Amendments to Regulation S-P Create New Cybersecurity Requirements for Financial Institutions

June 5, 2024 Kit Addleman, Kurt Gottschall, Tim Newman

PRACTICES Fund Formation and Management, Privacy and Cybersecurity, Securities and Shareholder Litigation

The Securities and Exchange Commission adopted amendments to Regulation S-P on May 15, 2024, to govern the handling of customers' nonpublic personal information by certain financial institutions.

The amendments apply to an expanded set of financial institutions including broker-dealers, funding portals, investment companies, registered investment advisers and transfer agents (collectively, "covered institutions"), and are designed to provide updates to "help protect the privacy of customers' financial data."[1] The changes require covered institutions to create or revise written incident-response programs and to notify affected individuals following a breach of sensitive customer information. The amendments also expand the recordkeeping requirements of Regulation S-P, institute additional obligations regarding service providers and confirm a carve-out to covered institutions' annual privacy-notice obligations.

Written Policies and Procedures Concerning Incident Response. The amendments require covered institutions to develop, implement, and maintain written policies and procedures that are "reasonably designed to detect, respond to, and recover from both unauthorized access to and unauthorized use of customer information."[2] The amendments do not prescribe specific steps to take when carrying out incident response activities so covered institutions can create "policies and procedures best suited to their particular circumstances."[3] However, the amendments require that incident response programs include written policies and procedures for:

- "[a]ssess[ing] the nature and scope of any incident involving unauthorized access to or use of customer information and identify[ing] the customer information systems and types of customer information that may have been accessed or used without authorization;"
- "[t]ake[ing] appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information; and
- notifying affected individuals as required by the amendments.[4]

Customer Notification Requirements. Incident response programs must include written policies and procedures for providing notice to "affected individual[s] whose sensitive customer information was, or was reasonably likely to have been, accessed or used without authorization."[5] The amendments provide additional details on the logistics of notification, including:

- **When Notice is Required:** Notice must be provided when "sensitive customer information" has been accessed or used. The amendments define "sensitive customer information" to mean "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."[6] While the amendments provide some examples of sensitive customer information (e.g., Social Security Number,

biometric records, and address), they make clear that the threshold "is broader in scope than the various state law notification triggers."[7]

- **To Whom Notice is Required:** Notice must be provided to "all individuals whose sensitive customer information resides in the customer information system that was, or was reasonably likely to have been, accessed without authorization."[8] While notification must be made to all affected individuals with a customer relationship with the covered institution, notice must also be provided to "customers of other financial institutions where such information has been provided to the covered institution."[9] In addition, if the covered institution cannot precisely determine the affected individuals, it "must provide notice to all individuals whose sensitive customer information resides in the customer information system."[10]
- **Timing of Notice:** Covered institutions must provide notice to affected individuals "as soon as practicable, but not later than 30 days, after becoming aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred."[11]
- **Method of Notice:** Covered institutions must provide "clear and conspicuous notice" to affected individuals "by a means designed to ensure that the individual can reasonably be expected to receive actual notice in writing."[12] The notice must also include, among other things, a description and timing of the incident and type of information accessed, contact information for the covered institution, and how the individual may obtain a credit report free of charge.[13]

"The final amendments reflect a presumption of notification."[14] However, notice is not required if a covered institution determines, after a reasonable investigation, "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."[15]

Additional Amendments

In addition to the requirements above, the amendments institute several other obligations. First, covered institutions must "establish and maintain written records documenting compliance with the [requirements] of Regulation S-P."[16] The retention period depends on the type of covered institution (e.g., investment adviser vs. broker-dealer) and the records at issue (e.g., policies and procedures vs. other records) and ranges from three to six years.[17]

The amendments also require covered institutions' written incident response programs to be designed to require oversight and monitoring of service providers.[18] The processes and procedures must be designed to ensure service providers take appropriate measures to (i) protect against incidents related to customer information and (ii) 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.[19]

Finally, the amendments create an exception to the requirement that covered institutions provide customers with annual notices informing them about the institutions' privacy practices. Currently, if certain conditions are met, covered institutions are exempt from this requirement.[20]

Expanded Scope and Coverage

SEC Chair Gary Gensler summarized the amendments to Regulation S-P by stating that "[t]he basic idea for covered firms is if you've got a breach, then you've got to notify."[21] But it's not that simple. The amendments also expanded the scope of Regulation S-P in three key ways.

1. First, the amendments apply to nonpublic personal information a covered institution collects from its own customers, as well as nonpublic personal information received from another financial institution.[22]
2. The amendments also expand the list of covered institutions to include transfer agents registered with the SEC or another appropriate regulatory agency.[23]
3. Finally, the definition of "sensitive customer information" is broadly defined and does not include an exhaustive list of what constitutes sensitive customer information.[24]

Takeaways

In light of these amendments, covered institutions should review their written incident response plans for compliance or, if necessary, create such written programs. Given the technical and prescriptive nature of the requirements (e.g., that written policies are reasonably designed to detect, respond to, and recover from cybersecurity incidents), covered institutions should consider whether to retain cybersecurity professionals in crafting such policies. In addition, if and when data incidents occur, covered institutions should be prepared to notify affected individuals in accordance with the amendments and other applicable law.

Larger entities will have 18 months after the date of publication in the Federal Register to comply with the amendments, and smaller entities will have 24 months after the date of publication in the Federal Register to comply. Despite these lead times, covered institutions should begin to evaluate and implement necessary changes today.

For more information or assistance with Regulation S-P or other securities or privacy laws, contact one of the Haynes Boone lawyers below.

---

[1] SEC Press Release 2024-58.
[2] 17 CFR § 248.30(a)(3).
[3] Final Rule: Discussion, 18.
[4] 17 CFR § 248.30(a)(3).
[5] 17 CRF § 248.30(a)(4)(i).
[6] 17 CFR § 248.30(d)(9).
[7] Final Rule: Discussion, 232.
[8] 17 CFR § 248.30(a)(4)(ii).
[9] 17 CFR § 248.30(d)(5)(i).
[10] 17 CFR § 248.30(a)(4)(ii).
[11] 17 CFR § 248.30(a)(4)(iii).
[12] 17 CFR § 248.30(a)(4)(i).
[13] 17 CFR § 248.30(a)(4)(iv).
[14] Final Rule: Discussion, 25.
[15] 17 CFR § 248.30(a)(4)(i).

[16] Final Rule: Discussion, 121-22.

[17] Final Rule: Discussion, 121-22.

[18] The amendments define service provider 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." 17 CFR § 248.30(d)(10).

[19] 17 CFR § 248.30(a)(5)(i).

[20] 17 CFR § 248.5(e)(1)(i) and (ii).

[21] SEC Press Release 2024-58.

[22] 17 CFR § 248.30(d)(5)(i).

[23] 17 CFR § 248.30(d)(3).

[24] 17 CFR § 248.30(d)(9).