Articles + Publications | September 17, 2026

Reg S-P Compliance Deadlines Have Passed. Is Your Firm Exam-Ready?

WRITTEN BY

Genna Garver | Kim Phan | Brianna L. Dally

KEY POINTS

- The SEC's 2024 amendments to Regulation S-P are now fully in effect. Covered institutions should be prepared to show that their written incident response programs, 30-day customer breach notification processes, and service provider oversight are functioning as intended, not just that implementation deadlines have been met.
- The SEC's Division of Examinations has identified Reg S-P as a Fiscal Year 2026 examination priority. Examiners will be assessing whether firms have genuinely put their administrative, technical, and physical safeguards into practice, rather than simply documenting them on paper, with particular attention to governance and risk management, service provider oversight, the compliance program (including the firm's most recent Rule 206(4)-7 annual review), and vendor management documentation.
- Vendor oversight is likely to be one of the more demanding areas for firms to demonstrate. Examiners will want to see that the 72-hour breach notification obligation flows back contractually to the firm, along with executed service agreements and a record of ongoing due diligence for vendors handling customer information.
- Firms that are unable to produce organized, complete documentation on short notice may find themselves in a more difficult position. Beyond deficiency letters, referral to the SEC's Division of Enforcement remains a possibility where staff identify significant or repeated gaps in safeguards.

The Security and Exchange Commission's (SEC) 2024 amendments to Regulation S-P are now fully in effect, with both compliance deadlines now behind us. For broker-dealers, investment advisers, private fund managers, and other covered institutions that worked hard to prepare incident response programs and other items necessary to meet their respective implementation deadlines, there's no rest for the weary. Covered institutions should expect the SEC's Division of Examinations to focus on whether firms have actually put their Reg S-P obligations into practice. According to the SEC's Division of Examinations (Division) Fiscal Year 2026 Examination Priorities, the Division will examine whether firms have developed, implemented, and maintained policies and procedures in accordance with the rule's new provisions that address administrative, technical, and physical safeguards for the protection of customer information. Now is the time for firms to assess their operational resiliency and the effectiveness of their programs in practice, not just on paper.

A REFRESHER ON THE AMENDED RULE'S KEY REQUIREMENTS

The SEC adopted amendments to Reg S-P on May 16, 2024, modernizing a framework largely unchanged since 2000. The amendments apply to broker-dealers, investment companies, SEC-registered investment advisers, funding portals, and transfer agents registered with the SEC or another appropriate regulatory agency. Larger entities were required to comply by December 3, 2025, and smaller entities by June 3, 2026.

The headline requirements are:

1. **Written Incident Response Program.** Firms must develop, implement, and maintain written policies and procedures for a program reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information.
2. **Customer Notification, 30-Day Clock.** When sensitive customer information was, or is reasonably likely to have been, accessed without authorization, firms must notify affected individuals as soon as practicable and no later than 30 days after becoming aware of the incident. Notices must describe the incident, the breached data, and steps affected individuals can take to protect themselves.
3. **Vendor Management, the 72-Hour Rule.** Firms must establish, maintain, and enforce written policies and procedures requiring oversight of service providers that handle customer information. Those policies must require service providers to notify the covered institution no later than 72 hours after becoming aware of a breach. The ultimate responsibility for customer notification rests with the firm, even if a written agreement delegates notification duties to the service provider.
4. **Expanded Safeguards and Disposal.** The amendments extend safeguarding and disposal requirements to cover all customer information, not just consumer information as under the prior rule, including data maintained by or on behalf of the firm through third-party providers.
5. **Recordkeeping.** Firms must maintain written records documenting their compliance with the amended rules.

WHAT EXAMINERS WILL WANT TO SEE

When examiners arrive, they will expect firms to produce documentation across four broad areas:

GOVERNANCE AND RISK MANAGEMENT

Examiners will want to understand how cybersecurity and privacy risk are managed at the organizational level. This means having a current org chart that reflects ownership structure and control persons, documentation of the roles and responsibilities of key personnel such as the CCO, CISO, and CTO, and a clear picture of how cybersecurity fits within the firm's broader governance structure. Firms should also be prepared to produce a list of current and terminated employees and contractors, a description of all relevant committees including their responsibilities and meeting frequency, and documentation of the firm's IT governance model. Client account information, including total assets under management and account categorization, as well as a list of outside legal counsel and compliance consultants retained during the review period, may also be requested.

SERVICE PROVIDERS

The SEC expects firms to have a clear picture of every service provider that touches their technology, cybersecurity, or compliance functions. For each such provider, firms should be able to describe the services rendered, the provider's affiliation with the firm if any, and whether the firm or any of its supervised persons holds an economic interest in the provider. This is not a one-time exercise. Examiners will look for evidence of ongoing oversight, not just a vendor list.

COMPLIANCE PROGRAM

This is where examiners are likely to spend the most time. Firms should have their complete written compliance policies and procedures ready to produce, along with a description of any material amendments made during the review period. Examiners will also expect to see the firm's most recent annual review performed pursuant to Rule 206(4)-7 of the Investment Advisers Act of 1940 (Advisers Act), results of any mock examinations or compliance

consultant reviews, a log of compliance testing performed, and a list of automated compliance tools in use.

Critically, firms must be able to produce their privacy notices and evidence of delivery to clients, a record of any client complaints or inquiries related to privacy or information security, documentation of any internal investigations into privacy or information security issues, and a log of any employee, contractor, or third-party noncompliance with the firm's cybersecurity policies. Written policies covering administrative, technical, and physical safeguards for customer information will also be on the list, as will documentation of any cybersecurity incidents or breaches that occurred during the review period, including the date, nature, and scope of each incident and any remediation steps taken.

VENDOR MANAGEMENT

Vendor oversight is one of the most operationally demanding areas of the amended rule, and examiners will probe it closely. Firms should have written policies covering the full vendor lifecycle, from selection and onboarding through ongoing monitoring and offboarding, as well as policies for assessing vendor information security. For each vendor with access to customer records, firms should be able to produce executed service agreements and evidence of initial and ongoing due diligence. Firms should also maintain a log of any instances where a vendor failed to meet its contractual obligations.

WHAT COMES NEXT

Firms should expect the Division's early Reg S-P examinations to likely generate broader guidance in the near term. Historically, the Division has followed a wave of thematic examinations with a risk alert summarizing staff observations, both the deficiencies most commonly identified and, sometimes, examples of practices viewed favorably. A Reg S-P risk alert of this kind would give firms a clearer benchmark against which to measure their own programs. At the same time, firms should not assume examination findings will be limited to deficiency letters. Where staff identifies significant or repeated failures to implement adequate safeguards, particularly following an actual breach or unauthorized disclosure of customer information, the SEC's Division of Enforcement could pursue an enforcement action. Firms that have not already stress-tested their Reg S-P policies and procedures against the rule's substantive requirements should treat the current examination cycle as the last opportunity to close gaps before either outcome materializes.

KEY TAKEAWAYS

Both compliance deadlines have now passed, and the examination cycle is underway. Firms, regardless of size, should consider taking the following steps now:

- Review and update written incident response program documentation.
- Audit vendor relationships and confirm that contracts include the 72-hour breach notification requirement flowing back to the firm.
- Confirm data inventories and data maps are current.
- Ensure evidence of employee security awareness training is documented and retrievable.
- Verify that board or executive-level cybersecurity governance is documented, including committee charters and meeting minutes.
- Compile a log of any security incidents or breaches in the past three years, along with remediation steps taken.

- Review cyber insurance coverage and confirm a current summary is readily available.
- Ensure privacy notices and evidence of client delivery are on file.

Firms that can produce organized, complete documentation on short notice will be far better positioned when an examiner calls.

We will continue to monitor the Division's guidance and related developments and will provide future client updates accordingly. This publication is for guidance only and is not intended to be a substitute for specific legal advice. For questions about your firm's Reg S-P compliance program, please contact Genna Garver, Kim Phan, Brianna Dally, or any member of Troutman Pepper Locke's Privacy + Cyber or Investment Funds + Investment Management practice groups.

RELATED INDUSTRIES + PRACTICES

- Investment Funds + Investment Management Services
- Privacy + Cyber