CLIENT ALERT

The SEC Amends Regulation S-P to Bolster Cybersecurity Requirements

May 23, 2024

AUTHORS

Gabriel Acri | Adam S. Aderton | Daniel K. Alvarez | Brian Baltz
Justin L. Browder | Anne C. Choe | Laura E. Jehl | A. Kristina Littman
Michelle Bae | Kari Prochaska | Marc J. Lederer

On May 16, 2024, the Securities and Exchange Commission ("Commission" or "SEC") announced the adoption of amendments to Regulation S-P that significantly expand data security and breach notification obligations for covered institutions.[1] The Commission proposed the amendments in March 2023, arguing that the proposals were justified by changes in technology and the ways that companies collect, use, share, and secure data about their customers. The Commission stayed true to those themes, concluding that the updated requirements ("Amended Regulation S-P") reflect the "expanded use of technology and corresponding risks that have emerged" and the "nature, scale, and impact of data breaches" since the adoption of Regulation S-P in 2000.

Specifically, the Amended Regulation S-P does four key things:

- Expands the scope of information to which Regulation S-P applies via the new term "customer information";

[1] Press Release. *SEC Adopts Rule Amendments to Regulation S-P to Enhance Protection of Customer Information* U.S. SECURITIES AND EXCHANGE COMMISSION (May 16, 2024) available at https://www.sec.gov/news/press-release/2024-58; *Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information*, Releases Nos. 34-100155; IA-6604; IC-35193; File No. S7-05-23 U.S. SECURITIES AND EXCHANGE COMMISSION (May 16, 2024) at 5.

- Requires covered institutions to develop, implement, and maintain written policies and procedures for an incident response program;
- Establishes a requirement that covered institutions notify affected individuals of the unauthorized access to or use of their sensitive customer information no later than 30 days after discovery of the unauthorized access; and
- Imposes service provider due diligence and oversight requirements on covered institutions, including taking appropriate measures to ensure that service providers provide notice of security breaches to the covered institution no later than 72 hours after becoming aware of such a breach.

Covered institutions have either 18 or 24 months (depending on whether you are a "larger entity," as defined by the SEC) to comply with these and other aspects of the Amended Regulation S-P after it is published in the Federal Register.

Expansion of Covered Information

The Amended Regulation S-P broadens the scope of information covered by both the Safeguards and Disposal Rules by replacing the term "customer records and information" with the newly defined term "customer information," with the goal of aligning the information protected under the Safeguards Rule and Disposal Rule. "Customer information" means any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, and includes both nonpublic personal information that a covered institution collects about its own customers *and* nonpublic personal information it receives from other financial institutions about customers of that financial institution.

The Amended Regulation S-P separately defines "sensitive customer information," primarily for purposes of the notification requirement, to mean "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." Examples of "sensitive customer information" include Social Security number, driver's license number, employer or taxpayer identification number, biometric records, and other types of identifying information that can be used to authenticate an individual's identity.

Obligations for Covered Institutions

- Written Incident Response Plan. Covered institutions must develop, implement, and maintain a written incident response program that is "reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information." The incident response program must include the following elements:
    - Assessing the nature and scope of any incident involving unauthorized access to or use of customer information and identifying the customer information systems and types of customer information that may have been accessed or used;

- Containing and controlling an incident to prevent further unauthorized access to or use of customer information (including, but not limited to, strategies like isolating compromised systems, enhancing monitoring or intruder activities, changing administrator passwords, or rotating private keys); and
- Providing clear and timely notice to affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.

- Security Incident Notification Requirements. The Amended Regulation S-P requires covered institutions to notify affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. A covered institution must notify affected individuals as soon as practicable, but not later than 30 days, after it becomes aware that any unauthorized access or use has occurred or is reasonably likely to have occurred, except under certain limited circumstances. The notification must include details about the incident and the compromised data, as well as information about how affected individuals can respond to the breach to protect themselves. The requirement extends to all customers affected by a data breach, regardless of state of residency, in order to provide timely disclosure.
  - A covered institution is not required to provide the notice if it determines, 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." (The SEC declined to define "substantial harm or inconvenience," despite having proposed a definition in its March 2023 notice.) The SEC expressly notes that the investigation is not an excuse to delay notice: discovery of the incident creates a "presumption of notice" that the covered institution apparently must overcome in the 30-day timeframe if it is to avoid notifying any individuals. Moreover, if a covered institution determines that notice is not required, it must maintain a record of the investigation and basis for its determination.
  - Covered institutions may delay notification in cases where the disclosure would pose a substantial risk to national security or public safety, subject to written notification by the Attorney General. The Commission also expanded the time period of delayed notification so that—upon notification by the Attorney General—an additional 60 days (following two 30-day extensions) may be granted.
  - Covered institutions are not required to notify the SEC of the breach, a decision that runs counter to recent regulatory and law making trends.
- Monitoring Service Providers. One of the key—and likely most complicated to implement—aspects of Amended Regulation S-P is that a covered institution's incident response program must establish, maintain, and enforce written policies and procedures to oversee and monitor its service providers. Some noteworthy aspects of this rule include:

- "Service provider" is not limited to third parties—it includes affiliates of covered institutions if they are permitted access to this information through their provision of services.

- The policies and procedures must be reasonably designed to ensure that service providers take measures to protect against unauthorized access to or use of customer information and to provide notification to the covered institution (within 72 hours after "becoming aware" of an incident) in the event of unauthorized access to sensitive customer information, customer information maintained by the service provider, or the service provider's customer information systems. Covered institutions are not required to address these issues in a written agreement with their service providers—an omission that cuts against the trends in data protection laws and may make it harder for covered institutions to make their service providers take the steps necessary to implement the SEC's requirement.

- Covered institutions ultimately retain the obligation to ensure that affected individuals are notified in accordance with the SEC's notice requirements. However, they may enter into written agreements with their service providers whereby the service providers would provide notification of a security incident on behalf of the covered institution.

Other Issues Covered in the SEC's Order

- Exception to the Annual Privacy Notice Delivery Requirement. The SEC joins the CFTC, CFPB, and FTC in conforming its privacy notice rules with the Fixing America's Surface Transportation ("FAST") Act of 2016, which included an amendment to the Gramm-Leach-Bliley Act ("GLBA") creating an exception to the annual privacy notice delivery requirement if a covered institution (1) only shares nonpublic personal information with non-affiliated third parties when an exception to the third-party opt-out applies; and (2) has not changed its policies and procedures with regard to nonpublic personal information from the most recent notice sent to customers.

- Transfer Agents. Under the Amended Regulation S-P, transfer agents registered with the SEC or another appropriate regulatory agency are now included within the scope of the Safeguards Rule and Disposal Rule. The SEC reasoned that transfer agents maintain information that is subject to a similar "risk of substantial harm and inconvenience" and therefore should be protected under the Rules.

- Recordkeeping. Covered institutions (other than funding portals) must create and maintain written documentation regarding their compliance with the Safeguards Rule and Disposal Rule. Depending on the classification of the covered institution, the time period for the retention of records evidencing compliance ranges from three to six years.

- Private Funds. The SEC reaffirms its guidance that Regulation S-P does not apply to private funds. The SEC also notes, however, that registered investment advisers are covered institutions under Amended Regulation S-P, many of which routinely collect customer information. Further, certain private funds and private fund advisers may already

be subject to existing cyber-related rules and reporting obligations of other federal agencies and member organizations. Private fund advisers registered with the CFTC and NFA members are required to promptly report cyber incidents to NFA under certain circumstances, including where a notice is provided to customers as required by state or federal law.[2] The SEC also highlights that private funds may be subject to the FTC Safeguards Rule's breach notification requirements. Consequently, even if the new requirements of Amended Regulation S-P do not apply directly to private funds, advisers to private funds are covered institutions and should view the existing regulatory landscape holistically, including the requirements of Amended Regulation S-P.

Compliance Deadlines and Next Steps

The Amended Regulation S-P becomes effective 60 days after publication in the Federal Register and includes a two-tiered threshold with respect to compliance deadlines based on the size of the entity. Companies designated as "larger entities"—defined as (1) investment companies together with other investment companies in the same group of related investment companies with net assets of $1.5 billion or more in assets at the end of the most recent fiscal year; (2) registered investment advisers with $1.5 billion or more in assets under management; or (3) all broker-dealers and transfer agents that are not small entities under the Securities Exchange Act for the purposes of the Regulatory Flexibility Act—will have 18 months from the date of publication in the Federal Register to comply with the Amended Regulation S-P. Those entities that fall outside of the "larger entity" classification are considered smaller entities and will have 24 months to comply with the updates to Amended Regulation S-P compliance requirements.

[2] For additional information regarding NFA's cyber reporting requirements, please see our client alert entitled "NFA to Require Cyber Breach Reporting," dated December 14, 2018, available here (https://www.willkie.com/-/media/files/publications/2018/12/nfa_to_require_cyber_breach_reporting.pdf).

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Gabriel Acri
212 728 8802
gacri@willkie.com

Adam S. Aderton
202 303 1224
aaderton@willkie.com

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Brian Baltz
202 303 1094
bbaltz@willkie.com

Justin Browder
202 303 1264
jbrowder@willkie.com

Anne C. Choe
202 303 1285
achoe@willkie.com

Laura E. Jehl
202 303 1056
ljehl@willkie.com

A. Kristina Littman
202 303 1209
aklittman@willkie.com

Michelle Bae
202 303 1166
ebae@willkie.com

Kari Prochaska
312 728 9080
kprochaska@willkie.com

Marc J. Lederer
212 728 8624
mlederer@willkie.com