WILLKIE

CLIENT ALERT

December 3 Compliance Date for SEC Amendments to Regulation S-P is Fast Approaching

October 16, 2025

AUTHORS

Benjamin B. Allensworth | Daniel K. Alvarez | James E. Anderson | Brian Baltz
Matthew Comstock | Laura E. Jehl | Jennifer R. Porter | Amelia Putnam

On May 16, 2024, the Securities and Exchange Commission ("SEC") adopted sweeping amendments to Regulation S-P that significantly expand data security, incident response, and breach notification obligations for regulated entities.[1] The amended Regulation S-P applies to various covered institutions, such as broker-dealers (including funding portals), investment companies, registered investment advisers, and transfer agents.

After over a year since the SEC's final rules were adopted, the dates for compliance with these new amendments are now on the horizon: *larger entities and most broker-dealers must be in compliance by December 3, 2025, and smaller entities must be in compliance by June 3, 2026.*

[1] 17 CFR 248.30.

Requirements Under the Amendments

In our previous Client Alert, we discussed the specific amendments adopted by the SEC.[2] In summary, the amended Regulation S-P introduces four key changes that materially expand compliance obligations for covered institutions:

- The amended Regulation S-P broadens the scope of information subject to Regulation S-P by replacing "customer records and information" with the newly defined term "customer information," which 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 requires covered institutions to implement a written incident response program reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including processes to (i) assess the nature and scope of an incident and the types of customer information involved in the incident, (ii) contain the incident and prevent further unauthorized access or use of customer information, and (iii) provide clear and timely notice to affected individuals whose sensitive customer information was accessed or used, or reasonably likely to have been accessed or used, without authorization.

- Covered institutions must notify individuals no later than 30 days after discovery of unauthorized access to or use of sensitive customer information, subject to limited exceptions and law enforcement delay.

- Covered institutions must comply with certain service provider oversight obligations, including implementing measures to ensure that providers notify the covered institution within 72 hours of becoming aware of an incident impacting customer information or customer information systems.

A Closer Look at Service Provider Monitoring Requirements

In recent years, companies across major industries have experienced significant cybersecurity incidents caused by inadequate information security controls or critical vulnerabilities in products provided by service providers. In response to this growing trend, and to bolster the oversight and monitoring of service providers processing customer information on behalf of covered institutions, the amended Regulation S-P requires covered institutions to adopt written policies and procedures to oversee and monitor service providers as a part of their incident response policies. These policies and procedures must be reasonably designed to ensure that:

- Service providers implement measures to protect against unauthorized access to or use of customer information; and

[2] https://www.willkie.com/-/media/files/publications/2024/05/the_sec_amends_regulatons_s-p_to-bolster_cybersecurity_requirements.pdf.

- Service providers provide notice to the covered institution no later than 72 hours after becoming aware of any incident involving unauthorized access to sensitive customer information, customer information maintained by the provider, or the provider's customer information systems.

The amended Regulation S-P provides flexibility for covered institutions to determine how they will comply with service provider requirements based on their specific circumstance, such as the leverage a covered institution may have to modify service provider contracts or a limited scope of services that a service provider may provide. In some circumstances, covered institutions may draft their policies and procedures to require actions other than modifying service provider contracts, which may include reviewing a service provider's cybersecurity certifications or obtaining written assurances from the service provider concerning its cybersecurity measures and practices.

Although the amended Regulation S-P does not mandate that covered institutions execute contractual provisions with service providers, as a practical matter covered institutions should make best efforts to obtain such contractual or other written assurances from their service providers to comply with their own regulatory obligations. To that end, covered institutions should strongly consider reviewing and revising their service provider contracts to ensure that service providers are obligated to notify the covered institution within 72 hours of a service provider identifying a cybersecurity incident. Contractual 72-hour notification provisions are critical because such provisions enable covered institutions to meet the amended Regulation S-P's 30-day individual notice deadline, help them to contain incidents quickly, and ensure compliance with various reporting obligations that may be applicable in other jurisdictions. Such provisions should also include binding contractual assurances that the service provider itself has implemented reasonable information security controls in light of the customer information it will process on behalf of the covered institution. Additionally, covered institutions may contractually authorize service providers to deliver individual notices on their behalf, although responsibility for compliance with the amended Regulation S-P ultimately remains with the covered institution.

Next Steps

In preparation for the rapidly approaching compliance dates, covered institutions should review and update their written cybersecurity policies to address risks to customer information. Covered institutions' written policies should describe in detail their incident response procedures as well as their procedures for complying with notification requirements in the event of a cybersecurity incident.

As part of this compliance review, covered institutions should also review their processes for onboarding and monitoring service providers as well as contracts with service providers that process customer information to ensure proper diligence and oversight over those service providers. In particular, covered institutions should consider whether to amend their service provider contracts to ensure that they require service providers to promptly, and in all cases within 72 hours following discovery of an incident, notify the covered institution of any actual or reasonably suspected incident impacting customer information.

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

Benjamin B. Allensworth	**Daniel K. Alvarez**	**James E. Anderson**	**Brian Baltz**
202 303 1273	202 303 1125	202 303 1114	202 303 1094
ballensworth@willkie.com	dalvarez@willkie.com	janderson@willkie.com	bbaltz@willkie.com
Matthew Comstock	**Laura E. Jehl**	**Jennifer R. Porter**	**Amelia Putnam**
202 303 1257	202 303 1056	202 303 1223	202 303 1089
mcomstock@willkie.com	ljehl@willkie.com	jporter@willkie.com	aputnam@willkie.com

WILLKIE

BRUSSELS CHICAGO DALLAS FRANKFURT HAMBURG HOUSTON LONDON LOS ANGELES
MILAN MUNICH NEW YORK PALO ALTO PARIS ROME SAN FRANCISCO WASHINGTON