NSCP Currents

October 24, 2024

How to Prepare for Amendments to Regulation S-P

By Michelle L. Jacko

1. Introduction

Effective November 13, 2000, the U.S. Securities and Exchange Commission ("SEC") adopted Regulation S-P to manage the use and protection of consumer non-public data by financial institutions. The regulation was put in place in response to the growing concern for consumers' loss of data privacy. The Commission adopted Regulation S-P pursuant to Section 504 of the Gramm-Leach-Bliley Act, and pursuant to the Securities Exchange Act of 1934 [15 U.S.C. 78] ("Exchange Act"), the Investment Company Act of 1940 [15 U.S.C. 80a] ("Investment Company Act"), and the Investment Advisers Act of 1940 [15 U.S.C. 80b] ("Investment Advisers Act"), making the regulation applicable to broker-dealers, investment companies, and investment advisers. Regulation S-P mandates that such financial institutions must create procedures designed to protect consumers' privacy.

Specifically, Regulation S-P requires financial institutions to:

- Provide **notice** to consumers about its privacy policies and procedures;
- Describe the **conditions** under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and
- Provide a **method** by which consumers may "opt out" of allowing a financial institution from disclosing nonpublic personal information to most nonaffiliated third parties (subject to exceptions).

Notably, Regulation S-P applies to financial institutions and persons associated with the financial institution. Moreover, certain states (such as California) have even stronger requirements which require "opt in" prior to disclosing nonpublic personal information about a consumer to nonaffiliated third parties. [1]

Since its implementation in 2000, Regulation S-P has been amended several times.

- *2000*: The SEC requires RIAs and registered broker-dealers to set in place policies and procedures that addressed how customer data would be protected through administrative, technical, and physical safeguards.
- *2005*: Regulation S-P was updated to include new requirements for written policies and procedures on the safeguarding of customer information, as well as the proper disposal of records.
- *2024*: Regulation S-P was amended in response to the availability and use of new technologies, as well as the presence of new threats to consumer data. The Amended Rule includes three new components:

1. *Safeguarding Rule*: Investment advisers, broker-dealers and others in the finance space must create and adopt written policies and procedures for how investor information is protected, including cybersecurity protocols and an incident response program.
2. *Notification Rule*: The Notification Rule requires businesses to notify affected individuals of any threat to their information within 30 days of the event. However, if the business determines that the event poses no harm to the individual, they may be exempt from notifying those affected.
3. *Disposal Rule*: The Disposal Rule mandates that all firms and practitioners dispose of customer and consumer information in a manner that protects said data. In addition, the rule requires that businesses implement policies and procedures on disposal methods.

II. Requirements for the New Regulation S-P Incident Response Program

The Incident Response Program addresses the policies and procedures a financial institution must have in place in the event of a cyber breach. They should include how a threat is assessed, steps taken to limit the damage, and how those affected will be notified.

- *Assessment*: Under the amended Regulation S-P, firms should include information on how they assess the presence of a threat or incident, establish the significance of the cyberattack, and identify the type of customer information compromised.
- *Containment and Control*: New requirements include business policies for how firms limit the threat of the cyberattack and prevent further access by unauthorized parties.
- *Notice*: This requires firms to have in place policies and procedures for how they will notify those impacted by the breach.

Under the amended Regulation S-P, Covered Institutions[2] are required to provide notice to consumers whose information may have been accessed or used by an unauthorized party within 30 days of the incident. However, the new amendment includes an exemption. If the affected business has conducted a reasonable investigation into the matter and determined that the breach will *not* cause substantial harm or inconvenience to those affected, the firm is likely exempt from notifying consumers.

For incidents in which notification is required, businesses must notify those affected within 30 days. To meet compliance requirements, the notifications must adhere to the following stipulations.

- *Covered Customers*: Notifications must be sent to covered customers, which include customers of the breached organization AND customers of other Covered Institutions whose information may also have been compromised but have no relationship with the affected business.
- *Scope of Affected Individuals*: If the business cannot determine who was impacted by the breach, they must notify everyone with sensitive information in their system.
- *Scope of Sensitive Customer Information*: Under the amended Regulation S-P, businesses are required to notify those affected if it is determined that the compromised data contains "Sensitive Customer Information." According to the SEC, "Sensitive Customer Information" is defined as information that, if compromised, exposes the individual to substantial risk or inconvenience. This includes identifiable information that is unique to that individual, such as biometric data, driver's license number, social security number, and such. Additionally, information that can be used to affect the individual's financial well-being, such as bank account numbers, mother's maiden name, username and password, or other

information that, in combination with other identifiable data, can give access to the unauthorized party, is deemed to be "Sensitive Customer Information."

- *Method and Content of Notification*: Financial institutions must ensure that their notifications meet the guidelines set forth by Regulation S-P; *i.e.*, the notice must clearly state the nature of the incident, the date the incident occurred, the type of information that was compromised, how to contact the company for more information, how individuals can protect themselves from the impact of the breach, and any measures the organization has taken to provide support to those affected.

Other Important Provisions

- Service Provider Oversight: Covered Institutions that hire third-party service providers to provide services by extension must safeguard non-public Sensitive Customer Information. The amended Regulation S-P stipulates that Covered Institutions which make use of service providers are responsible for oversight and must have written service agreements and policies that address the service providers' responsibilities in relation to safeguarding nonpublic customer information. This includes the vendor's obligation to take necessary steps to protect data against unauthorized access and inform the hiring Covered Institution of any cyber threats within 72 hours of the occurrence.
- Transfer Agents: Prior to recent amendments, Regulation S-P did not address the protection of customer information held by transfer agents. The amended Regulation S-P now includes that SEC-registered and unregistered Transfer Agents must adhere to the same privacy and safeguarding requirements.
- Records of Compliance / Recordkeeping: Under the amended Regulation S-P, institutions, including now Transfer Agents, are required to maintain records showing compliance with the privacy and safeguarding rules. This includes creating and maintaining policies and procedures for safeguarding nonpublic customer information and documentation on how the business satisfies the requirements of the Safeguards Rule.[3]

III. How to Prepare

Prior to amendments to Regulation S-P, Covered Institutions were not required to maintain Written Records of Compliance with the Safeguarding and Disposal Rules.[4] Today, this and other additional requirements are mandated. To prepare for the effective compliance date, firms should take steps to create and maintain:

- Written policies and procedures addressing the safeguards implemented to protect customer information;
- Documentation of any incidents that may have exposed customer information and the institution's response and prevention of further unauthorized access;
- Documentation of any investigations to determine if notification to those impacted is necessary, and if necessary, written documentation of the notice sent;
- Written agreements between the Covered Institution and its service providers (as applicable), including information on the service provider's protocols for safeguarding customer information; and
- Documentation on the disposal of the firm's customer information and steps taken to ensure that such disposal meets the Rule's requirements.

Furthermore, the amended Regulation S-P now requires that Covered Institutions retain written records of their compliance with the regulation for up to five years, with easy accessibility to those records for the first two years. Covered Institutions retained documentation should include:

- Adopted Policies and Procedures;
- Records of any incidents and steps taken to address them;
- Employee training; and
- Documentation of reviews of privacy safeguards and protocols in accordance with the requirements of amended Regulation S-P.

IV. Annual Privacy Notice Delivery Requirements

In general, Regulation S-P requires financial institutions to provide annual privacy notices, subject to certain exceptions. As part of the 2015 Fixing America's Surface Transportation ("FAST") Act, Congress amended the GLBA and added an exception to the annual privacy delivery requirement. In accordance therewith, financial institutions were required to provide a clear and conspicuous initial privacy notice which reflects the privacy policies and practices at the time a consumer became a customer of the firm, and annually thereafter, unless the nonpublic personal information provided to nonaffiliated third parties was in accordance with certain exceptions, and the privacy policies and practices of the firm had not changed from that which was originally disclosed to the consumer. Now, the amended Regulation S-P adds a new exception under Section 248.5(e) of Regulation S-P which aims to lessen the burden of the annual privacy notices delivery requirement. To qualify and forego the annual delivery requirement, financial institutions must satisfy the following conditions:

- The financial institution must share nonpublic personal information only in accordance with the pre-existing Regulation S-P exceptions[5] and provide customers an opportunity to opt out of the financial institution's information sharing with unaffiliated third parties;
- The financial institution's privacy policy and practices have not changed since the last notice was sent; and
- The financial institution must provide the privacy notice to customers electronically, if that is the consumer's preference (such as on the firm's website if the consumer reasonably expects to receive notice in this manner, or on a transaction page that links to the notice).

V. When The Amendments Will Go Into Effect

The amended Regulation S-P was published in the Federal Register on June 3, 2024, and went into effect August 2, 2024.

Firms are required to adopt the amended Regulation S-P program by **December 3, 2025**, for larger entities (*e.g.*,registered investment advisers with $1.5B in assets under management, investment companies with over $1B in assets, broker-dealers and transfer agents) and by **June 3, 2026**, for smaller entities.

VI. Remember to Adhere to Other Applicable Privacy Laws

It is important to understand that Covered Institutions may also be required to incorporate the other privacy laws, such as those set forth by the EU's General Data Protection Regulation ("GDPR") and state privacy laws (such as the California Consumer Privacy Act and others), as applicable.

General Data Protection Regulation ("GDPR")
The GDPR is viewed as the most stringent data protection policy in the world and applies to businesses in the EU and the UK who collect or process personal data of its residents, any entity outside of the EU and UK that

collects or processes data of European Union ("EU") and/or United Kingdom ("UK") residents, and businesses who analyze the data of EU and UK residents.

The GDPR went into effect in 2018 with the core objectives of establishing and protecting individuals' rights in the digital age and ensuring that those who collect and process data are required to do so ethically and compliantly or face penalties for violating their obligations.

The law is based on four major principles:

- *Lawfulness, Transparency and Fairness*: Data must be collected or handled in a manner that is lawful, transparent, and fair to the individual.
- *Data Minimization*: Data collected or used must be limited to only the essential information needed to meet the objective.
- *Purpose Limitation*: Data collected should be used only for the purpose intended and communicated to the individual.
- *Accuracy*: Entities processing data must ensure that the data is accurate and current.

To comply with the GDPR, firms need to:

- Conduct a privacy impact assessment;
- Provide clients with a means to access their personal data;
- Develop an easy-to-read privacy policy;
- Develop policies and procedures for: identifying and reporting of data breaches, conducting a GDPR compliance audit, employing risk mitigation, and reviewing third-party service providers for GDPR compliance;
- Provide a means for data subjects to request and exercise their rights; and
- Identify a legal basis for processing of the personal data.

Firms that breach the GDPR can face significant fines. Thus, businesses within the U.S. who handle personal data of EU citizens or residents must be vigilant in adhering to GDPR guidelines.

State Laws
Above and beyond Regulation S-P protections, over 19 states have enforced comprehensive privacy policies, including California, Colorado, Delaware, Massachusetts, Texas, and more. Seven other states, including New York, also have privacy laws, albeit narrower versions.

It is important for entities to understand and adhere to the privacy laws of each state in which they operate to protect its consumers and avoid state compliance violations. Although the laws may be different for each state, there are some key components that are universal such as:

- *Transparency*: Entities are required to be clear and honest to individuals on how the data collected will be used, shared or sold.
- *Consent*: Businesses collecting and processing data must have express permission from data subjects.
- *Data Minimization*: The data collected must be limited to only the information necessary for the purpose of collection.
- *Data Security*: Businesses are required to have in place adequate cybersecurity to protect the data collected and processed.

- *Data Processing Agreements*: Businesses working with third parties are responsible for ensuring those parties adhere to the same data privacy rules.
- *Accountability*: Businesses are required to meet compliance obligations such as recordkeeping, reviewing cybersecurity measures, and more, to demonstrate accountability.

TIP: In addition to Regulation S-P, be sure to note in your Compliance Policies and Procedures Manual any material procedures that must be followed for state-specific privacy requirements.

VII. Key Takeaways

The protection of Sensitive Customer Information is part of a financial institution's duty to the consumer. Financial institutions have been entrusted with this information to provide a service. Taking critical steps to develop robust privacy policies, which include cyber protections, incident response programs, and compliance records will help to not only protect consumers but, by extension, the firm.

With the amended Regulation S-P, the SEC is addressing the evolving landscape of technology and the associated threats. The rule is designed to strengthen existing regulation as threats to Sensitive Customer Information continue to grow.

To prepare for the compliance dates, Covered Institutions are encouraged to begin the process of implementing the amendments to Regulation S-P by:

- Performing a comprehensive review of their privacy safeguarding programs to identify gaps;
- Ensuring their Safeguarding and Disposal Policies and Procedures are updated to meet the requirements of the amended Regulation S-P;
- Reviewing and updating contracts with Service Providers to include the new stipulations to the rule;
- Developing a Privacy Incident Response Program in conformance with the amended Regulation S-P requirements;
- Updating books and records policies and procedures to meet the requirements of the amended Regulation S-P; and
- Developing a written review of the firm's privacy safeguards to substantiate how the Covered Institution is meeting the requirements of amended Regulation S-P.

For more information, please refer to the final rule, which is available at https://www.sec.gov/rules-regulations/2024/06/s7-05-23.

[1] It's important to note that obligations under Regulation S-P are separate from obligations under applicable state data privacy and security laws and regulations. So a financial institution subject to Regulation S-P may also have legal and compliance requirements under one or more state data privacy rules.

[2] A "Covered Institution" is defined as a financial institution that is subject to the rules of Regulation S-P, and includes broker-dealers, investment companies, registered investment advisers, funding portals, and transfer agents.

[3] The Safeguards Rule is a component of Regulation S-P that requires Covered Institutions to establish written policies and procedures to protect customer information by detecting, responding to and recovering from unauthorized access or use of customer information.

[4] The "Disposal Rule" requires Covered Institutions to properly dispose of "consumer report information" (as defined by the Fair Credit Reporting Act), which includes any record about an individual, whether in paper, electronic or other form, which is a consumer report or is derived from a consumer report. This rule applies to all Covered Institutions, except for notice-registered broker-dealers.

[5] Such exceptions provide that a financial institution is not required to provide customers an opportunity to opt out if the firm shares nonpublic information with unaffiliated third parties through a joint marketing arrangement or for purposes of servicing customer accounts

and effecting certain transactions, or in situations to comply with certain legal and regulatory requirements and/or required consumer reporting.

About the Author:

Michelle L. Jacko, Esq. is the Managing Partner and CEO of Jacko Law Group, PC.
She can be reached at michelle.jacko@jackolg.com.