Enhancements to Regulation S-P: A Small Entity Compliance Guide[i]

This compliance guide is divided into the following parts:

- Introduction
- Who is affected by the amendments?
- What is the scope of information protected by the amendments?
- What do the amendments require?
- When must a covered institution provide notice to customers that their sensitive customer information may have been subject to unauthorized access or use under the amendments?
- When must a covered institution begin to comply with the amendments?
- Other resources
- Contacting the Commission

Introduction

On May 16, 2024, the Securities and Exchange Commission (the "Commission") adopted amendments to Regulation S-P, the set of privacy rules that govern the treatment of nonpublic personal information about consumers by certain financial institutions. The amendments address the expanded use of technology and corresponding risks that have emerged since the Commission originally adopted Regulation S-P in 2000. Specifically, the amendments update the requirements for the proper safeguarding and disposal of customer information, including requiring the notification of customers when their sensitive customer information is reasonably likely to have been subject to unauthorized access or use. These amendments will provide enhanced protection of customer or consumer information and help ensure that customers of covered institutions receive timely and consistent notifications in the event of unauthorized access to or use of their sensitive customer information.

Who is affected by the amendments?

The amendments will apply to brokers and dealers, funding portals, investment companies, investment advisers registered with the Commission, and transfer agents registered with the Commission or another appropriate regulatory agency. We refer to these entities collectively as "covered institutions." Transfer agents previously did not need to comply with the rules' safeguarding requirements, and only needed to comply with the rules' disposal requirements if they were registered with the Commission. Under the amendments, transfer agents that are registered with the Commission or another appropriate regulatory agency will now need to comply with both the safeguarding and disposal requirements.

What is the scope of information protected by the amendments?

Under the amendments, the rules' safeguarding and disposal requirements will apply to all **customer information**, which for all covered institutions (except transfer agents) is any record containing nonpublic personal information about a customer of a financial institution, that is in the covered institution's possession or that is handled or maintained by the covered institution or on its behalf. For transfer agents, **customer information** is any record containing nonpublic personal information identified with a securityholder of an issuer for which the transfer agent acts or has acted as transfer agent, that is in the possession of a transfer agent or that is handled or maintained by the transfer agent or on its behalf.

Additionally, under the amendments, covered institutions will be required to notify customers regarding incidents involving **sensitive customer information**, a type of **customer information**. This is information that, either alone or in conjunction with any other information, could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information if it were compromised. Specific examples of **sensitive customer information** include:

- Information uniquely identified with an individual that is reasonably likely to be used as a means of authenticating that individual's identity, such as a Social Security number.
- Information identifying an individual or the individual's account, such as a user name or account number, in combination with other information that could be used to gain access to a customer's account, such as a security code or credit card expiration date.

This scope of coverage is broader than the pre-existing requirements of Regulation S-P.

What do the amendments require?

The amendments will require covered institutions to 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**. The response program must include procedures for covered institutions:

- to assess the nature and scope of any such incident and to take appropriate steps to contain and control such incidents to prevent further unauthorized access or use; and
- with certain limited exceptions, to provide notice to individuals whose **sensitive customer information** was or is reasonably likely to have been accessed or used without authorization.

The covered institution's response program must also include the establishment, maintenance, and enforcement of written policies and procedures reasonably designed to require oversight of service providers, including among other things, to ensure service providers take appropriate measures to:

- protect against unauthorized access to or use of customer information; and
- 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.

Additionally, the amendments will;

- expand the scope of the disposal requirements, which previously applied only to consumer information so that it now applies to both customer and consumer information;
- require covered institutions to maintain written records documenting compliance with the amended rules; and
- amend the existing requirement to provide annual privacy notices to codify a statutory exception.

When must a covered institution provide notice to customers that their sensitive customer information may have been subject to unauthorized access or use under the amendments?

- The amendments will require a covered institution to provide notice 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.
- A covered institution does not need to provide this notice if, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of **sensitive customer information**, it determines 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.
- The notices must include details about the incident, the breached data, and how affected individuals can respond to the breach to protect themselves.
- The final amendments permit a covered institution to enter into a written agreement with its service provider to notify affected individuals on the covered institution's behalf. However, the ultimate responsibility for such notice rests with the covered institution.
- The final amendments provide a mechanism for a covered institutions to delay providing notice if the Attorney General determines that the notice required under the final amendments poses a substantial risk to national security or public safety and notifies the Commission of such determination in writing.

When must a covered institution begin to comply with the amendments?

The amendments will become effective on August 2, 2024. The Commission is providing a tiered compliance period that will provide smaller entities with more time to prepare for compliance. Larger entities must comply with the amendments by December 3, 2025 (i.e., 18 months after publication in the Federal Register), while smaller entities must comply with the amendments by June 3, 2026 (i.e., 24 months after publication in the Federal Register).

Other resources

The adopting release can be found on the Commission's website at https://www.sec.gov/files/rules/final/2024/34-100155.pdf.

The proposing release can be found on the Commission's website at https://www.sec.gov/files/rules/proposed/2023/34-97141.pdf.

Contacting the Commission

The Commission's Divisions of Investment Management and Trading and Markets are available to assist small entities with questions regarding the amendments to Regulation S-P. You may submit a question by email to IMOCC@sec.gov or tradingandmarkets@sec.gov. Additionally, you may contact the Division of Investment Management's Office of Chief Counsel at (202) 551-6825, or the Division of Trading and Markets' Office of Chief Counsel at (202) 551-5777.

---

[i] This guide was prepared by the staff of the U.S. Securities and Exchange Commission as a "small entity compliance guide" under Section 212 of the Small Business Regulatory Enforcement Fairness Act of 1996, as amended. The guide summarizes and explains rules and form amendments adopted by the Commission, but is not a substitute for any rule or form itself. Only a rule or form itself can provide complete and definitive information regarding its requirements.