or held by transfer agents have increased dramatically since Regulation S-P was first adopted.[6] Previously, the Safeguards Rule, which required covered institutions to adopt written policies and procedures for the protection of customer records and information, did not apply to any transfer agents; and the Disposal Rule, which required proper disposal of consumer report information, applied only to transfer agents registered with the SEC.

**Oversight of Servicer Providers**

Regulation S-P defines a service provider as "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 financial institution]."[7]

Under the final amendments, covered financial institutions are required to establish and implement "written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers, including to ensure that the covered institution notifies affected individuals."

The procedures must address how the covered financial institution will "ensure service providers take appropriate measures to: (1) Protect against unauthorized access to or use of customer information; and (2) Provide notification to the covered institution as soon as possible, but no later than 72 hours after becoming aware that a breach in security has occurred resulting in unauthorized access to a customer information system maintained by the service provider."

While the proposed rule would have required covered institutions to enter into a written contract with its service providers to deliver data breach notices, the final amendments did not adopt the written contract requirement.

**Recordkeeping**

The final amendments conform the proposed recordkeeping rules for registered investment advisers, registered investment companies, and unregistered investment companies to the same detailed description that applies to broker-dealers and transfer agents and adopt the recordkeeping amendments substantially as proposed. The final amendments require covered institutions to maintain the following records:

- Written policies and procedures required to be adopted and implemented pursuant to the Safeguards Rule;
- Written documentation of any detected unauthorized access to or use of customer information, as well as any response to, and recovery from such authorized access to or use of customer information;
- Written documentation of any investigation and determination regarding whether notification to affected individuals is required;
- Written policies and procedures to oversee, monitor, and conduct due diligence on service providers, including to ensure that the covered institution is notified when a breach in security has occurred at the service provider;
- Written documentation of any contract entered into pursuant to the service provider oversight requirements; and
- Written policies and procedures required to be adopted and implemented pursuant to the Disposal Rule.

The required retention period varies by type of covered institution:[8]

| **Covered Institution** | **Retention Period** |
|---|---|
| Registered Investment Companies | *Policies and Procedures*. Six years, in an easily accessible place.<br>*Other records*. Six years, the first two in an easily accessible place. |
| Unregistered Investment Companies | *Policies and Procedures*. Six years, in an easily accessible place.<br>*Other records*. Six years, the first two in an easily accessible place. |
| Registered Investment Advisers | All records for five years, the first two in an easily accessible place. |
| | |

| | |
|---|---|
| Broker-Dealers | All records for three years, in an easily accessible place. |

**Compliance period**

Large entities are required to comply with the final rule within 18 months of its adoption. While smaller entities have a 24-month compliance period. Large entities include:

- ***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;
- ***Registered investment advisers*** with $1.5 billion or more in assets under management; and
- ***Broker-dealers and transfer agents*** that do not constitute small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act.

**Key Takeaways**

- **Cybersecurity remains a priority for the SEC**. Now, more than ever, financial institutions must implement a robust cybersecurity program, including assessing and determining the extent of actual or potential breaches, to protect against costly notifications, and reputational harm.
- **Firms must oversee their third-party service providers**. Financial institutions must ensure that their third-party due diligence and oversight program is sufficient and may want to consider (while not required by Regulation S-P) incorporating expectations of third parties into their service contracts.
- **Documentation of compliance is essential.** Regulation S-P now contains several recordkeeping requirements that span policies and procedures covered by the rule, as well as incident response and accompanying analysis.

**Conclusion**

If the past is any guide, the Commission's staff will have high expectations for registrants as they comply with the new rules and will scrutinize their compliance after the breach. Firms thus should ensure their policies and practices are updated to prepare for this scrutiny.

## Footnotes

[1] Adopting Release at 19-20.

[2] See Adopting Release at 26.

[3] Adopting Release at 342.

[4] Adopting Release at 35.

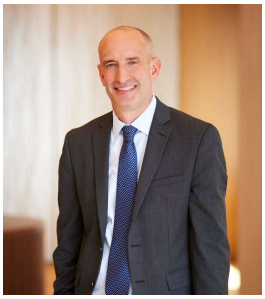
[5] Adopting Release at 127.

[6] See Adopting Release at 100, 108–11.

[7] Adopting Release at 70.

[8] Adopting Release at 122–23.

## Related Attorneys



**Charles D. Riely**
Partner
criely@jenner.com
+1 212 891 1686

**Gina Shabana**
Associate
gshabana@jenner.com
+1 202 639 6076

## Related Capabilities

Fintech and Crypto Assets

Hedge, Investment, and Private Equity Funds

Investigations, Compliance, and Defense

Investor and Securities Litigation



**Stay Informed** →