STRADLEY RONON

May 31, 2024

Client Alert | Investment Management

Take Notice: SEC Adopts New Requirements Under Regulation S-P

The U.S. Securities and Exchange Commission (SEC) published a final rule on May 16 adopting amendments to Regulation S-P (Reg S-P) that update certain requirements of the safeguards and disposal rules.[1] The final rule requires registered investment advisers, registered and unregistered investment companies, brokers and dealers, and transfer agents (together, covered institutions) to, among other things, adopt written policies and procedures for incident response programs that address unauthorized access to or use of customer information, including customer notification procedures. The final rule was supported by all five commissioners.[2]

Key Takeaways

- Covered institutions will need to review and likely update their policies and procedures to comply with the requirements of Reg S-P, including developing policies and procedures for an incident response program to address the unauthorized access or use of customer information.[3] Policies and procedures also must include provisions to oversee service providers, and if a service provider is not a covered institution and has a breach, the covered institution likely will be required to institute a response.
- The definition of customer is now broader than just direct customers. It also includes information about the customers of other financial institutions where such information has been provided to the covered institution.
- Covered institutions generally must provide notification to customers of data breaches unless they determine, following 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.

[1] Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, SEC Release Nos. 34-100155; IA-6604; IC-35193 (May 16, 2024).
[2] Commissioner Hester Peirce voted in support of the amendments but expressed some reservations with the breadth of the final rule and the likelihood of overnotification. Please Mr. Postman – Statement on Regulation S-P, Statement of Commissioner Hester Peirce, SEC (May 16, 2024).
[3] Fund boards may be asked to approve procedures revised in response to the final rule.

Background and Key Changes from Previous Standard

Reg S-P, initially adopted in 2000, prescribes privacy rules under the Gramm-Leach-Bliley Act (GLBA), which outlines requirements for certain financial institutions when handling nonpublic personal information about consumers.[4] The SEC proposed amendments in March 2023, and the final rule adopts several key changes to the previous standard.[5]

Previous Requirements	New Requirements
Incident response program. Reg S-P previously did not require an incident response program.	The final rule outlines the new requirement for covered institutions to adopt "incident response programs" that are reasonably designed to detect, respond to, and recover from both unauthorized access to and unauthorized use of customer information. In the event of an incident of unauthorized access to or use of sensitive customer information, a covered institution is required to provide notice, or ensure that notice is provided, to all affected individuals unless the covered institution determines after a reasonable investigation 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.
Application of safeguards rule and disposal rule. The previous rules had different terms for the same kind of customer information. Additionally, the safeguards rule did not apply to transfer agents.	The final rule aligns the information covered under both rules under one definition (customer information) and extends both rules to cover all transfer agents.
Recordkeeping. Previously, Reg S-P required only that covered institutions adopt and maintain policies and procedures to address safeguards for customer records and information.	The final rule requires covered institutions to make and maintain records documenting compliance with Reg S-P's safeguards rule and disposal rule.

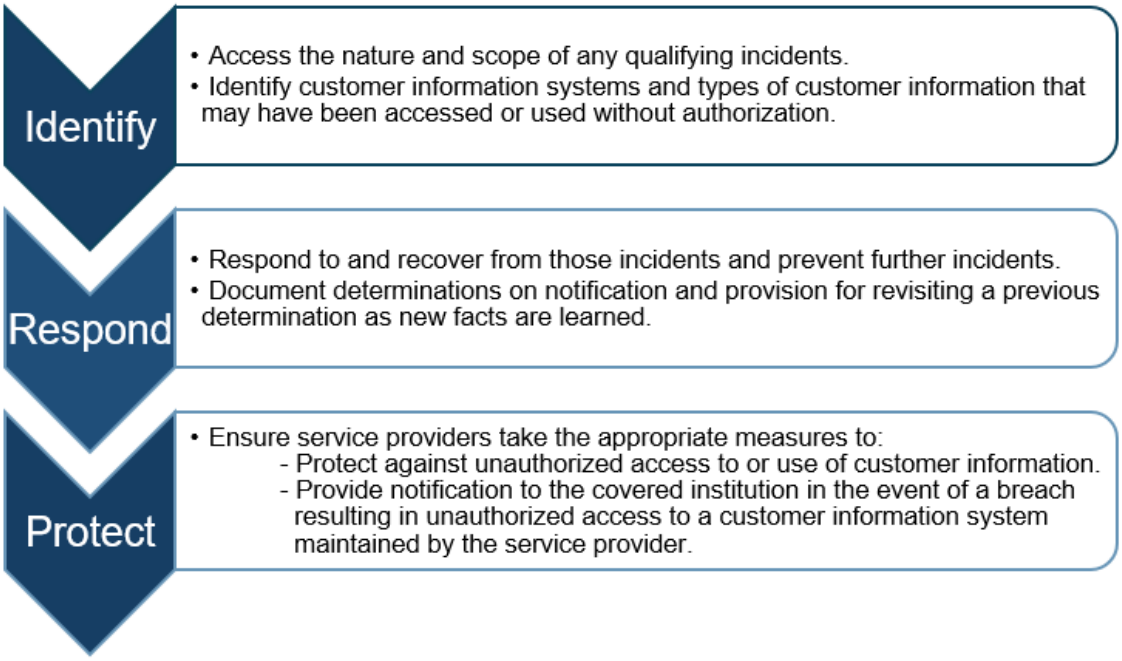
Incident Response Program and Related Notification Requirements

The final rule requires covered institutions to include incident response programs in their safeguards policies and procedures to address unauthorized access to or use of customer information, including procedures for providing timely notification to affected individuals. The final rule calls for the incident response plan to be triggered by any instance of unauthorized access to or use of sensitive customer information (i.e., the expectation is that there is no

[4] Privacy of Consumer Financial Information (Regulation S–P), 65 Fed. Reg. 40,334 (codified at 17 C.F.R. pt. 248) (June 29, 2000). The rule as initially adopted included Rule 248.30(a), the "safeguards rule," and Rule 248.30(b), the "disposal rule." The safeguards rule requires brokers, dealers, investment companies and registered investment advisers to adopt written policies and procedures for administrative, technical and physical safeguards to protect customer records and information. The disposal rule, which applies to transfer agents registered with the SEC in addition to the institutions covered by the safeguards rule, requires proper disposal of consumer report information.

[5] Proposed Rule: Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, SEC Rel. Nos. 34-97141; IA-6262; IC-34854 (March 15, 2023).

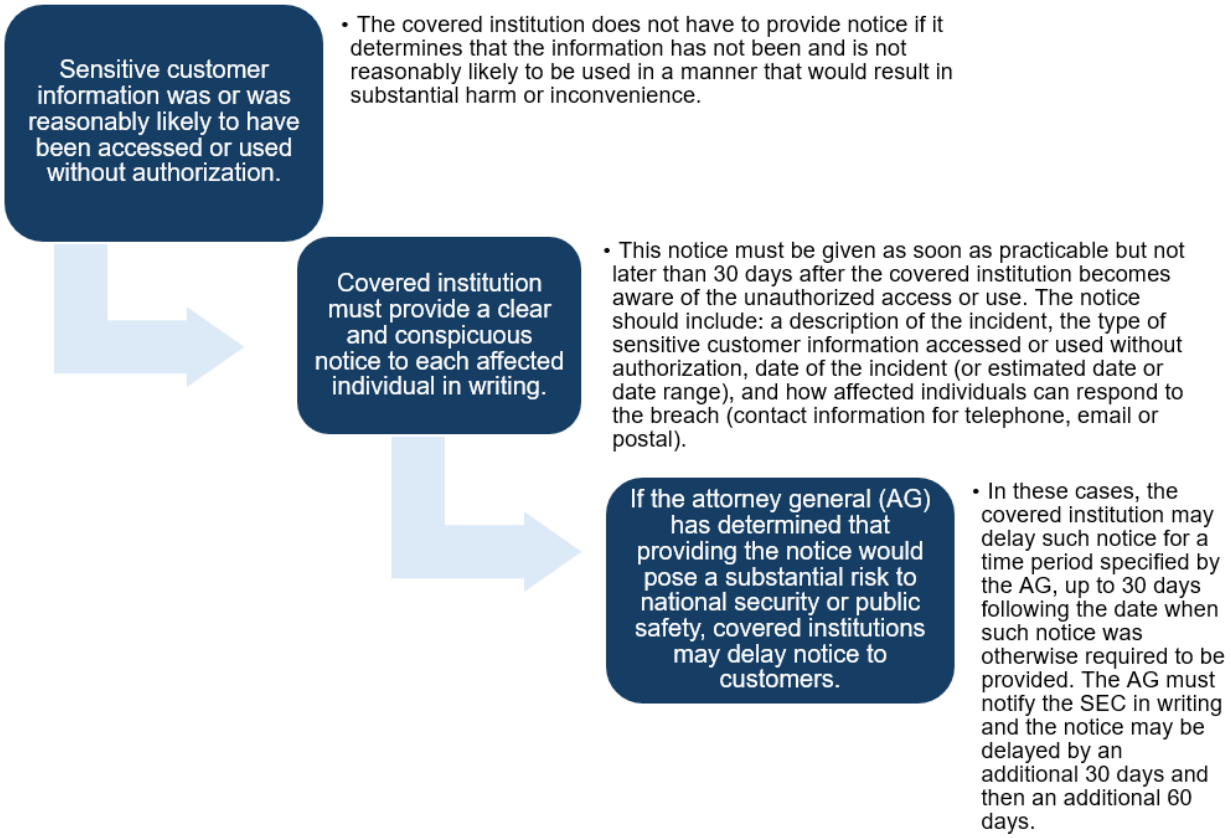
threshold required to trigger the incident response program). The incident response program must be able to:



The final rule also requires covered institutions to provide notice as soon as practicable, but not later than 30 days, after the covered institution becomes aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred except under limited circumstances. As such, a covered institution must provide a notice unless it can determine (after reasonable investigation) that notification is not required and 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"[6] to the client. If the investigation is inconclusive, the covered institution must notify clients. If the covered institution cannot identify which specific individuals' information has been accessed or used without authorization, the final rule requires notice to all individuals whose sensitive covered information resides in the customer information system that was, or was reasonably likely to have been, accessed without authorization.

[6] The formulation of "substantial harm or inconvenience" comes from the GLBA and is not further defined in the final rule.

Notification Requirements



Alignment of the Safeguards Rule and Disposal Rule

To better align the information protected by both rules, the final rule: (1) replaces the term "customer records and information" in the safeguards rule with "customer information," a newly defined term; and (2) adds customer information to the coverage of the disposal rule. Thus, the protections of both the safeguards rule and the disposal rule now apply to "customer information." The final rule also extends the safeguards rule and the disposal rule to all transfer agents registered with the SEC or another appropriate regulatory agency.

Recordkeeping

The final rule requires covered institutions to maintain certain books and records documenting compliance with the safeguards and disposal rules, including written documentation of any detected unauthorized access to or use of customer information, any response to the unauthorized access, and the basis for any determination of whether notice to an affected individual is required under the final rule.

Concurrent Regulation and Enforcement

In the backdrop of the amendments to Reg S-P, the SEC has also proposed several related rules and rule amendments; while some address slightly different components of information

security and privacy, others may implicate the final rule.[7] For example, the SEC has proposed certain amendments that, if adopted, would require investment advisers and funds to adopt cybersecurity policies and procedures and maintain records related to cybersecurity programs and incidents.[8] As several industry participants observed in comment letters, these rule proposals appear to be duplicative.

Additionally, the SEC announced an enforcement action on May 22 against the Intercontinental Exchange Inc. (ICE) for failure to timely inform the SEC of a cyber intrusion.[9] The action highlights the different standards posed by overlapping rules: While covered institutions have 30 days to provide notice to customers under Reg S-P, they may be required to report certain breaches sooner under other SEC rules.

Timing

The compliance date for Reg S-P is 18 months after the date of publication in the Federal Register for larger entities and 24 months after publication in the Federal Register for small entities.[10]

Key Terms	
Affected Individuals	If a covered institution is unable to identify specific individuals impacted by the unauthorized access or use of customer information, the covered institution must provide notice to all individuals whose sensitive customer information resides in the customer information system that was, or was reasonably likely to have been, accessed or used without authorization. However, if the institution reasonably determines that an individual's information is maintained in a system that was not accessed or used without authorization, the covered institution is not required to provide notice to the individual.
Covered Institution	Any broker or dealer, investment company, investment adviser or transfer agent registered with the SEC or any other relevant regulatory authority.
Customer	A consumer who has a customer relationship with the entity. A customer relationship is a continuing relationship between a consumer and the entity in which the entity provides one or more financial products or services to the consumer that are to be used primarily for personal, family or household purposes. With regard to a transfer agent: Any natural person who is a security holder of an issuer for which the transfer agent acts or has acted as a transfer agent.
Customer Information	Any record containing nonpublic personal information about a customer of a financial institution that is handled or maintained by the covered institution or on its behalf, regardless of whether the information pertains to an individual who has a customer relationship with the institution or to customers of other financial institutions whose information has been provided to the covered institution.

[7] See, e.g., Regulation Systems Compliance and Integrity, SEC Release No. 34-97143 (March 15, 2023) (dubbed "Reg SCI"); Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (Cybersecurity Risk Management Proposal), SEC Release Nos. 33-11028, 34-94197, IA-5956, IC-34497 (February 9, 2022).
[8] See Cybersecurity Risk Management Proposal.
[9] The SEC noted that under Reg SCI, ICE was required to immediately notify the SEC of the breach, as well as provide the SEC with a written notification within 24 hours after determining ICE was the subject of a system disruption, system compliance issue or system intrusion. (*In the Matter of Intercontinental Exchange*, SEC Release No. 34-100206 (May 22, 2024).)
[10] In general, investment company complexes with $1 billion or more in net assets, and registered investment advisers with $1.5 billion or more in assets under management, are considered larger entities.

	With regard to a transfer agent: Any record containing nonpublic personal information identified as a natural person, who is a security holder of an issuer for which the transfer agent acts or has acted as a transfer agent, that is handled or maintained by the transfer agent or on its behalf.
Customer Information Systems	Information resources owned or used by the covered institution to collect, process, maintain, use, share, disseminate or dispose of customer information to maintain or support the covered institution's operations.
Disposal	The discarding or abandonment of consumer or customer information, or the sale, donation, or transfer of any medium (including computer equipment) on which consumer or customer information is stored.
Sensitive Customer Information	Any component of customer information alone or in conjunction with any information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information.
Service Provider	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. This also includes affiliates of a covered institution if they are permitted to access customer information through their provision of services.

For more information, contact:

Peter Bogdasarian
Partner
202.419.8405
pbogdasarian@stradley.com

Cory O. Hippler
Partner
215.564.8089
chippler@stradley.com

Kristin H. Ives
Partner
215.564.8037
kives@stradley.com

Grace Wydeven
Associate
215.564.8145
gwydeven@stradley.com

Katie Gallop
Associate
202.507.5161
kgallop@stradley.com