The SEC Adopts Significant Cybersecurity Amendments to Reg S-P

May 17, 2024

On May 16, 2024, the SEC adopted amendments to Regulation S-P ("Reg S-P") one year after its proposed amendments (the "Proposed Amendments"). The finalized amendments ("Amended Reg S-P") largely track the Proposed Amendments and include significant requirements related to (1) incident response programs, (2) 30-day customer notifications of data breaches, (3) service provider oversight, (4) the scope of the Safeguards and Disposal Rules, (5) recordkeeping, and (6) an exception to the annual privacy notice requirement. Firms will have either 18 or 24 months (depending on size) from the date of publication in the Federal Register to come into compliance.

Since its initial adoption in 2000, Reg S-P has required broker-dealers, investment companies and registered investment advisers ("Covered Institutions")[1] to adopt written policies and procedures to safeguard customer records and information (the "Safeguards Rule") and to properly dispose of consumer report information (the "Disposal Rule"). Amended Reg S-P represents a substantial expansion of the protections available to the customers of institutional securities market participants under the federal securities laws and establishes a new federal minimum standard for data breach notification at such firms. We discuss Reg S-P's new and expanded requirements, as well as considerations for compliance, below.

A comparison of Amended Reg S-P to the Proposed Amendments is available here.

Incident Response Program

Amended Reg S-P now requires Covered Institutions' safeguards policies and procedures to include 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)(3). The requirements for an incident response program were finalized as

[1] The amendments to Reg S-P expand the definition of "Covered Institution" to include transfer agents. Additionally, while private funds are explicitly excluded from the definition, registered investment advisers that are advisers to private funds are in scope.

proposed (with some changes made to the specifics of the individual notification requirement, discussed below). Covered Institutions' incident response programs must include the following procedures:

- *Assessment*: To assess the nature and scope of any incident and to identify the customer information systems and types of customer information that may have been accessed or used without authorization. § 248.30(a)(3)(i).

- *Contain and Control*: To take appropriate steps to contain and control an incident to prevent further unauthorized access to or use of customer information. § 248.30(a)(3)(ii).

- *Notification*: To 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 Amended Reg S-P provides little detail on what an incident response program must contain, instead stating that Covered Institutions "may tailor their policies and procedures to their individual facts and circumstances." Adopting Release at 19-20. While Amended Reg S-P does not mandate how frequently incident response programs should be updated, the Adopting Release notes that Covered Institutions should "consider reviewing and updating the containment and control procedures periodically to ensure that the procedures remain reasonably designed." Adopting Release at 23.

Customer Notification

Amended Reg S-P establishes "a Federal minimum standard for covered institutions to provide data breach notifications to affected individuals." Fact Sheet at 1. The final rule provides that Covered Institutions must notify affected individuals "whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization." § 248.30(a)(4)(i). Amended Reg S-P provides for a "presumption of notification" but also allows a Covered Institution to not notify if it determines, following 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." § 248.30(a)(4)(i).

- *Sensitive Customer Information*: Sensitive customer information is a subset of customer information, the compromise of which would present a reasonably likely risk of substantial harm or inconvenience to an individual identified with the

information. Amended Reg S-P provides a nonexhaustive list of sensitive customer information in two categories. The first category is information that can be uniquely identified with an individual (like a Social Security Number or biometric identifiers). Second, sensitive customer information includes information that could be used to gain access to an account (*e.g.*, user name in conjunction with password or mother's maiden name).

- *Covered Customers*. As discussed in more detail below, Amended Reg S-P expands the definition of "customer information" to include not only information of individuals with whom the Covered Institution has a customer relationship, but also information about "the customers of other financial institutions where such information has been provided to the covered institution." Accordingly, Covered Institutions are expected to notify affected individuals even when they do not have a customer relationship with them.

- *Risk of Harm*. Notification is not required if the Covered Institution determines "after a reasonable investigation of the facts and circumstances of the incident . . . that sensitive customer information has not been, or 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 Proposed Amendments defined "substantial harm or inconvenience," Amended Reg S-P removed these definitions. Instead, as explained in the Adopting Release, "[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. While the finalized amendments provide more flexibility for analysis, the definition in the Proposed Amendments may still be instructive as to the types of harm and inconvenience that might potentially 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*. In line with its "presumption of notification," Amended Reg S-P retains the expansive characterization of "affected individuals" from the Proposed Amendments. *See* § 248.30(a)(4)(ii). Under this approach, notification is necessary even if the Covered Institution is unable to identify which specific individuals' sensitive customer information has been accessed or used without authorization. In such circumstances, the Covered Institution must provide notice 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. However, unlike the Proposed Amendments, Amended Reg S-P clarifies that Covered Institutions need not provide individual notices if they reasonably determine that a specific individual's sensitive customer information that resides on

the customer information system was not accessed or used without authorization. § 248.30(a)(4)(ii).

- *Timing*. Amended Reg S-P maintains the Proposed Amendments' requirement that Covered Institutions provide individual notices within 30 days of becoming aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred. § 248.30(a)(4)(iii). While the trigger for notification is tied to the compromise of "sensitive customer information," the 30-day clock starts at a Covered Institution's awareness of any unauthorized access to or use of customer information.

- *National Security & Public Safety Delay*. Under Amended Reg S-P, notification may be delayed for up to 30 days (with extensions for extraordinary circumstances) for either national security or public safety concerns, subject to a determination from the United States Attorney General, which, in practice, will likely be relied upon only in narrow circumstances.

- *Method and Content of Notification*. Amended Reg S-P does not prescribe how notifications must be sent to customers. It only specifies that "notice must be transmitted by a means designed to ensure that each affected individual can reasonably be expected to receive actual notice in writing." § 248.30(a)(4)(i). Amended Reg S-P dictates the contents of the notification to customers, including the nature and date of the incident, the data involved, and multiple means for the affected individuals to contact the Covered Institution.

Service Provider Oversight

Under Amended Reg S-P, Covered Institutions' incident response programs must include policies and procedures "reasonably designed to require oversight, including through due diligence on and monitoring, of service providers," including to ensure the Covered Institution meets its customer notification requirements. Amended Reg S-P defines "service provider" as "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). These 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).

Amended Reg S-P has removed the Proposed Amendment's requirement that these measures be provided for in a contract, although the Adopting Proposal notes that Covered Institutions "should generally consider whether a written contract that memorializes the expectations of both covered institutions and their service providers is appropriate." Adopting Release at 75, n. 233. Further, as discussed below, the Amended Reg S-P's recordkeeping requirements include a requirement for Covered Institutions to maintain "written documentation of any contract or agreement entered into pursuant to § 248.30(a)(5)." §§ 240.17a-4(e)(14(v) 240.17ad-7(k)(5), 270.31a-1(b)(13)(v), 275.204-2(a)(25)(v).

Expanded Scope of Safeguards and Disposal Rules

Amended Reg S-P expands the reach of the Safeguards and Disposal Rules in several ways. First, it increases the scope of information covered by those rules. Second, it extends the applicability of those rules to cover transfer agents.

With Amended Reg S-P, the SEC expanded the scope of information covered by the Safeguards and Disposal Rules by adjusting the definition of "customer information." The definition of "customer information" now includes "information in the possession of a covered institution or information that is handled or maintained by the covered institution or on its behalf, regardless of whether such information pertains to (a) individuals with whom the covered institution has a customer relationship or (b) the customers of other financial institutions where such information has been provided to the covered institution." § 248.30(d)(5)(i).

This means that the Safeguards and Disposal Rules now cover customer information received by Covered Institutions from third-party financial institutions, as well as customer information even when an individual no longer has a customer relationship with the Covered Institution. For example, information that a registered investment adviser receives from the custodian of a former client's assets is covered under the Safeguard and Disposal Rules if the former client remains a customer of either the custodian or of another financial institution, even though the individual no longer has a customer relationship with the investment adviser. Adopting Release at 99. This expanded definition impacts both the new notification requirements and also existing requirements to protect customer data and dispose of it securely.

Amended Reg S-P also extends the Safeguards and Disposal Rules to apply to any transfer agent registered with the SEC or another appropriate regulatory agency. The modifications to the definition of "customer information" described above extend to transfer agents for purposes of the Safeguards and Disposal Rules.

Recordkeeping

With these new regulatory requirements comes a set of new requirements for books and records. While the books and records that each type of Covered Institution is required to keep under Amended Reg S-P are the same, the retention period varies based on the type of Covered Institution and tracks the existing required retention periods for each type of entity. These new recordkeeping requirements include making and maintaining:

- Written policies and procedures required to be adopted and implemented pursuant to the Safeguards Rule, including the incident response program;
- Written documentation of 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;
- Written documentation of any investigation and determination made regarding whether notification to customers is required, including the basis for any determination made and any written documentation from the United States Attorney General related to a delay in notice, as well as a copy of any notice transmitted following such determination;
- Written policies and procedures required as part of service provider oversight;
- 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 for the Disposal Rule.

Annual Privacy Notice

Amended Reg S-P provides an exception to the annual privacy notice already required by Reg S-P, provided certain requirements are met. This brings Amended Reg S-P in line with the CFPB's Regulation P. To qualify for the exception, a Covered Institution (1) must only provide non-public personal information to non-affiliated third parties when an exception to third-party opt-out applies and (2) may not have 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).

Compliance Period

Large entities have 18 months after the date of publication in the Federal Register to comply with Amended Reg S-P and smaller entities have 24 months. The Adopting Release provides the following qualifications for different entities to be considered a "larger entity:"

- Investment companies that, together with other investment companies in the same group of related investment companies, have net assets of $1 billion or more as of the end of the most recent fiscal year.
- Registered investment advisers: $1.5 billion or more in assets under management.
- Broker-dealers: All broker-dealers that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act.
- Transfer agents: All transfer agents that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act.

Takeaways

- *Review and Update Policies and Procedures for Upcoming Compliance Dates*. Covered Institutions will want to begin reviewing and updating their policies and procedures to be ready for these compliance dates. This should include updates to existing safeguards and disposal policies to account for the expanded definition of "customer information," updates to incident response programs and updates to vendor risk management policies and procedures.
- *Assess Competing Incident Notification Requirements*. Amended Reg S-P provides another requirement in the patchwork of notifications that Covered Institutions face from other federal and state regulations. Integrating the Amended Reg S-P requirement into existing notification considerations and understanding how it interacts with other notification obligations will be key to successful incident response.
- *Identify and Update Service Provider Arrangements*. Identify the service providers in scope under Amended Reg S-P and review existing contracts or other agreements to ensure there is sufficient oversight in place for compliance. To the extent updates are necessary, determine whether changes need to be made to existing contracts or whether there are other means of oversight that satisfy Amended Reg S-P. Consider

updating standard contract provisions to ensure appropriate oversight provisions for new service providers going forward.

- *Update Retention Schedules*. Ensure that books and records generated by Amended Reg S-P compliance efforts are appropriately maintained and that any retention schedules are updated accordingly.

- *Consider Enhanced Logging and Auditing Tools.* The broad definition of affected individuals will expand potential notification obligations. Ensure robust logging and auditing of email and file access to assess notification obligations.

- *Considerations for Private Fund Advisers*. The Adopting Release's ambiguous guidance for private fund advisers means that such advisers may wish to consider whether to establish incident notification programs for natural person investors even though Amended Reg S-P does not apply to private funds, and an investor in a private fund may not as a matter of law be a "customer" of the private fund's adviser. Amended Reg S-P reaffirms the Commission's longstanding guidance that Reg S-P does not apply to private funds. Adopting Release at 5 n.2. Nonetheless, the Adopting Release states that registered investment advisers to private funds are Covered Institutions under Amended Reg S-P and posits that private funds themselves may be subject to the FTC Safeguards Rule's breach notification requirements. Adopting Release at 181-182, 202 n.614. As a result, as a practical matter private fund advisers may hold data about natural person investors that is equivalent to "customer information" under Amended Reg S-P. For this reason, as a prudential matter, a private fund adviser that experiences a breach of natural person investor information may wish to consider whether and how to notify natural person investors of such a breach. Moreover, private fund advisers may already be subject to state law, GDPR and FTC Safeguards Rule breach notification requirements for the natural person investors in the private funds they advise. For this reason, private fund advisers that possess the equivalent of "customer information" for their natural person investors may wish to consider whether to adopt an incident response and notification plan consistent with the requirements of Amended Reg S-P.

- *To subscribe to the Data Blog, please* click here.

* * *

Please do not hesitate to contact us with any questions.

Charu A. Chandrasekhar
Partner, New York
+ 1 212 909 6774
cchandrasekhar@debevoise.com

Luke Dembosky
Partner, Washington, D.C.
+1 202 383 8020
ldembosky@debevoise.com

Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com

Erez Liebermann
Partner, New York
+1 212 909 6224
eliebermann@debevoise.com

Marc Ponchione
Partner, Washington, D.C.
+1 202 383 8290
mponchione@debevoise.com

Julie M. Riewe
Partner, Washington, D.C.
San Francisco
+1 202 383 8070
jriewe@debevoise.com

Jeff Robins
Partner, New York
+1 212 909 6526
jlrobins@debevoise.com

Kristin A. Snyder
Partner, San Francisco
+1 415 738 5718
kasnyder@debevoise.com

Anna Moody
Counsel, Washington, D.C.
+1 202 383 8017
moody@debevoise.com

Sheena Paul
Counsel, Washington, D.C.
+1 202 383 8178
spaul@debevoise.com

Johanna N. Skrzypczyk
Counsel, New York
+1 212 909 6291
jnskrzypczyk@debevoise.com

Suchita Mandavilli Brundage
Associate, New York
+1 212 909 6486
smbrundage@debevoise.com

Ned Terrace
Associate, New York
+1 212 909 7435
jkterrac@debevoise.com