The Investment Lawyer
Covering Legal and Regulatory Issues of Asset Management
VOL. 32, NO. 2 • FEBRUARY 2025

Understanding the Recent Amendments to Regulation S-P: Key Changes and Implications for Covered Institutions

By Richard Kerr, Sasha Burstein, Brian Doyle-Wenger, and Aster Cheng

On May 16, 2024, the Securities and Exchange Commission (SEC or Commission) adopted amendments to Regulation S-P (Amendments) representing the first major changes to Regulation S-P since its initial adoption in 2000.[1] Recognizing the significant technological advances, including increased reliance on cloud computing and mobile communications,[2] since the rule's adoption, the Amendments impose new privacy-related protections and obligations for firms covered by the rule, including brokers and dealers, investment companies, registered investment advisers, funding portals, and transfer agents registered with the SEC or another appropriate regulatory agency (collectively, Covered Institutions), including: (1) adoption of incident response programs, (2) expansion of Regulation S-P to cover all transfer agents, (3) broadening of the scope of information covered by Regulation S-P, and (4) codifying exceptions to privacy policy delivery obligations.[3] While these Amendments seek to provide new protections for the privacy of customer information, they also create a necessity to review and adopt or modify policies and procedures, and amend contracts with third parties that are ripe with grey areas where covered institutions may reasonably interpret similar matters differently.

History of Regulation S-P

In 1999, Congress passed the Gramm-Leach-Bliley Act (GLBA), which imposed an obligation on "financial institutions" as defined in GLBA[4] to protect the nonpublic personal information of a customer or consumer.[5] In 2000, under authority granted under GLBA, the Commission adopted Regulation S-P, which: (1) requires broker dealers, investment companies, and registered investment advisers to adopt written policies and procedures to safeguard customer records and information (the Safeguards Rule); (2) requires proper disposal of consumer report information in a manner that protects against unauthorized access to or use of such information (the Disposal Rule); and (3) implements privacy policy notice and opt out provisions.[6] Since 2000, Regulation S-P remained largely unchanged, with only minor changes occurring in 2015[7] when Congress amended GLBA by passing the Fixing America's Surface Transportation Act (FAST Act).[8] The FAST Act amendment, titled "Eliminate Privacy Notice Confusion" added Section 503(f) to GLBA, which provided an exception under which financial institutions that meet certain conditions are not required to provide annual privacy notices to customers.[9]

Implementing the Amendments

In light of the Amendments and the impending effective date of December 3, 2025 or June 3, 2026 depending on the size of the institution,[10] Covered Institutions should consider taking steps now to implement the Amendments as we describe below.

Reviewing Existing Policies and Procedures

Among the new requirements imposed by the Amendments, is a requirement that Covered Institutions adopt an incident response program that addresses unauthorized access to or use of customer information and includes customer[11] notification procedures. Each Covered Institution's incident response program must have written policies and procedures that:

- Assess the nature and scope of any incident and identify the customer information systems and types of customer information that may have been accessed or used without authorization;
- Contain and control the incident to prevent further unauthorized access to or use of customer information; and
- Notify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization, unless the Covered Institution determines 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.[12]

The incident response program adopted by a Covered Institution must have procedures for addressing both assessment and identification of incidents. The assessment requirement is designed to determine both the customer information systems (that is, information resources owned or used by a Covered Institution, including physical or virtual infrastructure) and types of customer information that may have been accessed or used without authorization during the incident.[13] Whereas, the identification requirement provides that the institution must identify the specific customers affected, to comply with the Amendments' notification requirements.

Additionally, an incident response program must be designed to contain and control a security incident in order to prevent further unauthorized access to or use of customer information. This includes diagnostic measures such as gathering information about the type of access, the extent to which systems or other assets have been affected, the level of privilege attained by any unauthorized persons, the operational or informational impact of the breach, and whether any data has been lost or exfiltrated.

The amended Regulation S-P requires Covered Institutions to notify each individual whose sensitive customer information was, or was reasonably likely to have been, "accessed or used" without authorization, unless the Covered Institution has determined, after a reasonable investigation of the facts and circumstances, 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. For purposes of Regulation S-P, the Amendments define "sensitive customer information" as any component of customer information that the compromise of which, alone or in conjunction with any other information, could create a reasonably likely risk of substantial harm or inconvenience to the relevant customer. This definition and the "reasonably likely to have been accessed or used" threshold for notification are likely to result in inconsistent application among Covered Institutions, as whether or not access to information creates a "reasonably likely risk of substantial harm or inconvenience" or whether the information is reasonably likely to have been accessed or used, are facts and circumstances tests and require judgment of the Covered Institution. As such, we would expect to see industry participants coalesce around taking a conservative approach deeming virtually all customer information to be "sensitive customer information" and providing notice if there is any risk that such

information was accessed or used in order to avoid regulatory second-guessing.

When notice is determined to be required, the Covered Institutions must provide notice to affected customers[14] as soon as practicable but no later than 30 days after the institution becomes aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred. The amount of time that constitutes "as soon as practicable" may vary based on a number of factors, such as the time required to assess, contain, and control the incident and may be another area where institutions take different approaches.[15] Moreover, the adopting release provides that notice is not required if the Covered Institution conducts a reasonable investigation of the facts and circumstances, and determines that access to customer information has not occurred or is not reasonably likely to have occurred. However, Regulation S-P does not provide parameters or any time limits on the manner of investigation that is necessary to arrive at such a conclusion.

As such, Covered Institutions may vary in their investigation requirements and standard for determining when access or use of customer information is "reasonably likely" to have occurred. Although the Amendments grant Covered Institutions flexibility to investigate and determine whether access has occurred, adopting procedures with respect to customer notification is a new requirement. Currently, state law notifications govern in the event of a data breach. Following the implementation of the Amendments, Covered Institutions need to be mindful of any state law notification requirements, alongside the Regulation S-P notification requirements, which may impose different timelines.

Identifying and Evaluating Information Received from Third Parties

The Amendments broaden and more closely align the scope of both the Safeguards Rule and the Disposal Rule by applying the requirements of those rules to the information of not only a Covered Institution's own customers, but also the information of customers of other financial institutions that has been made available to the Covered Institution, including information handled or maintained on behalf of a Covered Institution.[16] As discussed further below, this is a significant expansion of the scope of information required to be protected and may result in the need for reviews of existing contracts with service providers and possibly significant contractual amendments.

Currently, Regulation S-P's protections under the Safeguards Rule and Disposal Rule apply to different, and at times overlapping, sets of information. Specifically, as required under GLBA, currently, the Safeguards Rule requires broker-dealers, investment companies, and registered investment advisers (but not transfer agents) to maintain written policies and procedures to protect "customer records and information," which is not defined in GLBA or in Regulation S-P. The Disposal Rule, however, requires every Covered Institution to properly dispose of "consumer report information," a different term that Regulation S-P defines consistently with the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) provisions.

To more closely align the information protected by both rules, the Amendments replace the term "customer records and information" in the Safeguards Rule with a newly defined term "customer information," which is defined as any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, and includes information "in the possession of or that is handled or maintained" by the Covered Institution.[17]

The Amendments also require that both the Safeguards Rule and the Disposal Rule apply to the information specified in those definitions regardless of whether such information pertains to (1) individuals with whom the Covered Institution has a customer relationship or (2) the customers of other financial institutions where such information has been provided to the Covered Institution.

This contrasts with the current requirement in Regulation S-P to protect only the information of "a consumer who has a customer relationship with you." Questions remain as to how the industry will implement this requirement, as the rule on its face creates regulatory responsibility for third-party data that Covered Institutions come into possession of, while existing agreements with third parties may limit contractual liability for access to such data.

The intention of this set of Amendments is to continuously better protect the nonpublic personal information of Covered Institution customers from unauthorized disclosure, regardless of who or what is maintaining or handling that information.[18] This is another area where we expect industry participants to engage and adopt accepted standards of care, policies and procedures, and even contractual amendments governing access, and it is ripe for inconsistent application across the industry as Covered Institutions take different approaches.

Reviewing Existing Contracts to Confirm Compliance with the Amendments

In addition to the incident response program requirements (described above), the Amendments require each program to include policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers.[19] The Amendments broadly define a 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. Rather than requiring each Covered Institution to enter into a written contract with its service providers, as initially proposed, the Amendments require that a Covered Institution's policies and procedures require and confirm service providers take appropriate measures to: (1) protect against unauthorized access to or use of customer information and (2) 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.[20]

As a practical matter, we expect that while not required, Covered Institutions will seek to memorialize compliance requirements and standards of care in their service provider agreements. Covered Institutions, as part of their incident response programs, may, but are not required to, enter into a written agreement with their service providers to notify affected individuals on the Covered Institution's behalf but the obligation to ensure that affected individuals are notified remains with the Covered Institution.

Expansion of the Safeguards Rule and Disposal Rule to All Transfer Agents

In acknowledging the sensitive and detailed information maintained by transfer agents, the Amendments extend both the Safeguards Rule and the Disposal Rule to any transfer agent registered with the SEC or another appropriate regulatory agency. Although the SEC received several comments opposing this change, including that it would exceed the SEC's authority and would result in regulatory confusion, the SEC asserted that the expansion was necessary to comply with GLBA and the FACT Act.[21] However, recognizing the different nature of the customer relationship with transfer agents, the Amendments establish a definition of "customer" that is specific to transfer agents and solely for purposes of the Amendments. Specifically, for a transfer agent, a "customer" is defined to be any natural person who is a securityholder of an issuer for which the transfer agent acts or has acted as a transfer agent.[22] This effectively codifies in regulation the transfer agent's service provider obligations to the issuer.

Exception to Annual Privacy Notice Delivery Requirement

Currently, Regulation S-P generally requires broker-dealers, investment companies, and registered investment advisers to provide customers with

annual notices informing them about the institutions' privacy practices. The Amendments conform Regulation S-P to the requirements of the FAST Act, which provides an exception to the annual privacy notice required by Regulation S-P, provided certain requirements are met. Specifically, under the FAST Act and the Amendments a Covered Institution is exempt from providing annual notices if (1) it only provides nonpublic personal information to non-affiliated third parties when an exception to third-party opt-out applies and (2) the institution has not changed its policies and practices with regard to disclosing nonpublic personal information from its most recent disclosure sent to customers.[23]

The conforming of Regulation S-P to the requirements of the FAST Act is unlikely to change how Covered Institutions are delivering or complying with Regulation S-P's annual privacy notice delivery requirement. However, this provision of the Amendments is important as it does remove regulatory uncertainty regarding the discrepancies between Regulation S-P and the FAST Act as they had been inconsistently analyzed by Covered Institutions. Nonetheless, Covered Institutions should continue to deliver privacy notices consistent with Regulation S-P.

Key Takeaways

The effective date for the Amendments for investment companies with net assets of US$1 billion or more, registered investment advisers with assets under management of US$1.5 billion or more, and broker-dealers and transfer agents that are not small entities under the Securities Exchange Act of 1934 is December 3, 2025, while other Covered Institutions have until June 3, 2026 to comply with the Amendments. While the effective date of the Amendments is still almost a year and, in some cases, more than a year away, the scope of the Amendments and the interpretative questions raised by the Amendments should highlight for Covered Institutions the need to commence work on implementation as soon as possible.

The key actions Covered Institutions should consider include: (1) reviewing existing policies and procedures to identify gaps that will need to be addressed prior to the applicable effective date; (2) identifying and evaluating information received from third parties to determine where the Covered Institution receives information that would be deemed to be protected under the Amendments; and (3) reviewing existing contractual arrangements with service providers and counterparties to confirm compliance with the Amendments and whether modification to those contracts is necessary.

As Covered Institutions begin to think about implementing the Amendments, the extended time period for compliance may allow for Covered Institutions to align adoption of new policies and procedures and negotiation of amended third party contracts with Board meeting schedules and renewal schedules for existing contracts. To take advantage of such timelines, Covered Institutions should begin the process now.

Mr. Kerr is a Partner in the Boston, MA office, **Ms. Burstein** is a Partner in the San Francisco, CA office, **Mr. Doyle-Wenger** is an Associate in the Nashville, TN office, and **Ms. Cheng** is a law clerk in the Boston, MA office, of K&L Gates, LLP.

NOTES

1 17 C.F.R. § 248.1-248.100 (2024).

2 *See Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information*, Exchange Act Release No. 97141 (May 16, 2024) (Adopting Release), available at *https://www.sec.gov/files/rules/final/2024/34-100155.pdf*.

3 *See id.*

4 Under GLBA, the term "financial institutions" is defined as any institution engaged in the business of providing financial services to customers who maintain a credit, deposit, trust, or other financial account or relationship with the institution. GLBA further

specifies "financial institutions" to include depository institutions, any broker or dealer, any investment adviser or investment company, any insurance company, any loan or finance company, any credit card issuer or operator of a credit card system, and any consumer reporting agency that compiles and maintains files on consumers on a nationwide basis. *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 527, 113 Stat. 1338, 1449 (1999).

5 *See generally* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, §§ 501-527, 113 Stat. 1338, 1436-50 (1999).

6 *See* Adopting Release, at 5.

7 It is worth noting that in 2008, the SEC proposed amendments to Regulation S-P primarily to help prevent information security breaches and to improve responsiveness when such breaches occur. *See Part 248—Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information*, Exchange Act Release No. 57427 (Mar. 4, 2008) 73 FR 13692, 13693-94 (Mar. 13, 2008).

8 Fact Sheet, Final Rules: Enhancements to Regulation S-P (May 16, 2024), *https://www.sec.gov/files/34-100155-fact-sheet.pdf*.

9 *See* Fixing America's Surface Transportation Act, Pub. L. No. 114-94, § 75001, 129 Stat. 1312, 1787 (2015).

10 Investment companies with net assets of US$1 billion or more, registered investment advisers with assets under management of US$1.5 billion or more, and broker-dealers and transfer agents that are not small entities under the Exchange Act must comply by December 3, 2025. All other Covered Institutions have until June 3, 2026.

11 For purposes of Regulation S-P, a customer is a consumer that has a customer relationship with the Covered Institution. A consumer is an individual who obtains or has obtained a financial product or service that is to be used primarily for personal, family, or household purposes, or that individual's legal representative. With respect to transfer agents, the amendments define a customer as any natural person who is a securityholder of an issuer for which the transfer agent acts or has acted as a transfer agent. Adopting Release, at 37.

12 Adopting Release, at 31.

13 Adopting Release, at 84.

14 If notice is required, the notice must contain key information such as details about the incident, how individuals can protect themselves, contact information for further assistance, and the estimated date or date range within which the incident occurred.

15 Adopting Release, at 56.

16 Adopting Release, at 92.

17 Adopting Release, at 94.

18 Adopting Release, at 99.

19 Adopting Release, at 196.

20 Adopting Release, at 69.

21 Adopting Release, at 95.

22 Adopting Release, at 101.

23 Adopting Release, at 127.