Simpson Thacher

Regulatory and Enforcement Alert

SEC Adopts Significant Amendments to Regulation S-P Requiring Notification of Sensitive Customer Information Breaches, Service Provider Oversight

May 22, 2024

The SEC voted last week to make significant amendments to Regulation S-P, which governs the treatment of consumer non-public personal information collected by certain financial institutions: broker-dealers, investment companies, registered investment advisers and transfer agents registered with the SEC or another appropriate regulatory agency (collectively, "**Covered Institutions**").[1] As discussed below, we estimate that compliance by large Covered Institutions will be required by early 2026, affording such Covered Institutions time to prepare with what may be onerous requirements.

At a high level, the amendments establish a federal "minimum" standard for Covered Institutions to provide data breach notifications to affected individuals. This federal standard applies regardless of, and is in addition to, any individual state's own requirements for data breaches. The federal standard expands the scope of customer information (as defined below) subject to Regulation S-P, requires a 30-day notification period for data breaches and establishes a new notification trigger that starts the 30-day notice period. The amendments further require each Covered Institution to adopt an incident response program for situations in which there is unauthorized access or use of customer information, specifically instituting a notification requirement to affected individuals if their "sensitive customer information"[2] is, or is reasonably likely to have been, accessed or used without authorization. In addition, the amendments also implement recordkeeping requirements, provide an exception to the annual privacy notice delivery requirement (pending certain conditions) as well as requirements for oversight of service providers.

The principal elements of the amendments are discussed in further detail below.

---

[1] Regulation S-P's initial adoption in 2000 included a requirement for broker-dealers, investment companies and registered investment advisers to adopt written policies and procedures that address administrative, technical and physical safeguards to protect customer records and information (the "safeguards rule"), and a requirement for proper disposal of consumer report information in a manner designed to protect such information from unauthorized access (the "disposal rule"). The disposal rule was applicable to transfer agents in addition to the institutions covered by the safeguards rule; prior to the adoption of last week's amendments, transfer agents were not required to comply with the safeguards rule. Regulation S-P also included a requirement for such broker-dealers, investment companies and registered investment advisers to issue privacy notices that included an opt-out provision in certain circumstances.

[2] Sensitive customer information is defined under the amendments as 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 (*e.g.*, social security numbers and other types of identifying information that can be used alone to authenticate an individual's identity such as a driver's license, passport number, employer or taxpayer ID).

- **Application to More Customer Information.** The amendments adopt a new definition of "customer information," combining the scope of information covered by both the safeguards and disposal rules to now encompass both customer and consumer information (collectively "**customer information**"). The term is also expanded to encompass customer information in the possession of a Covered Institution as well as customer information being handled or maintained on its behalf. The protections afforded by both the safeguards and disposal rules now apply to customer information regardless of whether such information is in the possession of the Covered Institution or being handled or maintained on its behalf.
- **Incident Response Program.** Covered Institutions must implement written policies and procedures for an incident response program reasonably designed to detect, respond to, and recover from an unauthorized access to or use of customer information. The incident response program will be required to include procedures to:

    1. assess the nature and scope of any incident and identify the type of customer information that has been accessed or used without authorization,
    2. take appropriate steps to contain and control the incident to prevent further unauthorized access or use of customer information and
    3. notify each affected individual (*as discussed in Notification Requirement bullet below*).

    The amendments provide general guidelines that are intended to help Covered Institutions develop and adopt incident response programs that are specifically tailored to suit the size, complexity and the nature and scope of their activities.
- **Notification Requirement.** Covered Institutions must provide notice to affected individuals as soon as practicable, but no later than 30 days[3] after becoming aware that "sensitive customer information" was, or is reasonably likely to have been, accessed or used without authorization.[4] The notice must include details about the incident, the date of the breach and the steps affected individuals can take in response to protect themselves and their sensitive information. A customer notice must be clear and conspicuous and provided by a means designed to ensure that each affected individual can reasonably be expected to receive it.[5]
- **Recordkeeping and Annual Notice Amendments.** Covered Institutions will be required to maintain written records documenting compliance with the requirements of the safeguards and the disposal rules. The SEC indicated in the adopting release that the recordkeeping requirements are consistent with each

[3] Covered Institutions will be permitted to delay providing notice after the Commission receives a written request from a state's Attorney General that this notice poses a substantial risk to national security or public safety. The notice may be delayed for an additional period of 30 days from the date the Commission receives such notice; 60 days in extraordinary circumstances.

[4] A Covered Institution is not required to provide notice if a Covered Institution determines, after a reasonable investigation of the facts and circumstances of the incident of an unauthorized access to or use of sensitive customer information, that the 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.

[5] The requirement to provide "written" notice can be satisfied electronically for those customers who have agreed to receive information electronically, provided notice is distributed through electronic means consistent with the SEC's guidance on electronic delivery of documents.

Covered Institution's respective recordkeeping requirements[6] (*i.e.*, for RIAs, the requirements track the requirement in Section 204-2 of the Advisers Act to maintain all records for five years, the first two in an easily accessible place).

- **Exception from Requirement to Deliver Annual Privacy Notice.** The amendments include a change to the current requirement under Regulation S-P to provide annual privacy notices to conform with the delivery requirement of the Fixing America's Surface Transportation Act (FAST Act), now providing an exception to the annual privacy notice requirement if the following conditions are met: (i) the Covered Institution only provides non-public personal information to non-affiliated third parties when an exception to third-party opt-out applies and (ii) the Covered Institution has not changed its policies and practices with regard to disclosing non-public personal information from its most recent disclosure sent to customers.
- **Oversight of Service Providers.**[7] Covered Institutions are required to implement written policies and procedures reasonably designed to require oversight of service providers, including through due diligence and monitoring. The policies must be reasonably designed to ensure service providers take appropriate measures to (i) protect against unauthorized access to or use of customer information and (ii) provide notification to the Covered Institution as soon as possible, but no later than 72 hours after becoming aware of a breach in security resulting in unauthorized access to a customer information system maintained by the service provider. The amendments allow a Covered Institution to enter into a written contract with the service provider to notify affected individuals on the Covered Institution's behalf.

Compliance Dates

For large[8] Covered Institutions, the Commission provided an 18-month compliance period after the Federal Register publishes the amendments. Publication has not occurred by the date of this memo; assuming a July 2024 publication date, we estimate that the compliance date will be in early 2026. Smaller entities have a 24-month compliance period.

Private Fund Adviser Considerations

These Regulation S-P amendments are relevant to private fund managers that are registered investment advisers, which are already subject to the privacy notice and safeguarding requirements under Regulation S-P with respect

[6] *See* Table 1 on pg. 122 of the adopting release.

[7] Service Provider is defined under the amendments to mean 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.

[8] The particular thresholds vary depending on the type of Covered Institution. For example, a large SEC-registered investment adviser is defined as having $1.5bn in AUM whereas a large investment company (together with other investment companies in the same group of related investment companies) is defined as having net assets of $1bn or more as of the end of the most recent fiscal year.

to natural person investors in the private funds they manage.[9] Upon the compliance date of the Regulation S-P amendments discussed herein, registered investment advisers will need to comply with the incident response program, notification, and other requirements with respect to natural person investors in the private funds they manage. Accordingly, registered investment advisers to private funds should establish policies and procedures to comply with these requirements.

Conclusion

The SEC intended the amendments to consolidate standards for informing customers of sensitive information breaches, rather than rely on varying state requirements. While standardization of requirements can generally be helpful, the amendments impose operationally challenging notification requirements and deadlines. Covered Institutions will likely need the entire compliance period to prepare operationally for those requirements.

[9] While private funds (*i.e.*, 3(c)(1) and 3(c)(7) funds) are not subject to Regulation S-P, they may be subject to regulations that have been adopted by other federal regulatory agencies pursuant to Gramm-Leach-Bliley Act and impose privacy notice and safeguarding obligations similar to Regulation S-P. Registered investment advisers to private funds typically provide notice to natural person investors in the private fund(s) to satisfy both the adviser's privacy notice obligations under Regulation S-P and similar obligations that may be applicable to the private fund(s) they manage.

For further information regarding this Alert, please contact one of the following authors:

WASHINGTON, D.C.

David W. Blass
+1-202-636-5863
david.blass@stblaw.com

Meaghan A. Kelly
+1-202-636-5542
mkelly@stblaw.com

David Nicolardi
+1-202-636-5571
david.nicolardi@stblaw.com

Nicolas Valderrama
+1-202-636-5960
nicolas.valderrama@stblaw.com

NEW YORK CITY

Meredith J. Abrams
+1-212-455-3095
meredith.abrams@stblaw.com

Manny M. Halberstam
+1-212-455-2388
manny.halberstam@stblaw.com

William LeBas
+1-212-455-2617
william.lebas@stblaw.com

Jeffrey Caretsky
+1-212-455-7764
jeffrey.caretsky@stblaw.com

Margaret Foster
+1-212-455-3622
margaret.foster@stblaw.com

Humza Rizvi
+1-212-455-7654
humza.rizvi@stblaw.com