SIDLEY

SIDLEY UPDATE

U.S. SEC Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information Amendments Adopted

June 4, 2024

On May 16, 2024, the U.S. Securities and Exchange Commission (SEC or Commission) adopted amendments to Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information (Final Amendments). While the Final Amendments will become effective on August 2, 2024, larger entities will have until December 3, 2025, to comply, and smaller entities will have until June 3, 2026, to comply. Regulation S-P, as amended through the Final Amendments, apply to all brokers-dealers; registered investment companies; registered investment advisers; funding portals; and transfer agents registered with the SEC, Comptroller of the Currency, Board of Governors of the Federal Reserve System, or Federal Deposit Insurance Corporation (Covered Entities). This is the first time Regulation S-P will apply to transfer agents registered with the federal banking regulators.

The Final Amendments substantially adopt the SEC's March 2023 proposal but include certain changes designed to minimize potential cybersecurity risk that the proposed amendments could have introduced. The Final Amendments create a substantial expansion of protections available to the customers of Covered Entities, and, as noted in Chair Gary Gensler's statement on the Adopting Release, "[the Final Amendments] would help ensure that customers receive sufficient notice to take measures to protect themselves from harm that might result from the breach." However, the Final Amendments are also likely to result in a larger volume of notices given the presumption of notification unless Covered Entities can determine that notification is not required within 30 days of an incident where unauthorized access or use of customer information has or is reasonably likely to have occurred.

Key Requirements

- **Incident Response Program**: Covered Entities are required 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. As stated in the Adopting Release, "[a]ny instance of unauthorized access to or use of customer information will trigger a [Covered Entity's] incident response program."

- **Customer Notification Requirement**: As part of the incident response program, Covered Entities must notify affected individuals whose "sensitive customer information" was, or is reasonably likely to have been, accessed or used without authorization. However, notice is not required if a Covered Entity determines that sensitive customer information has not been, or is not reasonably likely to have been, used in a manner that would result in substantial harm or inconvenience — which is not specifically defined. Notices must include information concerning the incident, such as the data affected, how individuals can respond to protect themselves, and other key facts.

    - **What Is Meant by "Sensitive Customer Information"**: The term "sensitive customer information" means "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." While "substantial harm or inconvenience" is undefined, the definition of "sensitive customer information" includes several specific examples, including Social

Security numbers; unique electronic identification numbers, addresses, or routing codes; driver's license numbers; biometric records; or types of information that could be used to gain access to a customer's account. Importantly, sensitive customer information does not include sensitive personal information of mere "consumers," except where it overlaps with customer information, because, as noted in footnote 294 of the Adopting Release, "the safeguards rule is adopted pursuant to the Gramm-Leach-Bliley Act (GLBA) and therefore is limited to information about 'customers.' " However, sensitive personal information of consumers could nevertheless be subject to state data breach notification laws or other cybersecurity obligations.

- **Timing of Notification Requirements:** Covered Entities must provide notices to affected individuals as soon as practicable but no 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. However, if the U.S. Attorney General provides written notice to the Commission that notification poses a substantial risk of national security or public safety, notification may be delayed for an additional 30-day period, or a 60-day period in extraordinary circumstances. The Adopting Release states that the Commission has engaged the Department of Justice (DOJ) to assist in establishing an interagency communication process to allow the Attorney General to provide written notification to the Commission in a timely manner. Such a process may mirror the December 12, 2023, guidance from the DOJ concerning material cybersecurity incident delay determinations that, among other things, recommends that Covered Entities immediately contact the FBI concerning any cybersecurity incident.

- **Service Providers**: Covered Entities must establish, maintain, and enforce written policies and procedures reasonably designed to require service provider oversight, including through due diligence and monitoring. Specifically, Covered Entities must adopt policies and procedures that are reasonably designed to require service providers to take appropriate measures to protect against unauthorized access to or use of customer information and provide notification to the Covered Entity as soon as possible but no later than 72 hours after becoming aware of a breach in security that has caused unauthorized access to a customer information system maintained by the service provider. Notably, this is a more concrete notice trigger for service providers to alert the Covered Entity than the trigger on Covered Entities to provide notice to customers for "reasonably likely" unauthorized access. Upon receipt of such notification, the Covered Entity must begin its incident response program.

  The term "service provider" means "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." The definition can include affiliates of a Covered Entity.

- **Information Protected Under the Safeguards Rule and Disposal Rule**: The scope of information covered by the safeguards rule and disposal rules is expanded to cover both customer information and consumer information. First, customer information to be protected under both rules shall mean "any record containing nonpublic personal information as defined in section 248.3 (t) about a customer of a financial institution, whether in paper, electronic, or other form" and include customer information in the possession of a Covered Entity as well as customer information handled or maintained on its behalf, including information from customers of other financial institutions whose information has been provided to a Covered Entity. Additionally, the disposal rule was expanded to cover consumer information. The Adopting Release states that the definition is consistent with the objectives of the GLBA and the Fair and Accurate Credit Transactions Act (FACT Act) and based on the definition of "customer information" in the Federal Trade Commission (FTC) safeguards rule.

- **Safeguards Rule and the Disposal Rule to Cover All Registered Transfer Agents**: The safeguards and disposal rules apply to any registered transfer agent. Prior to the Final Amendments, only the disposal rules applied to SEC-registered transfer agents and the safeguards rule did not apply to any transfer agents. However, Regulation S-P now applies both the safeguards rule and disposal rules to all registered transfer agents, even if the transfer agent is registered with another appropriate regulatory agency. Transfer agent customers are defined as "any natural person who is a securityholder of an issue for which the transfer agent acts or has acted as a transfer agent." This definition applies only in the context of the Final Amendments and not to any other rules, including those codified at 17 C.F.R. § 240.17(A)(d). The Final Amendments do not prohibit transfer agents' abilities to enter or modify contracts with issuer clients concerning compliance with law and notification of security incidents, which the

Adopting Release states should minimize the likelihood that a customer receives multiple notices for a single incident.

- **Notice-Registered Broker-Dealers**: Notice-registered broker-dealers are expressly excluded from the scope of the disposal rule but not the safeguards rule. The Adopting Release indicates that under substituted compliance provisions, the Commission will consider a notice-registered broker-dealer in compliance with the safeguards rule if it is subject to, and complies with, the financial privacy rules of the Commodity Futures Trading Commission (CFTC), including the CFTC's similar safeguard customer information obligations.

- **Recordkeeping That Will Significantly Expand Cyber Program Policy and Documentation Requirements:** The Final Amendments require Covered Entities to draft and maintain written records to document their compliance with the requirements of the safeguards and disposal rules. The records required under the Final Amendments include written (1) policies and procedures to address administrative, technical, and physical safeguards for the protection of customer information; (2) documentation of any detected unauthorized access to or use of customer information, including any response to and records from such unauthorized access to or use of customer information; (3) documentation of any investigation and determination made regarding whether notification to affected individuals is required pursuant to the Final Amendments, including the basis for such determination, written documentation from the Attorney General related to delayed notification, and a copy of any notice sent following such determinations; (4) policies and procedures to oversee, monitor, and conduct due diligence on service providers, including to ensure that the Covered Entity is notified when a security breach has occurred at the service provider; (5) contracts or agreements between the Covered Entity and a service provider entered pursuant to the Final Amendments; and (6) policies and procedures addressing proper disposal of customer information. The recordkeeping retention time periods for Covered Entities are consistent with their previous obligation, as outlined in the chart below:

Covered Institution	**Rule**	**Retention Period**
Registered Investment Companies	17 C.F.R. 270.31a-1(b) 17 C.F.R. 270.31a-2(a)	*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, the first two in an easily accessible place.
Unregistered Investment Companies	17 C.F.R. 248.30(c)	*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, the first two in an easily accessible place.
Registered Investment Advisers	17 C.F.R. 275.204-2(a)	All records for five years, the first two in an easily accessible place.
Broker-Dealers	17 C.F.R. 240.17a-4(e)	All records for three years, the first two in an easily accessible place.

Transfer Agents	17 C.F.R. 240.17ad-7(k)	All records for three years, the first two in an easily accessible place.

- **Exception From Annual Privacy Notice Delivery:** Aligning with the proposed amendments and the requirements of the FACT Act, the Final Amendments provide an exception to Regulation S-P's annual privacy notice delivery requirement if the Covered Entity (1) provides nonpublic personal information to nonaffiliated third parties only when the exception to third-party opt-out rights apply (i.e., does not engage in data sharing that requires the opt-out right) and (2) the Covered Entity has not changed its policies and procedures with regard to disclosure of nonpublic personal information from the most recent privacy notice transmitted to its customers. If changes in disclosure of nonpublic personal information require the Covered Entity to send a revised privacy notice, the revised notice will be considered an initial notice for timing purposes and the Covered Entity must resume notice at the same time it otherwise provides its annual privacy notice. If a revised notice is not required, Covered Entities must resume sending annual privacy notices within 100 days of the change.

Compliance Dates

As the Final Amendments were published in the Federal Register on June 3, 2024, larger entities will have until December 3, 2025, to comply, while smaller entities will have until June 3, 2026, to comply. The entity distinction is outlined in the chart below:

Entity	**Larger Entity Qualification**
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

Key Changes From the Proposed Amendments

- **Narrowing the Information Required in a Customer Notification**: The Final Amendments do not require customer notifications to outline the steps taken by a Covered Entity to protect sensitive customer information from further unauthorized access or use, as the Commission agreed that this proposal could create opportunities for threat actors to act nefariously and did not provide actionable items for affected individuals.

- **Attorney General Permitted Delay in Reporting**: Consistent with the SEC's rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (Public Company Cybersecurity Disclosure rule), the Final Amendments permit notification delay to affected customers in cases where the U.S. Attorney General provides either the Commission or the Covered Entity with written determination that disclosure poses a "substantial risk to national security or public safety." Such exemptions may delay notification by 30 or 60 days, and delay can be renewed for another 30- or 60-day period. The national security exception falls short of the broader and more common exception for law enforcement investigation delay mentioned in most other breach-reporting obligations. As with the Public Company Cybersecurity Disclosure rule, the DOJ may issue guidance on how it will make a determination on whether an incident poses a substantial risk to national security or public safety.

- **Preventing Multiple Notifications for Single Incident**: While a Covered Entity is responsible for ensuring that customer notification occurs, it may satisfy this obligation by coordinating with another Covered Entity or a service provider. Such a change is intended to prevent multiple entities from notifying the same affected individual about the same incident.

- **Removing the Definition of Substantial Harm or Inconvenience**: The Final Amendments do not define "substantial harm or inconvenience," but, instead, its determination would depend on the particular facts and circumstances surrounding the incident. The Commission's decision to omit a definition for "substantial harm or inconvenience" in its Final Amendments better aligns with the banking agencies' Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. However, unlike the banking agencies' Interagency Guidance, the Final Amendments have a much broader definition of "sensitive customer information" that would require notification, which includes several types of identifying information.

- **72-Hour Incident Reporting for Service Providers**: The Final Amendments extend service providers' security breach notification requirements from 48 to 72 hours. Such a change allows service providers to conduct a more thorough investigation, resulting in a more accurate notification to the Covered Entity and is aligned with other existing regulatory standards (e.g., CIRCIA, NYDFS, GDPR).

- **Removing Required Service Provider Contracts**: Covered Entities are not expressly required to enter a written agreement with their service providers to protect against the unauthorized access or use of customer information and notify the Covered Entity of breaches of security. However, the Final Amendments still require policies and procedures that are designed to ensure that service providers protect against the unauthorized access or use of customer information and notify the Covered Entity of breaches of security, and while a risk-based approach could work in certain circumstances, a written contract may be the most prudent way to ensure that this requirement is met.

- **Removing "Third Parties" From Definition of "Service Provider"**: The proposed definition of "service provider" was revised to remove reference to third parties. The SEC stated that this is to make plain that the definition of "service provider" can include affiliates of Covered Entities.

- **Clarification of Customer Information for Safeguards and Disposal Rules**: To avoid confusion, the Final Amendments made structural changes to the proposed amendments to clearly define that "consumer information" includes information maintained or otherwise possessed by a Covered Entity for a business purpose and that the customer information definition includes information in the possession of or that is handled or maintained by the Covered Entity or on its behalf.

Key Commissioner Points

The SEC Commissioners unanimously approved the Final Amendments.

Commissioner Hester M. Peirce published a statement acknowledging that the Final Amendments are essential in protecting customers' information and require Covered Entities to appropriately prioritize safeguarding customer information. However, Commissioner Peirce shared reservations on "notifications [not] having the intended effect" and creating fear among Covered Entities to either overreport or underreport. Conversely, as she also noted, the Final Amendments will result in a greater volume of customer notifications, potentially "undermin[ing] the value of the customer notifications by making them so commonplace that people ignore them."

Commissioner Mark T. Uyeda also published a statement, similarly agreeing that the Final Amendments are imperative to protecting customer information. He shared no reservations in its finalization and highlighted that rapid technological innovation warrants "Commission action to ensure that the hundreds of millions of affected customers benefit form robust customer privacy protections."

Related Cybersecurity Rulemakings

The SEC has also proposed first-time cybersecurity regulations for registered investment advisers and funds and broker-dealers and "Rule 10" entities as well as amendments for entities operating systems that support key market and trading functions under Regulation SCI. For a detailed analysis and timeline, see Sidley's blog post.

SIDLEY

CONTACTS

If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you usually work, or

Andrew T. Blake, Partner	+1 202 736 8977, ablake@sidley.com
Colleen Theresa Brown, Partner	+1 202 736 8465, ctbrown@sidley.com
W. Hardy Callcott, Partner	+1 415 772 7402, hcallcott@sidley.com
Stephen L. Cohen, Partner	+1 202 736 8682, scohen@sidley.com
David C. Lashway, Partner	+1 202 736 8059, dlashway@sidley.com
Charles A. Sommers, Partner	+1 202 736 8125, csommers@sidley.com
Alan Charles Raul, Senior Counsel	+1 202 736 8477, araul@sidley.com
Sasha Hondagneu-Messner, Managing Associate	+1 212 839 5403, shondagneumessner@sidley.com
Erica S. Robertson, Managing Associate	+1 202 736 8691, erica.robertson@sidley.com
Casey D. Grant, Associate	+1 202 736 8042, casey.grant@sidley.com