SIDLEY

SIDLEY UPDATE

U.S. SEC Regulation S-P and Checklist: Compliance Deadline, December 3, 2025, Approaching for Large Entities

October 29, 2025

On May 16, 2024, the U.S. Securities and Exchange Commission (SEC or Commission) issued amendments to Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, which became effective on August 2, 2024 (the Final Amendments). The deadline for larger entities to comply with the Final Amendments is December 3, 2025, and for smaller entities, June 3, 2026.

At a high level, Regulation S-P sets forth requirements around the treatment of nonpublic personal information about consumers. The Final Amendments amend Regulation S-P requirements, generally, as they relate to "customer information" of "covered institutions." Pursuant to the Final Amendments, "covered institution" generally is defined to include any brokers, dealers, investment companies, registered investment advisers, funding portals, and registered transfer agents as further specified in the regulation. The Final Amendments also address, among other things, the scope of written policies and procedures reasonably designed to safeguard customer information, incident response, notice of incidents involving sensitive customer information, service providers, recordkeeping, information disposal with regard to both customer information and "consumer information" as defined in the regulation, and annual privacy notices. The Final Amendments are complex and mandate a careful review of, and potentially significant updates to, existing policies and procedures for organizations otherwise subject to Regulation S-P.

Below is a high-level outline and checklist to guide you as a "final check" before the compliance deadlines. This document serves merely as a guide and is not meant to be legal advice or a replacement for legal advice. Sidley's Privacy and Cybersecurity and Securities Enforcement and Regulatory teams can assist you on an *expedited basis* with any questions you may have related to the Final Amendments, including assisting you with developing a compliance and risk management program or updating components of any existing program, to address the requirements of Regulation S-P and the Final Amendments.

For summary definitions of "covered institution," "customer information," "financial institution," "sensitive customer information," and "service provider," please refer to **Appendix A** to this checklist. A version of the checklist in table format that may be useful to complete while addressing the requirements of Regulation S-P is attached at **Appendix B**.

Do the Final Amendments to Regulation S-P Apply to Your Organization?

Is your organization a "covered institution" under the Final Amendments to Regulation S-P? Are you a registered investment adviser, broker, dealer, investment company, funding portal, or registered transfer agent?

If you have answered "yes" to these questions, your organization is within scope for the Final Amendments. You should continue through the checklist below.

Checklist

I. Identifying Customer Information and Where It Resides

a. Consider a data mapping exercise to document company data inventories and data flows, including information received from other financial institutions, information received from customers, and information provided to service providers — applicable to both paper and electronic records. While this is not an express requirement under the Final Amendments, data mapping can facilitate compliance with requirements and support broader risk management efforts.

b. Do you *or* any of your service providers have nonpublic personal information about your customers or customers of another financial institution that was provided to you?

> Note: For private fund advisers, a customer of a financial institution includes natural-person investors.

c. Are you *or* any of your service providers likely to obtain and have personal information of your customers or of customers of a financial institution?

d. For the responses above, identify all potential categories of data subjects and your relationship with the data subjects (i.e., individuals for whom you have customer information).

e. Where does that customer information reside (e.g., on premises, on a third-party cloud platform)?

II. Written Policies and Procedures to Safeguard Customer Information

Summary of the requirement: *Every covered institution must develop, implement, and maintain written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer information. These written policies and procedures must be reasonably designed to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of customer information, and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. Those written policies and procedures must include an incident response program that is reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information.*

a. Create, implement, and maintain written policies and procedures to safeguard customer information and provide that such policies and procedures will be periodically reviewed and updated to reflect changes in technology, data flows, business practices, and regulatory requirements.

> Note: Beyond the high-level requirements and objectives set forth above for safeguarding customer information, the Final Amendments generally do not prescribe in detail the policies and procedures that the SEC expects covered institutions to implement beyond stated requirements for an incident response program and vendor due diligence and monitoring (see below). However, other cybersecurity regulatory regimes may provide helpful content guides. For example, the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Handbook and the New York Department of Financial Services (NYDFS)

Cybersecurity Regulation could be helpful points of reference and guide the potential content and structure of such policies and procedures. In all events, your policies and procedures should be reasonably designed based on particular facts and circumstances.

b. Policies and procedures must include a written incident response program that addresses the following requirements.

   i. Assessment and Reasonable Investigation: Assess the nature and scope of any incident involving unauthorized access to or use of customer information and identify the customer information systems and types of customer information that may have been accessed or used without authorization.

   ii. Containment and Control: Take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information.

   iii. Notice to Affected Individuals: Notify affected individuals whose "sensitive customer information" (see Appendix A for definition) was, or is reasonably likely to have been, accessed or used without authorization subject to certain risk of harm analysis as set forth below.

      1. Notification substance and method: Develop, implement, and maintain incident response procedures to ensure that notice is provided to affected individuals as required, in a clear and conspicuous manner, and is transmitted in a manner through which individuals can reasonably be expected to receive actual notice in writing. The Final Amendments specify in detail the required content of such notices. In addition, while a covered institution can enter into a written agreement with a service provider that had a breach of customer information systems to notify affected individuals on its behalf, the ultimate responsibility for ensuring required notice remains with the covered institution.

      2. Notification timing: Consider adopting or clarifying incident response procedures to ensure that any required notice under Regulation S-P occurs 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. The only basis for limited delay under the Final Amendments is if the U.S. Attorney General determines and notifies the SEC in writing that notice would pose a substantial risk to national security or public safety.

      3. Documentation and Risk of Harm: If notification is not required, implement a process for documenting the reasonable investigation and basis that notification is not required, including any determination that customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience and therefore no notice is required.

   iv. Consult Sidley's Privacy and Cybersecurity team on additional topics, such as law enforcement reporting, third-party coordination, and communicating with regulators, that may be appropriate for further incident response planning and procedure buildout.

c. Service Provider Oversight

> ***Summary of the requirement:*** *Covered institutions' response programs 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. These policies and procedures must be reasonably designed to ensure that service providers take appropriate measures to protect against unauthorized access to or use of customer information and provide notification to the covered institution as soon as possible (but no later than 72 hours after the service provider becomes aware of a breach in security resulting in unauthorized access to a customer information system maintained by the service provider).*

i. The Final Amendments do not prescribe in express detail what steps are required for service provider oversight beyond due diligence and monitoring as described above. The following are additional measures that your organization may wish to consider to support compliance with the requirements.

1. Identify all in-scope service providers — which may include affiliates (see Appendix A for definition of "service provider").

2. Determine whether such service providers have access to customer information through their provision of services.

3. Enter into written agreements that ensure compliance with applicable law and include provisions for notification in the event of a security incident in a time period sufficient to comply with the legal requirement described above.

> Note: The Final Amendments to Regulation S-P do not specifically require covered institutions to enter into written agreements with the service provider addressing these areas; they mandate the policies and procedures be reasonably designed to ensure that service providers take appropriate measures.

ii. Include in your written policies and procedures the steps you will undertake for

1. initial and ongoing due diligence of service providers' safeguarding of customer information

2. ongoing monitoring of service providers' safeguarding of customer information

iii. Consider developing a vendor due diligence questionnaire to be used for onboarding and periodic re-diligencing of vendors. While not expressly required by the Final Amendments, a carefully crafted questionnaire may be a useful tool to provide consistency for vendor oversight and management.

iv. Periodically review and update policies and procedures as well as in response to incidents and changes in technology, data flows, business practices, and regulatory requirements.

III. Recordkeeping

Summary of the requirement: *Covered institutions must draft and maintain written records to document their compliance with the requirements of the safeguards and disposal rules including expansion of the disposal rule, as applicable, to cover consumer information and customer information as defined in the regulation. The records required to be maintained under the Final Amendments include (1) written policies and procedures to address administrative, technical, and physical safeguards for the protection of customer information; (2) written documentation of any detected unauthorized access to or use of customer information, including any response to and recovery from such unauthorized access to or use of customer information; (3) written 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 U.S. Attorney General related to delayed notification, and a copy of any notice sent following such determinations; (4) written policies and procedures to oversee, monitor, and conduct due diligence on service providers, including, among other requirements, to ensure that the covered institution is notified when a security breach has occurred at the service provider; (5) written contracts or agreements between the covered institution and a service provider entered pursuant to the Final Amendments; and (6) written policies and procedures addressing proper disposal of customer information and consumer information where applicable. The rule also sets forth retention time periods.*

a. Generate and maintain the following records:

   i. documentation concerning the creation, implementation, maintenance, and periodic updating of the required written policies and procedures

   ii. documentation of any detected unauthorized access to or use of customer information, including any response to and recovery from such unauthorized access to or use of customer information

   iii. documentation of any investigation and determination made regarding whether notification to affected individuals is required, including the basis for such determination and a copy of any notice sent following such determination

   iv. if applicable, written documentation from the U.S. Attorney General related to delayed notification

   v. policies and procedures to oversee, monitor, and conduct due diligence on service providers, including, among other requirements, to ensure that the covered institution is notified when a security breach has occurred at the service provider

   vi. contracts or agreements between the covered institution and a service provider entered pursuant to the Final Amendments

   vii. policies and procedures addressing proper disposal of customer information and consumer information

b. Consider adding the above recordkeeping requirements to written policies and procedures to demonstrate compliance.

c. Update the books and records retention schedule to reflect the recordkeeping retention periods in the Final Amendments.

Covered Institution	Rule	Retention Period as Applies to the Types of Documents Listed in 17 C.F.R. § 248.30(c)
Registered Investment Companies	17 C.F.R. § 270.31a-1(b)(13) 17 C.F.R. § 270.31a-2(a)(8)	*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 years' records in an easily accessible place.
Unregistered Investment Companies	17 C.F.R. § 248.30(c)(2)	*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 years' records in an easily accessible place.
Registered Investment Advisers	17 C.F.R. § 275.204-2(a)(25), (e)(1)	All records in an easily accessible place for five years, from the end of the fiscal year during which the last entry was made on such record, the first two years in an appropriate office of the investment adviser.
Brokers and Dealers	17 C.F.R. § 240.17a-4(e)(14)	All records for three years in an easily accessible place, in some cases from the date of the record and in some cases from the date the policy or procedure was last in use.
Transfer Agents	17 C.F.R. § 240.17ad-7(k)	All records for three years, in an easily accessible place, in some cases from the date of the record and in some cases from the date the policy or procedure was last in use.

IV. Provide Annual Privacy Notice

The Final Amendments also add an exception to the requirement that specified financial institutions provide an annual privacy notice to their customers. In particular, the amendments to § 248.5(e) stated that "[y]ou are not required to deliver an annual privacy notice if you:

a. provide nonpublic personal information to nonaffiliated third parties only in accordance with [existing provisions that except certain data sharing from customer opt-out right]; and

b. have not changed your policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed to the customer under [other regulation S-P requirements] in the most recent privacy notice provided pursuant to this part."[1]

V. Notification to Affected Individuals

a. As discussed above, a covered institution must notify each affected individual whose sensitive customer information was, or was reasonably likely to have been, accessed or used without authorization, unless the covered institution has determined, after a reasonable investigation of the incident, 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 covered institution will be required to provide a clear and conspicuous notice to each affected individual by a means designed to ensure that the individual can reasonably be expected to receive actual notice in writing. The notice must be provided 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. The only reason for delay is where the Attorney General has determined that providing the notice would pose a substantial risk to national security or public safety.

b. In addition to notification requirements under the Final Amendments, there may be individual (as well as regulator) notification obligations pursuant to other applicable laws and regulations, including under state data breach laws, in addition to federal and international laws. Sidley's Privacy and Cybersecurity team can assist with determining notification obligations and certain other legal compliance and risk considerations related to security incidents.

Additional Checklist Items

While not prescribed under the Final Amendments, consider taking the below additional compliance-related steps.

I. Examination preparedness — Conduct a mock examination or otherwise take steps to prepare for an SEC examination on compliance with the Final Amendments.

II. Risk management program — During a recent webinar hosted by the SEC, staff indicated an expectation that covered institutions have risk management programs to identify, assess, and

[1] How this exception applies to a given set of facts must be carefully considered in light of the nature of data sharing that is occurring, an evaluation of whether customer opt-out of data sharing applies or not under existing rules, and a review of any changes to the policies and practices of the entity since the time the most recent privacy notice was provided.

mitigate safeguarding risks. This risk assessment would consider technology and controls and scope in critical vendors with access to customer information, among other things.

III. Testing and training — During the same webinar, SEC staff suggested that covered institutions engage in testing and training with respect to the requirements of Regulation S-P. This could include tabletop exercises that test the incident response plan as well as regular security training for employees.

Appendix A: Summary of Key Definitions

"**Covered institution**" (17 C.F.R. § 248.30(d)(3)) means any broker or dealer, any investment company, and any investment adviser or transfer agent registered with the Commission or another appropriate regulatory agency as further defined in the regulation. It applies to investment companies, including business development companies, regardless of whether they are registered with the SEC. It also applies to funding portals.

"**Customer information**" (17 C.F.R. § 248.30(d)(5)) means, with certain exceptions, any record containing nonpublic personal information as defined in the regulation, about a customer of a financial institution, whether in paper, electronic, or other form, that is in the possession of a covered institution or that is handled or maintained by the covered institution or on its behalf regardless of whether such information pertains to (A) individuals with whom the covered institution has a customer relationship or (B) to the customers of other financial institutions where such information has been provided to the covered institution. A separate definition is provided for registered transfer agents.

"**Financial institution**" (17 C.F.R. § 248.3(n)) means any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in Section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. § 1843(k)). In practical terms, this generally means any brokers or dealers, investment companies, or investment advisers registered with the SEC under the Investment Advisers Act of 1940.

"**Sensitive customer information**" (17 C.F.R. § 248.30(d)(9)) 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." Enumerated examples include Social Security number (SSN), official state- or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, biometric record, unique electronic identification number, address or routing code, telecommunication identifying information or access device, or customer information identifying an individual or the individual's account, including account number, name, or online user name, in combination with authenticating information or in combination with similar information that could be used to gain access to the customer's account such as an access code, a credit card expiration date, a partial SSN, a security code, a security question and answer, or the individual's date of birth, place of birth, or mother's maiden name.

"Service provider" (17 C.F.R. § 248.30(d)(10)) 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."

Appendix B: Regulation S-P Checklist

The checklist below is intended to be used in coordination with outside counsel to track items, responses, and potentially applicable documents as they relate to the Final Amendments checklist.

Do the Final Amendments to Regulation S-P Apply to You?

Action Item	Answer	Observations
Are you a "covered institution" under the Final Amendments to Regulation S-P?		
Are you a registered investment adviser? If so, you are covered.		
Are you an investment company? If so, you are covered.		
Are you a broker or dealer? If so, you are covered.		
Are you a funding portal? If so, you are covered.		
Are you a registered transfer agent? If so, you are covered.		

Identify What Customer Information You Have and Where It Resides

Action Item	Answer	Observations
Consider a data mapping exercise to document company data inventories and data flows, including information received from other financial institutions, information received from customers, and information provided to service providers (applicable to both paper and electronic records). While this is not an express requirement under the Final Amendments, data mapping can facilitate compliance with requirements and support broader risk management efforts.		
Do you *or* any of your service providers have nonpublic personal information about your		

Action Item	Answer	Observations
customers or customers of another financial institution that was provided to you?		
Are you *or* any of your service providers likely to obtain and have personal information of your customers or of customers of a financial institution?		
For the responses above, identify all potential data subjects and your relationship with the data subjects (i.e., individuals for whom you have customer information).		
Where does that customer information reside? (e.g., on premises, on a third-party cloud platform)		

Written Policies and Procedures to Safeguard Customer Information

Action Item	Status	Observations
Create, implement, and maintain written policies and procedures to safeguard customer information. Specify that such policies and procedures will be periodically reviewed and updated to reflect changes in technology, data flows, business practices, and regulatory requirements.		
Policies and procedures must include a written incident response program that addresses the following requirements: (1) assessment, (2) containment and control, and (3) notice.		
Consult legal counsel on additional topics, such as law enforcement reporting, third-party coordination, and communicating with regulators, that may be appropriate for		

Action Item	Status	Observations
further incident response planning and procedure buildout.		
Third-party coordination: Do you have a process for coordinating notification with issuers or other financial institutions if required by contract or business relationship?		
Identify all in-scope service providers — which may include affiliates.		
Determine whether such service providers have access to customer information through their provision of services directly to you.		
Enter into written agreements that ensure compliance with applicable law and include provisions for notification in the event of a reportable security incident in a time period sufficient to comply with the legal requirements of the Final Amendments.		
Include in your written policies and procedures the steps you will undertake for (1) initial and ongoing due diligence of service providers' safeguarding of customer information and (2) ongoing monitoring of service providers' safeguarding of customer information.		
Consider developing a vendor due diligence questionnaire. While not expressly required by the Final Amendments, a carefully crafted questionnaire may be a useful tool to provide consistency for vendor oversight and management.		
Periodically review and update policies and procedures as well as		

Action Item	Status	Observations
in response to incidents and changes in technology, data flows, business practices, and regulatory requirements.		

Recordkeeping

Action Item	Status	Observations
Generate and maintain the following records:		
Documentation concerning the creation, implementation, maintenance, and periodic updating of the required written policies and procedures.		
Documentation of any detected unauthorized access to or use of customer information, including any response to and recovery from such unauthorized access to or use of customer information.		
Documentation of any investigation and determination made regarding whether notification to affected individuals is required, including the basis for such determination and a copy of any notice sent following such determinations.		
If applicable, written documentation from the U.S. Attorney General related to delayed notification.		
Policies and procedures to oversee, monitor, and conduct due diligence on service providers, including, among other requirements, to ensure that the covered institution is notified when a security breach has occurred at the service provider.		
Contracts or agreements between the covered institution and a service provider entered pursuant to the Final Amendments.		
Policies and procedures addressing proper disposal of customer information and consumer information.		

Action Item	Status	Observations
Consider adding the above recordkeeping requirements to your written policies and procedures to demonstrate compliance.		
Update your books and records retention schedule to reflect the recordkeeping retention periods in the Final Amendments.		

Provide Annual Privacy Notice

Action Item	Status	Observations
Determine whether the exemption for annual privacy notices may apply to you. For entities currently required to provide annual privacy notices, the Final Amendments provide a new exception if you only provide nonpublic personal information to nonaffiliated third parties pursuant to existing exceptions from opt-out and notice requirements and you have not changed your policies from the notice most recently provided subject to certain additional requirements.		

Notification to Affected Individuals

Action Item	Status	Observations
Notify each affected individual whose sensitive customer information was, or was reasonably likely to have been, accessed or used without authorization, unless the covered institution has determined, after a reasonable investigation of the incident, 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. See Final Amendments and consult with Sidley's Privacy and Cybersecurity team on the substance and timing requirements for such notice.		
There may be individual (as well as regulator) notification obligations pursuant to other applicable laws and regulations, including under state data breach laws, in addition to federal and international laws. Sidley's Privacy and Cybersecurity team can assist with determining notification obligations and other legal compliance and risk considerations for security incidents.		

Additional Items

Action Items	Status	Observations
Examination preparation (e.g., mock examination)		
Risk management program		
Testing and training (e.g., tabletop exercise, regular employee training)		

CONTACTS

Ranah Esmaili, Partner +1 202 736 8742, resmaili@sidley.com

Jonathan M. Wilan, Partner +1 202 736 8635, jwilan@sidley.com