Regulation S-P Readiness Checklist

For Smaller Financial Firms

COMPLIANCE DEADLINE: JUNE 3, 2026

STACK CYBERSECURITY

What the Regulation Requires

Who it covers

Registered investment advisers under $1.5B AUM, smaller broker-dealers, investment companies, funding portals, and transfer agents.

Written programs required

Firms must maintain documented policies for incident response, customer notification, vendor oversight, and recordkeeping.

Your deadline

Larger firms were required to comply by Dec. 3, 2025. Smaller firms must comply by June 3, 2026.

The Two Requirements Most Firms Will Struggle With

30 DAYS

Customer Notification Requirement

When sensitive customer information is compromised, your firm has 30 days to assess what happened, determine notification is required, and deliver it. That requires pre-approved templates, assigned roles, and a decision process — in place before an incident occurs.

72 HOURS

Vendor Breach Notification Requirement

Service providers must notify your firm within 72 hours of discovering a breach involving your customer data. Many large vendors don't include this language by default. If your contracts don't require it, you have a gap.

01

Data Awareness and Mapping

Confirm your firm understands what customer information it holds and how it moves through the business.

- [ ] **IDENTIFY ALL CUSTOMER INFORMATION CATEGORIES**
  Confirm every category of data your firm collects, stores, or accesses.

- [ ] **DOCUMENT SYSTEMS AND DATA FLOWS**
  Inventory all systems and map how data moves between systems, vendors, and users.

- [ ] **IDENTIFY ALL SERVICE PROVIDERS**
  Maintain a current list of every third party that touches customer data.

- [ ] **REVIEW DATA FOR SECURE DELETION**
  Assess whether unnecessary or outdated customer data has been identified and disposed of.

02

Written Incident Response Program

Confirm your firm has a formal, documented incident response capability.

- [ ] **WRITTEN INCIDENT RESPONSE PLAN EXISTS**
  The plan is formally approved and defines how to detect, investigate, and contain unauthorized access.

- [ ] **ROLES AND RESPONSIBILITIES ARE ASSIGNED**
  Staff know their specific duties before an incident occurs, not after.

- [ ] **RECOVERY AND REMEDIATION PROCEDURES**
  The plan includes documented steps for restoring systems and customer data.

- [ ] **PLAN COVERS ASSESSMENT AND SCOPE DETERMINATION**
  Procedures exist to determine which systems and data were affected.

03

Breach Notification Preparedness

Confirm your firm can meet the SEC's 30-day customer notification requirement.

- [ ] **PROCESS TO ASSESS BREACH SCOPE**
  Your firm can determine whether 'sensitive customer information' was compromised and document that decision.

- [ ] **NOTIFICATION DECISION PROCESS**
  A documented procedure defines when notification is required and who authorizes it.

- [ ] **PRE-APPROVED NOTIFICATION TEMPLATES**
  Templates are ready and include what happened, what data was affected, and customer protection steps.

- [ ] **30-DAY EXECUTION CAPABILITY**
  The firm has tested its ability to identify, assess, and deliver notifications within the deadline.

04

Service Provider Oversight

Confirm your firm has control over third parties that handle customer data.

- [ ] **VENDOR CONTRACTS ADDRESS DATA PROTECTION**
  Agreements include requirements to safeguard customer information.

- [ ] **72-HOUR BREACH NOTIFICATION REQUIREMENT**
  Contracts explicitly require vendors to notify your firm within 72 hours of discovering a breach.

- [ ] **VENDOR RISK ASSESSMENTS ARE DOCUMENTED**
  Security posture is assessed during onboarding and reviewed periodically.

- [ ] **ONGOING MONITORING PROCESS EXISTS**
  A defined process tracks vendor security posture over time.

05

Policy and Procedure Updates

Confirm existing policies reflect the amended rule's expanded scope.

- [ ] **POLICIES REFLECT EXPANDED DEFINITION**
  Privacy and security policies address the broader definition of 'customer information,' including vendor-held data.

- [ ] **INCIDENT RESPONSE AND NOTIFICATION COVERAGE**
  Policies address how to respond, when to notify customers, and how to oversee service providers.

- [ ] **DOCUMENTATION IS CURRENT AND ACCESSIBLE**
  Written policies are up to date and available for examination.

06

Documentation and Recordkeeping

Confirm your firm can demonstrate compliance, not just claim it.

- [ ] **INCIDENT INVESTIGATIONS ARE DOCUMENTED**
  Records of every investigation, including decisions made, are retained.

- [ ] **VENDOR DUE DILIGENCE IS ON FILE**
  Documentation of vendor assessments and agreements is maintained and accessible.

- [ ] **NOTIFICATION COPIES ARE ARCHIVED**
  Copies of any customer notifications sent are retained as part of the compliance record.

- [ ] **EVIDENCE SUPPORTS EACH REQUIREMENT**
  Documentation exists that demonstrates compliance with every area of the rule.

07

Testing and Employee Training

Confirm that your controls work in practice.

STAFF TRAINING ON UPDATED POLICIES

☐ Employees understand how to recognize a potential incident and know the reporting process.

INCIDENT RESPONSE PLAN IS TESTED

☐ Tabletop exercises or simulations have been conducted to verify the plan functions as written.

LESSONS LEARNED ARE INCORPORATED

☐ Findings from testing are documented and used to update controls and procedures.

Immediate Actions

1 **IDENTIFY ALL CUSTOMER DATA LOCATIONS**

Every system and vendor that touches customer information, including platforms managed on your behalf.

2 **AUDIT VENDOR CONTRACTS FOR THE 72-HOUR CLAUSE**

Review every service provider agreement and confirm breach notification timelines are defined and enforceable.

3 **BUILD OR UPDATE YOUR INCIDENT RESPONSE PLAN**

Assign roles, define the assessment process, and prepare customer notification templates before you need them.

4 **RUN A TABLETOP EXERCISE**

Walk through a breach scenario and determine whether your firm can meet the 30-day notification deadline.

STACK CYBERSECURITY

Find gaps you can't close on your own?

STACK Cybersecurity helps financial firms build incident response programs the SEC expects to see.

Schedule a Gap Assessment

(734) 744-5300 • info@stackcyber.com • stackcyber.com