hi@solanasis.com
303-900-8969
solanasis.com

Regulation S-P Readiness Guide

What the updated rule means for your firm and what to do about it

COMPLIANCE DEADLINE: JUNE 3, 2026 (SMALLER ENTITIES)

What Changed

The SEC adopted amendments to Regulation S-P (Safeguards Rule) in May 2024. The updated rule significantly expands what firms must do to protect customer information. If your firm is SEC-registered or state-registered, these requirements apply to you.

The compliance date for smaller entities is **June 3, 2026**. Larger entities had an earlier deadline (December 2025). Let's face it: if you haven't started preparing, you're behind; the technical implementation alone takes weeks to do properly.

The Three Major Requirements

1. Written Incident Response Program

Your firm must have a written program that includes procedures for detecting, responding to, and recovering from unauthorized access to customer information. This is not the same as having a WISP. The incident response program must be a separate, specific set of procedures.

Key requirements:

- Named roles and responsibilities (who does what during an incident)
- Procedures for assessing the nature and scope of any incident
- Containment and remediation steps
- Documentation and evidence preservation requirements

2. Expanded Service Provider Oversight

You must require your service providers to implement and maintain safeguards, and you must monitor their compliance. The rule now explicitly requires that service providers notify you of a security incident **within 72 hours**.

What this means in practice:

- Review vendor contracts for breach notification provisions (most don't have them yet)
- Establish a vendor inventory with access levels and data handled
- Document your oversight process (how you verify vendor security)
- Ensure 72-hour notification language is in all contracts involving customer data

3. Client Notification Requirements

If you discover that customer information was (or is reasonably believed to have been) accessed or used without authorization, you must notify affected individuals as soon as practicable, and no later than **30 days** after becoming aware.

The notification must include:

- Description of the incident in general terms
- Types of customer information involved
- Contact information for questions
- Information about protective measures (credit monitoring, etc.)

What Most Firms Are Missing

Based on our work with RIAs and financial advisory firms, these are the blind spots we find most often. The risk debt is real; firms that look compliant on paper often have the widest gaps in practice.

Incident response exists on paper only

Many firms have an incident response section in their WISP, but it's never been tested. Tabletop exercises and simulated scenarios are not optional; they're how you find out whether your plan actually works before you need it.

Vendor contracts lack notification clauses

The 72-hour notification requirement means every vendor agreement touching customer data needs updated language. Most existing contracts either have no notification clause or specify 30-60 days, not 72 hours.

No vendor inventory exists

You can't oversee what you haven't cataloged. Many firms cannot produce a complete list of vendors with access to customer data, let alone document what access each vendor has and what happens when the relationship ends.

Breach detection is absent

The 30-day notification clock starts when you "become aware." Without detection capabilities (activity monitoring, access anomaly alerts), you may not know about a breach for months. The notification timeline becomes a breach of the notification timeline.

A Practical Readiness Checklist

Use this as a starting point for assessing your firm's Reg S-P readiness. Each item maps directly to the updated rule's requirements.

Incident Response

- ✓ Written incident response program (separate from WISP)
- ✓ Named incident response team with contact information
- ✓ Defined escalation procedures and decision-making authority
- ✓ Evidence preservation and documentation procedures
- ✓ Tabletop exercise conducted within the last 12 months

Service Provider Oversight

- ✓ Complete vendor inventory with data access levels
- ✓ All vendor contracts include 72-hour breach notification
- ✓ Documented vendor oversight process (annual review at minimum)
- ✓ Vendor offboarding procedure (access revocation, data handling)
- ✓ Due diligence records for each vendor handling customer data

Client Notification

- ✓ Notification procedures documented (who decides, who drafts, who sends)
- ✓ Template notification letters prepared and reviewed by counsel
- ✓ Process for identifying affected individuals
- ✓ 30-day notification timeline tracked from point of awareness
- ✓ Credit monitoring or protective measures pre-arranged with a provider

Detection and Monitoring

- ✓ Activity logging enabled on all systems with customer data
- ✓ Anomalous access alerts configured (failed logins, unusual hours, geographic anomalies)
- ✓ Regular log review process (automated or manual)
- ✓ Data loss prevention controls on email and file sharing

Timeline for Getting Ready

If your firm is starting from a typical baseline (WISP exists, basic security in place, no formal incident response testing), here's a realistic timeline:

TIMEFRAME	FOCUS AREA	KEY ACTIONS
Weeks 1-2	Assessment	Gap analysis against Reg S-P requirements. Identify what exists, what's missing, and what needs updating.
Weeks 3-4	Incident Response	Draft or update incident response program. Assign roles, define procedures, prepare templates.
Weeks 5-6	Vendor Oversight	Complete vendor inventory. Begin contract review and amendment process for 72-hour notification.
Weeks 7-8	Detection & Notification	Implement or verify monitoring. Prepare notification procedures and templates.
Weeks 9-10	Testing	Tabletop exercise. Disaster recovery test. Verify the whole system works end to end.
Ongoing	Maintenance	Quarterly reviews. Annual testing. Vendor contract renewals with updated language.

The Role of Your Compliance Consultant

Your compliance consultant handles the regulatory interpretation: what the rule requires, how it applies to your specific registration status, and how to document your compliance program. They handle the "what" and "why."

The technical implementation is a separate effort: configuring monitoring, testing disaster recovery, reviewing vendor security configurations, and documenting evidence. That's where firms like Solanasis come in. We handle the "how" and provide the proof.

How Solanasis Can Help

Our 10-day Compliance Readiness Assessment covers every item on the checklist above. We test what others only check on paper, including a real disaster recovery restore, and we map every finding to Reg S-P, SEC exam priorities, and NIST CSF.

After the assessment, you can execute the roadmap independently, bring us in for a remediation sprint, or engage us as an ongoing Fractional Cybersecurity Partner; no lock-in at any stage.

Book a 30-minute conversation: go.solanasis.com/intro

Download the free compliance checklist: go.solanasis.com/checklist

BOOK A CALL