Skadden

SEC Reporting & Compliance Alert

May 23, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Ave., N.W.
Washington, D.C. 20005
202.371.7000

155 N. Wacker Dr.
Chicago, IL 60606
312.407.0700

SEC Amends Reg S-P To Strengthen Data Breach Response Requirements and Protect Investor Information

On May 16, 2024, the Securities and Exchange Commission (SEC) announced the adoption of amendments to Regulation S-P (Reg S-P), which broadly track the changes originally proposed in March 2023. The revised Reg S-P requires that covered institutions:

- Adopt written policies and procedures establishing an incident response program.
- Notify impacted customers of data breaches.
- Keep records of written incident response programs, agreements with service providers, and documents regarding data breaches and the subsequent notification processes.
- Implement the amendments' new requirements within 18 months for larger entities or 24 months for smaller entities.

Several definitional changes also somewhat expand Reg S-P's scope.[1]

Incident Response Program

The final safeguards rule requires covered institutions to develop written policies and procedures for an incident response program to detect and respond to unauthorized access to customer information. §248.30(a)(3). This response program must include procedures for the covered institution to:

- **Assess the nature and scope of an incident** involving unauthorized access or use of customer information and identify customer information that may have been accessed or used without authorization. §248.30(a)(3)(i).
- **Contain and control the incident** to prevent further unauthorized access or use of customer information. §248.30(a)(3)(ii).
- **Notify each affected individual** whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. §248.30(a)(3)(iii).

The Adopting Release for the Reg S-P amendments notes that covered institutions should develop policies and procedures suited to their size, complexity, and the nature and scope of their activities. Adopting Release at 19. Therefore, the SEC declined to provide further detail on what steps the incident response program must contain, which individuals must undertake oversight responsibilities, and how frequently the incident response program must be updated.

[1] The scope of the safeguards rule (which requires written policies and procedures to safeguard customer records) and disposal rule (which requires proper disposal of consumer report information) are also expanded to cover all "customer information" — a newly defined term under the amendments. In addition, "covered institution" now extends to transfer agents.

SEC Amends Reg S-P To Strengthen Data Breach Response Requirements and Protect Investor Information

Customer Notification Requirement

Because the impact of data breaches on the financial industry has "transformed substantially" since Reg S-P was first released in 2000, SEC Chair Gary Gensler said in a statement, the amendments introduce a customer notification requirement into the safeguard rule. §248.30(a)(4). Covered institutions must provide clear and conspicuous notice, or ensure that such notice is provided, to each affected individual whose sensitive customer information was (or is reasonably likely to have been) accessed or used without authorization.

The amended regulation provides further detail on the nature and timing of customer notification:

- **Sensitive customer information.** Notification is required where there has been an actual or likely compromise of individuals' "sensitive customer information," which is a subset of customer information generally. Sensitive customer information is defined as any customer information "the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information." §248.30(d)(9)(i).
- **Risk of harm.** There is no obligation to notify customers if a covered institution determines "after a reasonable investigation of the facts and circumstances of the incident ... 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." §248.30(a)(4)(i). While the finalized amended Reg S-P does not define "substantial harm or inconvenience," the Adopting Release explained that "[d]etermining whether a given harm or inconvenience rises to the level of a substantial harm or a substantial inconvenience would depend on the particular facts and circumstances surrounding an incident." Adopting Release at 48-49. Though not incorporated in the finalized version, the definition suggested in the proposed amendments may still offer guidance on the types of harm and inconvenience that may require notification (*e.g.*, theft, fraud, harassment, physical harm, impersonation, intimidation, damaged reputation, impaired eligibility for credit, or misuse of an individual's information to obtain a financial product or service or to misuse the individual's account).
- **Affected individuals.** The population of affected individuals requiring notification is defined broadly under the amended Reg S-P. The definition of "customer information" includes "any record containing nonpublic personal information as defined in final rule 248.3(t) about a customer of a financial institution," which includes "personally identifiable financial information" as well as "any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available information." §248.30(d)(5)(i). The rules apply to customer information regardless of whether it pertains to individuals with whom the covered institution itself has a customer relationship. Where the covered institution cannot identify which specific individuals' customer information has been accessed, it must provide notice to all individuals whose sensitive customer information resided on the system that was accessed (or likely accessed) without authorization. However, conversely, notification is not required if the covered institution reasonably determines that the individual's sensitive customer information was not accessed or used without authorization. §248.30(a)(4)(ii).
- **Timing.** Covered institutions must provide individual notices as soon as reasonably practicable, but not later than 30 days after becoming aware that unauthorized access to or use of customer information has occurred or is likely to have occurred. Covered institutions may delay providing required notices but only if the SEC receives a written request from the U.S. Attorney General that such notices pose a substantial risk to national security or public safety. §248.30(a)(4)(iii).
- **Notice contents.** Amended Reg S-P directs the contents of customer notifications, including the nature and date of the incident, the data involved, and multiple means for the affected individuals to contact the covered institution. The amendments also require notices to detail how affected individuals can respond to the incident to protect themselves with recommendations that customers review account statements, report suspicious activity, place a fraud alert in their credit reports, periodically obtain credit reports free of charge, and review guidance from the Federal Trade Commission to protect against identity theft. §248.30(a)(4)(iv).

Service Providers

Amended Reg S-P requires covered institutions' incident response programs to include written policies and procedures "reasonably designed to require oversight, including through due diligence and monitoring, of service providers." §248.30(a)(5). Specifically, the policies and procedures must be reasonably designed to ensure service providers take appropriate measures to "(A) Protect against unauthorized access to or use of customer information; and (B) 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." §248.30(a)(5)(i).

A service provider is "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." §248.30(d)(10).

SEC Amends Reg S-P To Strengthen Data Breach Response Requirements and Protect Investor Information

Recordkeeping and Annual Privacy Notice

The amendments require covered institutions to make and maintain written records documenting compliance with the requirements of the safeguards rule and disposal rule. §248.30(c). While the retention period varies based on the type of institution, it tracks with existing required retention periods for each type of entity. Covered institutions must make and maintain:

- Written policies and procedures required to be adopted and implemented (i) pursuant to the Safeguards Rule, including the incident response program, (ii) pursuant to the Disposal Rule, and (iii) as part of service provider oversight.
- Written documentation of:
    i. Any detected unauthorized access to or use of customer information, as well as any response to and recovery from such unauthorized access to or use of customer information required by the incident response program.
    ii. Any investigation and determination made regarding whether notification to customers is required, including the basis for any determination made and any written.
    iii. Any communication from the U.S. Attorney General related to a delay in notice.
    iv. Any contract entered into pursuant to the service provider oversight requirements.

Also, the amendments modify Reg S-P's existing annual privacy notice delivery provisions to provide an exception to the requirement to conform with the Consumer Finance Protection Bureau's Regulation P. A covered institution is not required to deliver an annual privacy notice if it (a) only provides non-public personal information to non-affiliated third parties when an exception to third-party opt-out applies and (b) has not changed its policies and practices with regard to disclosing non-public personal information from its most recent disclosure sent to customers. §248.5(e)(1)(i) and (ii).

Implementation

The amendments will become effective 60 days after publication in the Federal Register. Larger entities (*e.g.*, investment companies with $1 billion or more in net assets or registered investment advisors with $1.5 billion or more in assets under management) will have 18 months after the date of publication in the Federal Register to comply with the new requirements. Smaller entities will have 24 months after the date of publication to comply.

Takeaways

- **Review and update policies, procedures and service provider agreements.** Covered institutions should review the amendments against their existing (i) privacy, incident response, and information security policies, (ii) incident notification procedures, and (iii) service provider agreements to ensure compliance by each entity's compliance date.
- **Focus on recordkeeping and retention.** Compliance with Reg S-P requires making and maintaining an enumerated list of books and records. Each covered institution should check its retention schedules and update as necessary.
- **Ensure compliance.** The amendments serve as yet another example of the SEC's continuing focus on cybersecurity issues, including the adequacy and compliance of firms' programs. After updating, covered institutions should ensure enforcement of their own policies and procedures.
- **Consider state laws as well.** While many of Reg S-P's requirements correspond to state data breach laws that apply to businesses broadly, the state laws vary in their details, and compliance with the revised Reg S-P will not necessarily satisfy state requirements.

Contacts

Brian V. Breheny
Partner / Washington, D.C.
202.371.7180
brian.breheny@skadden.com

Daniel Michael
Partner / New York
212.735.2200
daniel.michael@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Kyle G. Kysela
Associate / Chicago
312.407.0546
kyle.kysela@skadden.com

Emma Hlavin
Associate / Chicago
312.407.0610
emma.hlavin@skadden.com