SEC Adopts Information Security and Notification Amendments to Regulation S-P

12 June 2024

On May 16, 2024, the Securities and Exchange Commission ("SEC") announced that it had adopted amendments ("Amendments")[1] to Regulation S-P ("Reg S-P")[2]. The SEC explained that the Amendments represent an effort to "modernize and enhance" rules designed to protect consumers' nonpublic information and privacy. The rules create new requirements for "covered institutions," which include brokers or dealers ("broker-dealers") and registered investment advisers ("RIAs").[3]

The Amendments will require, among other things, broker-dealers and RIAs (1) to develop, implement and maintain written policies and procedures for an incident response plan, (2) to develop written policies and procedures reasonably designed to require service provider oversight and (3) to provide notice to customers within 30 days in the event that "sensitive customer information" is compromised. The Amendments also broaden the scope of information covered by Reg S-P, implement additional recordkeeping obligations for covered institutions, and provide an exception to the annual privacy notice delivery requirement.

The Amendments will become effective on Aug. 2, 2024, when any RIA with $1.5 billion or more in assets under management and any broker-dealer that is not a small entity under the Securities Exchange Act of 1934, as amended ("Exchange Act"), for purposes of the Regulatory Flexibility Act will have 18 months to comply. RIAs with less than $1.5 billion in assets under management and other broker-dealers will have 24 months to comply.

New Obligations for Broker Dealers and RIAs

Incident Response Plan. The Amendments will require that broker-dealers and RIAs "develop, implement, and maintain written policies and procedures for an incident response program that is reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information."[4] The Amendments do not prescribe specific steps for response plans, but a response plan must include certain general elements, including procedures "to assess the nature and scope of any incident and to take appropriate steps to contain and control the incident to prevent further unauthorized access."[5] Covered institutions will be required to maintain written documentation of any detected breach, as well as any related response and recovery, under the Amendments' recordkeeping obligations described below.

Further, incident response plans must include procedures to notify individuals whose sensitive customer information was, or is reasonably likely to have been accessed or used without authorization (in each instance a "breach" as used in this alert) in accordance with a covered institution's notification obligations under the Amendments.[6] Incident response plans must also include written policies and procedures to require service provider oversight as further described below.

Service Provider Oversight. The Amendments require that incident response plans include, "written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring," of service providers[7] and to ensure that applicable notification requirements are carried out in the event of a breach at the service provider.[8] The Amendments require that broker-dealers and RIAs ensure service providers take measures to "(A) protect against unauthorized access to or use of customer information, and (B) provide

notification to the covered institution in the event of a breach resulting in unauthorized access to a customer information system maintained by the service provider," as soon as possible but no later than 72 hours after becoming aware of a breach, in order to allow covered institutions to carry out their own incident response plans and notice obligations, to the extent they have any.[9] Service provider oversight may include independent certifications and attestations obtained from service providers as part of due diligence and monitoring but ultimately oversight remains a risk-based analysis and should generally be tailored to the facts and circumstances of each service provider relationship.[10]

Customer Notification Requirements. Broker-dealers and RIAs will be required to provide clear and conspicuous written notice, or ensure that such notice is provided, to affected individuals[11] whose sensitive customer information[12] was, or was reasonably likely to have been, accessed or used without authorization. While the requirement in the Amendments is to adopt an incident response plan that addresses unauthorized access to or use of *customer information*, the notification requirement only applies to *sensitive customer information* that has been, or is reasonably likely to be, used in a manner that would result in substantial harm or inconvenience (i.e., the notification requirement is narrower than the plan requirement). Covered institutions must provide notice to customers as soon as practicable, but no 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."[13] Note, in the event that a covered institution experiences a breach affecting another covered institution's customers, the covered institution that experienced the breach may meet its notice obligation by "ensur[ing] that such notice is provided" by coordinating with the other covered institution to determine that only one of the covered institutions will provide the notice.[14] Such notice must include, among other things, a description of the incident and the type of information that was accessed or used without authorization, relevant or estimated dates of the incident and contact information to inquire about the incident.[15]

There is a presumption in the Amendments that notification is required, and notification may only be avoided if covered institutions determine, after a reasonable investigation of the breach, 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."[16] The determination must be conclusive.[17] Accordingly, after becoming aware of that a breach occurred, or was reasonably likely to have occurred, covered institutions will have 30 days to conduct an investigation, and if determined necessary, provide notice to affected individuals.[18] Note, while the Amendments require notice no later than 30 days after the "becoming aware" trigger, notice may be required earlier if, based on the facts and circumstances of the incident, notice is practicable earlier (e.g., a few days).[19] Certain factors are applicable, including "the time required to assess, contain, and control the incident."[20]

Determining whether a harm or inconvenience caused by a breach is "substantial" requires a facts and circumstances analysis. The Amendments do not define "substantial harm or inconvenience;" however, harms or inconveniences provided in the Proposed Amendments like "personal injury, financial loss, expenditure of effort, or loss of time" or "theft, fraud, harassment, physical harm, impersonation, intimidation, damaged reputation, or impaired eligibility for credit", among others, may be a starting point for a covered institution's determination.[21] Lastly, for any determination that notice is not required, the deciding broker-dealer or RIA must maintain a record of the investigation and the basis for its determination that notice to customers was not warranted.[22] Such records should support that the investigation was reasonable (i.e., outlining the nature and scope of the breach, including whether the breach was the result of an intentional external intrusion or an inadvertent internal unauthorized employee, the overall duration of the incident, the accounts and information compromised, etc.).[23]

Customer Notification of Service Provider Breaches. Broker-dealers and RIAs will be required to provide customers with notice, or ensure notice, of a breach of one of its service providers that is not itself a covered institution. The Amendments provide that covered institutions "may enter into a written agreement with [] service

provider[s] to notify affected individuals on [a] covered institution's behalf".[24] However, the Amendments make clear that the obligation to ensure affected individuals are notified in accordance with the Amendments' notice requirements remains with the covered institution.[25] Accordingly, broker-dealers and RIAs may need to conduct due diligence to confirm service providers have provided sufficient notice. This may include maintaining or requesting copies of notices provided to customers by service providers, request certifications or attestations regarding notifications from service providers or, among other things, test that service providers have given notice by confirming delivery of notice from customers.[26]

Scope of Information Covered by Reg S-P. The Amendments expand the scope of information covered by Reg S-P. The new defined term "customer information" applies Reg S-P to personal information regardless of a client relationship – meaning not only is a covered institution's own customer information in scope, but also the customer information of other financial institutions[27] whose information has been provided to the covered institution.[28] This amendment brings consistency to the information currently protected under Reg S-P's safeguards and disposal rules.

Annual Privacy Notice Delivery Exception. The Amendments also include an exception to the requirement to deliver a privacy notice on an annual basis if the covered institution (1) only discloses non-public personal information to non-affiliated third parties in accordance with exceptions to the requirement that consumers must be given certain rights to opt out of such disclosure or notice[29] and (2) it has not changed its policies and practices regarding the disclosure of non-public personal information from its most recently delivered notice.

Recordkeeping Obligations. The Amendments require certain recording keeping obligations, including, but not limited, to covered institutions' written policies and procedures established under the Amendments, written documentation of any detected breach, as well as any related response and recovery, investigation and determination regarding the covered institution's notice obligation related to a breach. A covered institution's recordkeeping obligations also extend to policies and procedures established to oversee, monitor and conduct due diligence on service providers and any written documentation of any related service provider agreements.

Implementation Timeline

A "Larger Entity" will need to comply with the Amendments by Feb. 2, 2026, 18 months following the Amendments' effective date on Aug. 2, 2024. Any RIA with $1.5 billion or more in assets under management is considered a larger entity. All broker-dealers that are not small entities under the Exchange Act for purposes of the Regulatory Flexibility Act will be considered a larger entity for purposes of compliance with the Amendments. All other broker-dealers and RIAs will be considered a "Smaller Entity" and will need to comply by Aug. 2, 2026, 24 months following the Amendments' effective date.

Next Steps for Broker-Dealers and RIAs

With compliance dates ranging from 18 to 24 months following publication of the Amendments, broker-dealers and RIAs should begin work to understand their obligations and how their current compliance framework will need to change under the revised rules. Such steps should include:

- Reviewing and revising incident response plans to meet the policy and procedure and notification requirements under the Amendments. Many broker-dealers and RIAs have already implemented incident response plans that might need to be updated in light of the changes. A review of whether your organization's incident response plan is reasonably designed to detect, respond and recover from a breach should take place, including whether the plan is easy for employees to understand and carry out when faced with a breach.

- Assessing existing policies and procedures regarding internal access to customer information, including assessments of the firm's processes and procedures for approving access to customer information and periodic assessments of existing permissioning.
- Due to the 30-day notice requirement in the Amendments, covered institutions should identify mechanisms for providing notice to customers and make sure those mechanisms are available and can be used quickly, if needed.
- Develop and enhance policies and procedures for overseeing service providers through due diligence and monitoring. Covered institutions should review service provider due diligence questionnaires to know whether changes are necessary to ensure appropriate measures are in place for covered institutions to meet their Reg S-P obligations.
- Revisit current service provider agreements. While the Amendments do not require written agreements with service providers, a written agreement and certain representations or attestations may facilitate covered institutions' compliance with the Amendments' oversight and notification obligations.
- Ensure that there is a process in place for service provider agreements that are due to be renewed are done so in a manner that accounts for the Amendments' requirements.
- Work to understand the scope of the "customer information" within your organization. Because the Amendments apply to not only a covered institution's own customer information, but also the customer information of other financial institutions, covered institutions should review the customer information that either they, or service providers on their behalf, are in possession of or handle or maintain.

Authored by *William J. Barbera, Kelly Koscuiszka, Philip J. Bezanson, Tarik M. Shah* and *Cody A. Lind.*

If you have any questions concerning this *Alert*, please contact your attorney at Schulte Roth & Zabel or one of the authors.

---

[1] The amendments were initially proposed in March 2023 ("Proposed Amendments"). *See also* "Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information," Exchange Act No. 34-100155 (May 16, 2024) ("Adopting Release").

[2] Originally adopted in 2000, Reg S-P generally requires proper safeguards for customer nonpublic information through the adoption of written policies and procedures, proper disposal of consumer information and obligations to provide privacy notice and opt-out provisions to customers.

[3] In addition to broker-dealers (including funding portals) and RIAs, the Amendments also apply to investment companies and certain registered transfer agents - collectively, "covered institutions" under the Amendments. Although private funds are not "covered institutions" subject to Reg S-P, the Adopting Release explains that private funds may be subject to the Federal Trade Commission's Safeguards Rule under Regulation P which requires, generally, a comprehensive information security plan that includes an incident response plan as well as requirements related to selecting and retaining service providers. *See* Adopting Release at 5, footnote 2; 181-82.

[4] Adopting Release at 13. The Adopting Release makes clear, both any instance of unauthorized access to and unauthorized use of customer information are considered an "incident" and will trigger a covered institution's incident response program. Adopting Release at 16-7.

[5] Adopting Release at 13.

[6] Adopting Release at 17.

[7] A service provider is defined 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." See

final rule 248.30(d)(10). The Adopting Release makes clear this includes affiliates of covered institutions. *See* Adopting Release at 88.

[8] *See* final rule 248.30(a)(5).

[9] Adopting Release at 71.

[10] Adopting Release at 76.

[11] If unable to identify the specific individuals whose sensitive customer information has been accessed or used, covered institutions must provide notice to all individuals whose sensitive customer information resides on the breached customer information system. *See* Adopting Release at 25.

[12] Notification requirements under the amendments are limited to breaches involving "sensitive customer information" defined 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." *See* final rule 248.30(d)(9). Certain enumerated examples include information uniquely identified with an individual (e.g., social security number, biometric record, routing code, telecommunication identifying information, etc.) and account information in combination with authenticating or access information. *See* final rule 248.30(d)(9)(ii).

[13] *See* final rule 248.30(a)(4)(iii).

[14] *See* final rule 248.30(a)(4).

[15] *See* final rule 248.30(a)(4)(iv).

[16] *See* final rule 248.30(a)(4).

[17] For example, if a covered institution has information that an external actor has gained unauthorized access to sensitive customer information, but lacks information indicating whether any individual's sensitive customer information was or was not used in a manner that would result in substantial harm or inconvenience, the investigation would be inconclusive and would require notice to affected individuals. *See* Adopting Release at 26-7.

[18] Adopting Release at 54.

[19] Adopting Release at 56.

[20] Adopting Release at 56.

[21] Adopting Release at 49.

[22] *See* final rule 275.204-2(a)(25)(iii).

[23] Adopting Release at 26.

[24] *See* final rule 248.30(a)(5)(ii).

[25] *See* final rule 248.30(a)(5)(iii).

[26] *See* Adopting Release at 86-7.

[27] Reg S-P defines “financial institution” generally to mean any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). 17 CFR 248.3(n). Although the definition of “financial institution” is broad, the Adopting Release includes that private funds “are not subject to Reg S-P”. *See* Adopting Release at 5, footnote 2.

[28] “Customer information” includes “any record containing nonpublic personal information as defined in section 248.3(t) about a customer of a financial institution, whether in paper, electronic, or other form, that is in the possession of a covered institution or that is handled or maintained by the covered institution or on its behalf.” *See* final rule 248.30(d)(5)(i). The Adopting Release explains that defining customer information to include “handled or maintained on behalf of a covered institution” expands the scope to a covered institution’s customer information handled or maintained by a service provider. *See* Adopting Release at 97.

[29] Exceptions generally include (1) an exception to opt out requirements for service providers and joint marketing when nonpublic personal information is provided to a nonaffiliated third party to perform services or functions on the covered institution’s behalf, (2) an exception to notice and opt out requirements for processing and servicing transactions where disclosing nonpublic personal information as necessary to effect, administer or enforce a transaction that a consumer requests or authorizes, and (3) other notice and opt out exceptions for specific instances (e.g., with consent, to protect confidentiality, prevent fraud, report to necessary organizations, etc.) as described under 248.15. *See* 17 CFR 248.13-15.
