waystone | Compliance Solutions

Regulation S-P Amendments are Here

The US Securities and Exchange Commission (SEC) has finalized significant amendments to Regulation S-P (Reg S-P), which governs how financial institutions handle the privacy and protection of consumers' Nonpublic Personal Information (NPI).

Overview of the Rule

These S-P updates enhance key components of the regulation, including the:

- **Safeguards Rule:** (which addresses the protection of customer records) and the
- **Disposal Rule:** (which governs the secure disposal of consumer report information).

The Reg S-P amendments introduce important new requirements, such as mandatory incident response programs and customer notification protocols in the event of a data breach. These rule changes mark a critical shift in regulatory expectations, and failure to comply could have significant consequences for your organization.

Compliance updates from the Reg S-P amendments

Here's a breakdown of the key updates:

1. **Incident response program**
   Firms must develop, implement, and maintain written incident response policies to address unauthorized access or use of customer information.

2. **Technical controls & procedures**
   Financial institutions are now required to:
   - Detect, respond to, and recover from unauthorized access to customer data
   - Apply safeguarding and disposal procedures to nonpublic personal information received from other financial institutions — not just your own customers.

3. **Mandatory customer notifications**
   If customer data is — or is reasonably likely to have been — accessed or misused:
   - Notify affected individuals as soon as possible, no later than 30 days from becoming aware
   - You must notify even if your investigation is inconclusive.

Who's affected by Reg S-P?

The amended Regulation S-P expands its reach and imposes enhanced obligations on a broad range of financial institutions. Understanding whether your organization falls under the scope of these changes is essential for Reg S-P compliance. The following outlines the key groups impacted by the rule:

- **Covered Institutions:** Broker-dealers (including funding portals), SEC-registered investment advisers (RIAs), investment companies, and SEC-registered transfer agents.
- **Scope:** Applies to NPI of customers and information received from other financial institutions, expanding protections beyond direct customer relationships.
- **Exclusions:** Foreign (non-resident) brokers, dealers, investment companies and advisers not registered with the SEC are not subject to the rule.

Upcoming compliance dates by entity

Larger Entities:

Must comply by December 3, 2025 (18 months from June 3, 2024, Federal Register publication). Includes broker-dealers not classified as "small entities" under the Securities Exchange Act, RIAs with ≥$1.5Bn AUM (assets under management), and investment companies with ≥$1 billion net assets.

Smaller Entities:

Must comply by June 3, 2026 (24 months from publication). Includes broker-dealers and RIAs classified as small entities (AUM < $1.5Bn).

How to prepare for Reg S-P

The clock is ticking. With the Reg S-P amendments officially in motion, now is the time to move from awareness to action. Whether you're building from the ground up or refining existing data security programs, now is the time to strengthen your security posture and ensure full compliance.

Steps to ensure Reg S-P compliance

Get ahead of the curve by starting with these essential steps:

- review and update your data security program
- build or enhance your incident response plan
- align technical controls with new safeguard rules
- develop a customer notification framework.

Need help navigating Reg S-P compliance?

Download our comprehensive checklist

Our US cyber security compliance experts have developed a practical checklist to help you stay on track with Reg S-P requirements—making it easier to understand the key steps, maintain ongoing compliance, and ensure you're fully prepared for what's ahead.

How can Waystone help

Waystone is a leading provider of cyber security consulting and compliance services to the financial services industry. Our US Compliance Solutions team helps clients navigate the regulatory landscape with confidence, aligning investment strategies and operational processes with compliance requirements.

Our cyber security solutions

With over 100 compliance specialists based across North America, Asia, the Middle East and Europe, we offer a comprehensive range of cyber security solutions, including:

- **Policy development –** assist in drafting and updating Safeguards and Disposal Rule policies, including incident response programs.
- **Risk assessments –** conduct thorough reviews to identify and mitigate data security risks.
- **Service provider oversight –** provide frameworks for due diligence and monitoring of third-party providers.
- **Training and implementation –** deliver compliance training for staff and support integration of compliance processes.
- **Ongoing support –** offer continuous regulatory guidance to ensure sustained compliance with SEC requirements.

If you need help navigating the new Reg S-P amendments or assessing your current compliance measures, reach out to your usual representative or contact us below.

Contact us →