GT GreenbergTraurig

Alert | Data Privacy & Cybersecurity/ Financial Regulatory & Compliance

June 2024

SEC Adopts Cybersecurity Amendments to Regulation S-P

On May 16, 2024, the U.S. Securities and Exchange Commission finalized amendments to Regulation S-P[1] (the Amendments) that largely adopt the proposed amendments the SEC issued in 2023. As discussed in further detail below, the Amendments will require broker-dealers, investment companies,[2] SEC-registered investment advisers,[3] funding portals, and transfer agents registered with the SEC or other appropriate regulatory agency agents (collectively, Covered Institutions) to adopt written policies and procedures for incident response programs to address unauthorized access to or use of "customer information."

The Amendments create broad federal consumer notification requirements by mandating timely notification to individuals affected by an information security incident involving "sensitive customer information." The Amendments close a longstanding gap created by the 2005 Interagency Guidance, which did not apply to certain financial institutions—i.e., those subject to the GLBA as implemented by

[1] Regulation S-P governs financial institutions' treatment of consumers' nonpublic information.
[2] Regulation S-P applies to investment companies as that term is defined in Section 3 of the Investment Company Act of 1940, as amended (the ICA), whether or not the investment company is registered with the SEC. For example, a business development company, which is an investment company but is not required to register as such with the SEC, is subject to Regulation S-P; similarly, employee securities' companies are also covered. In contrast, an issuer that is excluded from the ICA's "investment company" definition (*e.g.*, a private fund that is able to rely on Section 3(c)(1) or 3(c)(7) of the ICA) is not subject to Regulation S-P but would be subject to the Federal Trade Commission's (FTC) privacy regulations under the Gramm-Leach-Bliley Act (GLBA) (12 C.F.R. Part 313) and safeguards regulation (12 CFR Part 314).
[3] Exempt reporting advisers not subject to Regulation S-P would be subject to the FTC's GLB Act privacy regulations (12 CFR Part 313) and safeguards regulation (12 CFR Part 314).

Regulation S-P. The Interagency Guidance sets forth how financial institutions that the SEC does not regulate must notify consumers of a breach.

Additionally, the Amendments (i) extend the application of Regulation S-P's requirements to safeguard customer records and information to transfer agents, (ii) broaden the scope of information covered by the requirements for safeguarding customer records and information and for properly disposing of consumer report information, (iii) impose record-keeping requirements to demonstrate compliance with the Amendments, and (iv) conform annual privacy notice delivery provisions to the terms of an exception provided by a statutory amendment to the GLBA in December 2015.

The Amendments

1. Incident Response Program

The Amendments require Covered Institutions to adopt an incident response program "reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information."[4] Such incident response programs must include the following procedures:

A. Assess: To assess the nature and scope of any incident and to identify the customer information systems and types of customer information that may have been accessed or used without authorization.

B. Contain and Control: To take appropriate steps to contain and control an incident to prevent further unauthorized access to or use of customer information.

C. Notify: To notify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.[5]

2. Customer Notification Requirements

The Amendments require Covered Institutions to notify affected individuals "whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization."[6]

A. Sensitive Customer Information. Sensitive customer information is customer information that, if compromised, would present a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information. The Amendments provide a non-exhaustive list of sensitive customer information falling into two categories. The first category is information that can be uniquely identified with an individual (*e.g.*, a Social Security Number or biometric record). The second category is sensitive customer information that includes information that could be used to gain access to an account (*e.g.*, username in conjunction with password, mother's maiden name, or security question and answer).

B. Covered Customers. The Amendments expand the definition of "customer information" to include not only information of individuals with whom the Covered Institution has a customer relationship, but also information about "the customers of other financial institutions where such information has been provided to the covered institution."[7] Accordingly, Covered Institutions are

[4] Final Rule 17 CFR § 248.30(a)(3).
[5] However, a Covered Entity need not notify affected individuals if "after a reasonable investigation of the facts and circumstances… 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." Final Rule 17 CFR § 248.30(a)(4)(i).
[6] Final Rule 17 CFR § 248.30(a)(3).
[7] Final Rule 17 CFR § 248.30(d)(5)(i).

expected to notify affected individuals even when they do not have a customer relationship with them.

C. Risk of Harm. There is no obligation to notify customers if a Covered Institution determines that "after a reasonable investigation of the facts and circumstances of the incident…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."[8] The Amendments do not define "substantial harm or inconvenience"; however, the Adopting Release explains that "[d]etermining whether a given harm or inconvenience rises to the level of a substantial harm or a substantial inconvenience would depend on the particular facts and circumstances surrounding an incident."[9]

D. Affected Individuals. The persons requiring notification are defined broadly under the Amendments. The definition of "customer information" includes "any record containing nonpublic personal information…about a customer of a financial institution," which includes "personally identifiable financial information" as well as "any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available information."[10] Where the Covered Institution cannot identify which specific individuals' customer information has been accessed, it must provide notice to all individuals whose sensitive customer information resided on the system that was accessed (or likely accessed) without authorization.

E. Timing. The Amendments require Covered Institutions to provide individual notices within 30 days of becoming aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred.[11] While the trigger for notification is tied to the compromise of "sensitive customer information," the 30-day clock starts at a Covered Institution's awareness of any unauthorized access to or use of customer information.[12]

F. Method and Content of Notification. While the Amendments do not prescribe how notifications must be sent to customers, the Amendments specify that "notice must be transmitted by a means designed to ensure that each affected individual can reasonably be expected to receive actual notice in writing."[13] The contents of such notification must include the nature and date of the incident, the data involved, and multiple means for the affected individuals to contact the Covered Institution. The Amendments also require notices to detail how affected individuals can respond to the incident to protect themselves, with recommendations that customers review account statements, report suspicious activity, place a fraud alert in their credit reports, periodically obtain credit reports free of charge, and review guidance from the Federal Trade Commission to protect against identity theft. These requirements align with the 2005 Interagency Guidance.

[8] Final Rule 17 CFR § 248.30(a)(3).
[9] Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, Exchange Act Release No. 97141, 48-49 (May 16, 2024) (the Adopting Release). While the finalized amendments provide more flexibility for analysis, the definition in the proposed amendments may still offer guidance as to the types of harm and inconvenience that might potentially require notification (*e.g.*, theft, fraud, harassment, physical harm, impersonation, intimidation, damaged reputation, impaired eligibility for credit or misuse of an individual's information to obtain a financial product or service or to misuse the individual's account).
[10] Final Rule 17 CFR § 248.30(d)(5)(i).
[11] Final Rule 17 CFR § 248.30(a)(4)(iii).
[12] Under the Amendments, notification may be delayed for up to 30 days (with extensions for extraordinary circumstances) for either national security or public safety concerns, subject to a determination from the U.S. Attorney General, which, in practice, will likely be relied upon only in narrow circumstances.
[13] Final Rule 17 CFR § 248.30(a)(4)(i).

3. Service Provider Oversight

A Covered Institution's incident response program must include policies and procedures reasonably designed to require oversight, including through due diligence on and monitoring of service providers, including to ensure the Covered Institution meets its customer notification requirements. Such policies and procedures must be reasonably designed to ensure service providers take appropriate measures to "(A) Protect against unauthorized access to or use of customer information; and (B) 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."[14]

The Amendments define "service provider" 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."[15]

4. Expanded Scope Of Safeguards And Disposal Rules

The Amendments expand the reach of the Safeguards and Disposal Rule (Safeguards Rule) in several ways. First, the Amendments increase the scope of information covered by such rules. Specifically, the Amendments expand the definition of "customer information." As noted above, the definition of "customer information" is broadened to include information the entity has or has access to "regardless of whether such information pertains to (a) individuals with whom the covered institution has a customer relationship or (b) the customers of other financial institutions where such information has been provided to the covered institution."[16] This means that the Safeguards Rule now covers customer information received from third-party financial institutions, as well as customer information even after the relationship with the Covered Institution has ended. For example, information that a registered investment adviser receives from the custodian of a former client's assets is covered under the Safeguards Rule if the former client remains a customer of either the custodian or of another financial institution, even though the individual no longer has a customer relationship with the investment adviser.[17]

Second, the Amendments extend the applicability of the Safeguards Rule to cover transfer agents registered with the SEC or another appropriate regulatory agency. This is a significant change because, prior to the Amendments, the Safeguards rule did not apply to any transfer agents and the Disposal provisions applied only to those transfer agents registered with the SEC. Additionally, the Amendments specifically define "customer" for transfer agents (i.e., any natural person who is a securityholder of an issuer for which the transfer agent acts or has acted as a transfer agent).

5. Recordkeeping

The Amendments require Covered Institutions to make and maintain written records documenting compliance therewith. While the retention period varies based on the type of institution, the Amendments align with existing required retention periods for each type of entity. Covered Institutions must make and maintain:

[14] Final Rule 17 CFR § 248.30(a)(5)(i).
[15] Final Rule 17 CFR § 248.30(d)(10).
[16] Final Rule § 248.30(d)(5)(i).
[17] Adopting Release at 99.

A. Written policies and procedures required to be adopted and implemented (i) pursuant to the Safeguards Rule, including the incident response program, (ii) pursuant to the Disposal provisions, and (iii) as part of service provider oversight.

B. Written documentation of:

(i) Any detected unauthorized access to or use of customer information, as well as any response to and recovery from such unauthorized access to or use of customer information required by the incident response program.

(ii) Any investigation and determination made regarding whether notification to customers is required, including the basis for any determination made and any written.

(iii) Any communication from the U.S. Attorney General related to a delay in notice.

(iv) Any contract entered into pursuant to the service provider oversight requirements.

6. Annual Privacy Notice

The Amendments modify Regulation S-P's annual privacy notice delivery provisions to conform to the terms of an exception added by the Fixing America's Surface Transportation (FAST) Act of 2015, which provides that a Covered Institution is not required to deliver an annual privacy notice if:

A. The Covered Institution has not materially changed its policies and practices with regard to disclosing non-public personal information from its most recent disclosure sent to customers; and

B. The Covered Institution only provides non-public personal information to non-affiliated third parties when an exception to third-party opt-out applies, such as when information is (i) shared so the third party can perform services for or functions on behalf of the Covered Institution and is subject to a contractual requirement to maintain the confidentiality of such information; or (ii) shared in situations related to protecting against fraud or complying with certain regulatory requirements and required consumer reporting.

Implementation

Large entities have 18 months after the date of publication in the Federal Register to comply with the Amendments and smaller entities have 24 months. Per the Amendments, "larger entities" are:

- Investment companies that, together with other investment companies in the same group of related investment companies, have net assets of $1 billion or more as of the end of the most recent fiscal year.
- Registered investment advisers with $1.5 billion or more in assets under management.
- All broker-dealers that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act.[18]
- All transfer agents that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act.[19]

[18] 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.
[19] 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.

Takeaways

- **Review and update policies, procedures, and service provider agreements**. Covered Institutions should review the amendments against their existing (i) privacy, incident response, and information security policies, (ii) incident notification procedures, and (iii) service provider agreements to ensure compliance by the compliance date.
- **Focus on recordkeeping and retention**. Compliance with Regulation S-P requires making and maintaining an enumerated list of books and records. Each Covered Institution should check its retention schedules and update as necessary.
- **Ensure compliance**. The Amendments serve as another example of the SEC's continuing focus on cybersecurity issues, including the adequacy and compliance of firms' programs. After updating, Covered Institutions should ensure enforcement of their own policies and procedures.
- **Consider state laws**. While many of Regulation S-P's requirements correspond to state data breach laws that apply to businesses broadly, the state laws vary in their details and compliance with the revised Regulation S-P will not necessarily satisfy state requirements.

Authors

This GT Alert was prepared by:

- Jena M. Valdetero | +1 312.456.1025 | Jena.Valdetero@gtlaw.com
- Arthur Don | +1 312.456.8438 | dona@gtlaw.com
- David E. Beale | +1 312.476.5047 | David.Beale@gtlaw.com