PAUL HASTINGS

Stay Current

June 2024

Follow @Paul_Hastings

SEC ADOPTS AMENDMENTS TO REGULATION S-P

By Aaron Charfoos, Ryan Swan & Kimia Favagehi

BACKGROUND

On May 15, 2024, the Securities and Exchange Commission (the "SEC") adopted amendments to Regulation S-P. Originally passed in 2000, Regulation S-P regulates the treatment of non-public personal information of consumers by certain financial institutions. The final amendments (the "Final Amendments"), which were originally proposed in March 2023, are intended to modernize and enhance the protection of consumer financial information by certain financial institutions. Regulation S-P applies to the following, also known as "covered institutions":

- Broker-dealers (including fund portals)
- Investment companies
- Registered investment advisers; and
- Transfer agents

WHY IT MATTERS

The updated Regulation S-P will require covered institutions to reevaluate current information security policies and procedures. In particular, the SEC will likely be imposing more scrutiny on how companies respond to data breaches and notify their customers. Covered entities will also need to enhance their practices for monitoring third parties' adherence to rules around the protection of data and customer notification requirements, as laid out by the respective entities.

WHAT'S REQUIRED?

The Final Amendments provide a new set of requirements. As a practical matter, covered institutions will need to update existing policies and procedures to ensure they address the following requirements (most notably among them, the new customer notification requirements), which we discuss below:

- Incident Response Program and Customer Notification
- Scope of the Safeguards Rule and Disposal Rule
- Recordkeeping
- Exception from Requirement to Deliver Annual Privacy Notice; and
- Existing Staff No-Action Letters and Other Staff Statements

INCIDENT RESPONSE PROGRAM AND CUSTOMER NOTIFICATION

1. Incident Response Program

The Final 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. Specifically, written policies and procedures must account for the following:

- ***Assessment***. Assessing the nature and scope of an incident, and identifying the customer information systems and types of customer information that may have been accessed or used without authorization.
- ***Containment & control***. Taking appropriate steps to contain and control the incident to prevent further unauthorized access.
- ***Service providers***.[1] The Final Amendments will also impose requirements to appropriately diligence, monitor, and oversee service providers with respect to their protection of consumer information. Additionally, covered institutions may enter into written agreements with service providers to notify affected individuals in the event of a data breach on the covered institution's behalf. Under the Final Amendments, these policies and procedures must be designed 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 and resulted in unauthorized access to a customer information system maintained by the service provider.

2. Customer Notification

Any instance of unauthorized access to or use of customer information will require that a covered institution **notifies affected individuals** whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.

- ***Notice to affected individuals***. Notification is required for each affected individual whose sensitive customer information[2] was, or is reasonably likely to have been, accessed or used without authorization, *unless* the covered institution has determined, after 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.[3] Covered institutions will be required to provide a clear and conspicuous notice to all affected individuals **as soon as practicable, but not later than 30 days after** becoming aware that

[1] *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."
2 Sensitive Customer Information is 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."
[3] *Substantial Harm or Inconvenience* is defined as "all personal injuries, as well as instances of financial loss, expenditure of effort, or loss of time when they are more than trivial."

unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred.

- ***Notice contents and format***. The Final Amendments, consistent as proposed, require customer notices to include essential information such as:
  - The date (or estimated date/date range) of the incident;
  - The breached data;
  - How individuals can respond to the breach to protect themselves; and
  - Any contact information sufficient to permit an individual to contact the covered institution to inquire about the incident.
- ***National security and public safety delay***. Covered institutions will be allowed to delay notice if the Attorney General determines that the notice presents a substantial risk to national security or public safety and notifies the SEC of such determination in writing, in which case the covered institution may delay such notice for a time period specified by the Attorney General up to 30 days following the date when such notice would otherwise be required. In extraordinary circumstances, notice may be *additionally* delayed for a period of up to 60 days if the Attorney General determines that notice continues to pose a substantial risk to national security and notifies the SEC in writing.

SCOPE OF SAFEGUARDS RULE AND DISPOSAL RULE

- ***Scope of information protected***. The Final Amendments further define the scope of information covered by the safeguards rule and disposal rule to broaden and more closely align the scope of both rules to apply to information of not only a covered institution's *own* customers, but also the customers of *other* financial institutions that have been provided to the financial institution.
- ***Transfer agents***. The Final Amendments extend both the safeguards rule and the disposal rule to apply to any transfer agent registered with the SEC, or any other appropriate regulatory agency, since transfer agents also maintain sensitive and detailed information related to securityholders.
- ***Maintaining current regulatory framework for notice-registered broker-dealers***. The Final Amendments, which are the same as originally proposed, contain several amendments to Regulation S-P in the continuation of the same regulatory treatment that notice-registered broker-dealers were subject to under the existing safeguards rule and disposal rule. Notice-registered broker-dealers are explicitly excluded from the scope of the disposal rule, but subject to the safeguards rule. Now, however, notice-registered broker-dealers are deemed to comply with the safeguards rule (as well as other aspects of Regulation S-P, other than the disposal rule) if they are subject to, and comply with, the financial privacy rules of the Commodity Futures Trading Commission ("CFTC"), including similar obligations to safeguard customer information.

RECORDKEEPING

The Final Amendments will require covered institutions to make and maintain written records documenting compliance with the requirements of the safeguards rule and of the disposal rule. The Final Amendments provide the following recordkeeping requirements:

RECORDKEEPING REQUIREMENTS[4]

Covered Institution	Retention Period
Registered Investment Companies	*Policies and Procedures:* A copy of policies and procedures in effect, or that at any time in the past six years were in effect, in an easily accessible place. *Other records:* Six years, with the first two years in an easily accessible place.
Unregistered Investment Companies	*Policies and Procedures:* A copy of policies and procedures in effect, or that at any time in the past six years were in effect, in an easily accessible place. *Other records:* Six years, with the first two years in an easily accessible place.
Registered Investment Advisers	All records for five years, with the first two years in an easily accessible place.
Broker-Dealers	All records for three years, in an easily accessible place.
Transfer Agents	All records for three years, in an easily accessible place.

EXCEPTION FROM REQUIREMENT TO DELIVER ANNUAL PRIVACY NOTICE

Currently, Regulation S-P requires broker-dealers, investment companies, and registered investment advisers to provide customers with annual privacy notices. However, the Final Amendments provide an exception to the annual privacy notice if certain requirements are satisfied. Accordingly, amendments to Regulation S-P will include an exception to the annual privacy notice requirement if an institution:

- Only provides non-public personal information to non-affiliated third parties when an exception to third-party opt-out applies; and
- The institution has not changed its policies and practices with regard to disclosing non-public personal information from its most recent disclosure sent to customers.

EXISTING STAFF NO-ACTION LETTERS AND OTHER STAFF STATEMENTS

Upon the compliance date of the final rule, staff letters and other staff statements will be withdrawn or rescinded to the extent that they are moot, superseded, or otherwise inconsistent with the rules.

COMPLIANCE PERIODS

The SEC is providing an 18-month compliance period after the date of publication in the Federal Register for **larger entities**, and a 24-month compliance period after the date of publication in the Federal Register for **smaller entities.** The amendments provide various designations for what constitutes a

[4] This table follows the same organization as that provided in the Final Amendments. Please refer to the final rule for additional information regarding recordkeeping requirements.

larger entity, which we have outlined below. Smaller entities are covered institutions that do not meet these standards.

LARGER ENTITIES AS DEFINED BY REGULATION S-P AMENDMENTS[5]

Entity	Qualification to be Considered a Larger Entity
Investment companies together with other investment companies in the same group of related investment companies	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.

Paul Hastings' Data Privacy and Cybersecurity practice regularly advises companies on compliance with cybersecurity requirements at the federal, state, and international levels. If you have any questions concerning how to better prepare for the Final Amendments to Regulation S-P or other cybersecurity requirements, please do not hesitate to contact a member of our team.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Chicago

Aaron Charfoos
1.312.499.6016
aaroncharfoos@paulhastings.com

Washington D.C.

Kimia Favagehi
1.202.551.1736
kimiafavagehi@paulhastings.com

Ryan Swan
1.312.499.6080
ryanswan@paulhastings.com

[5] This table follows the same organization as that provided in the Final Amendments. Please refer to the final rule for additional information regarding the designation of larger entities.