FORsights™

SEC Issues New Regulation S-P Rules

On May 16, 2024, the SEC released a final rule updating Regulation S-P (Reg S-P), which covers the treatment of nonpublic personal information by broker-dealers (including funding portals), investment companies, registered investment advisers, and for the first time, transfer agents. Enhancements include:

- Covered institutions must 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 to provide timely notification to affected individuals whose sensitive customer information was—or is reasonably likely to have been—accessed or used without authorization.
- Broadening the scope of information covered by Reg S-P's requirements.

Background

Reg S-P was issued in 2000 and required broker-dealers, investment companies, and registered investment advisers (covered institutions) to adopt written policies and procedures to safeguard customer records and information, to properly dispose of consumer report information to protect against unauthorized access, and to implement a privacy policy notice and opt-out provisions. Since then, technology has evolved, and states have adopted their own privacy regulations. This final rule establishes a federal minimum standard for covered institutions for data breach notifications.

Incident Response Program

Covered institutions must adopt an incident response program as part of their written policies and procedures. The response program must be reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information and include procedures to assess an incident's nature and scope, as well as appropriate steps to contain and control such incidents to prevent further unauthorized access or use. The program

also must include the establishment, maintenance, and enforcement of written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers.[1]

Customer Notification Requirement

Covered institutions must notify affected individuals whose *sensitive customer information* was—or is reasonably likely to have been—accessed or used without authorization. The notice must be provided 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, except under certain limited circumstances, *e.g.*, if the attorney general notifies the SEC, in writing, that the notice poses a substantial risk to national security or public safety. The notices must include details about the incident, the breached data, and how affected individuals can respond to the breach to protect themselves. A covered institution is not required to provide the notification if it 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* (the SEC did not include a definition of substantial harm in the final rule).

> A covered institution is permitted to enter into a written agreement with its service providers to notify affected individuals on behalf of the covered institution; however, the obligation to ensure that affected individuals are notified in accordance with this rule rests with the covered institution.

Sensitive Customer Information

The final rule defines "sensitive customer information" 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."

The SEC's definition is broader than that used by several states and the Banking Agencies' Incident Response Guidance.

[1]The final rule defines a "service provider" to mean 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.

Reasonable Investigation

Whether an investigation is reasonable will depend on the particular facts and circumstances of the unauthorized access or use. For example, unauthorized access as the result of intentional intrusion by a threat actor may warrant more extensive investigation than inadvertent unauthorized access or use by an employee.

A covered institution cannot avoid its notification obligations in cases where an investigation's results are inconclusive; the notification requirement is excused only where a reasonable investigation supports a determination 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. If an entity concludes that notice is not required, it is required to maintain a record of the investigation and basis for its determination.

A covered institution would not have an obligation to provide notice to an affected individual whose files happened to reside on a breached information system if it was able to reasonably conclude that those files were not subject to unauthorized use or access.

Other Updates

- Expand and align the safeguards and disposal rules to cover both nonpublic personal information that a covered institution collects about its own customers and nonpublic personal information it receives from another financial institution about customers of that financial institution.
- Require covered institutions—other than funding portals—to make and maintain written records documenting compliance with the requirements of the Safeguards Rule and Disposal Rule.
- Conform Reg S-P's annual privacy notice delivery provisions to the terms of an exception added by the *Fair and Accurate Credit Transactions Act of 2003* (FAST Act), which provide that covered institutions are not required to deliver an annual privacy notice if certain conditions are met.

Effective Dates & Estimated Costs

Compliance with the change is required for larger entities by February 2, 2026 (18 months after **Federal Register** publication) and smaller entities will have until August 2, 2026.

Larger Entity	
Entity	Qualifications
Investment companies (including 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

Larger Entity	
Broker-dealers	All broker-dealers that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act[2]
Transfer agents	All transfer agents that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act[3]

All SEC final rules contain an economic analysis. The rule notes that these changes will directly affect every broker-dealer (3,476 entities), every funding portal (92 entities), every investment company (13,766 distinct legal entities), every SEC-registered investment adviser (15,565 entities), and every transfer agent (315 entities) registered with the SEC or another appropriate regulatory agency.

> "For the U.S. financial industry as a whole, this implies an estimate of aggregate notification costs under the baseline of between $200 million and $250 million. Because these estimates are based on data breach incidence rates for all firms, and because financial firms are part of one of the most attacked industries, the actual aggregate notification costs are likely higher than this estimated range."

Conclusion

Forvis Mazars delivers extensive experience and skilled professionals to assist with your objectives. Our proactive approach includes candid and open communication to help address your financial reporting needs. We help broker-dealers, bank holding companies, and others across the capital markets with financial and nonfinancial regulatory reporting. From data origination through report remediation, we help clients with their complex regulatory reporting challenges. For more information, visit forvismazars.us.

[2]A broker or dealer is a small entity if it: (i) had total capital of less than $500,000 on the date in its prior fiscal year as of which its audited financial statements were prepared or, if not required to file audited financial statements, on the last business day of its prior fiscal year; and (ii) is not affiliated with any person that is not a small entity.

[3]A transfer agent is a small entity if it: (i) received less than 500 items for transfer and less than 500 items for processing during the preceding six months; (ii) transferred items only of issuers that are small entities; (iii) maintained master shareholder files that in the aggregate contained less than 1,000 shareholder accounts or was the named transfer agent for less than 1,000 shareholder accounts at all times during the preceding fiscal year; and (iv) is not affiliated with any person that is not a small entity.

Contributors

Brian Matlock
Partner/Financial Services
National Asset Management Leader
brian.matlock@us.forvismazars.com

Anne Coughlan
Director
anne.coughlan@us.forvismazars.com