

REGULATION S-P AMENDMENTS

INCIDENT RESPONSE. CUSTOMER NOTIFICATION. DEFENSIBLE RECORDKEEPING.

The SEC amended Regulation S-P to require covered institutions to formalize incident response, document harm determinations, and notify affected individuals within strict timelines.

What's changed: regulators will assess not only what decision was made, but whether the decision process was consistent, reasonable, and documented.

WHO IS COVERED

- Broker-dealers, including funding portals
- Registered investment advisers
- Investment companies
- Transfer agents

KEY DATES

Effective date: August 2, 2024

Compliance deadlines:

- Larger entities: December 3, 2025
- Smaller entities: June 3, 2026

WHAT THE AMENDMENTS REQUIRE



CONSISTENCY IS NOW SCRUTINIZED

Policies and procedures reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information.



30-DAY FEDERAL NOTIFICATION CLOCK

If unauthorized access to or use of sensitive customer information occurred or is reasonably likely, firms must notify affected individuals: As soon as practicable, but no later than 30 days after becoming aware. The 30-day clock begins when the firm becomes aware of the incident.



RECORDKEEPING

Firms must preserve records of:

- Incident response policies
- Investigations and determinations
- Customer notifications
- Service provider oversight
- Records must be retained consistent with existing SEC books and records requirements.



SERVICE PROVIDER OVERSIGHT

Firms must:

- Maintain written policies to oversee service providers
- Ensure providers protect customer information
- Require providers to notify the firm as soon as possible, but no later than 72 hours after becoming aware of a breach affecting a customer information system they maintain.



PRESUMPTION OF NOTIFICATION

Notification is required unless, after a reasonable investigation, the firm determines the information has not been and is not reasonably likely to be used in a manner that would result in substantial harm or inconvenience. That investigation and determination must be documented.

A vendor may send notices on your behalf, but regulatory responsibility remains with the firm.



CONSEQUENCES OF NON-COMPLIANCE

- SEC examination findings
- Required remediation programs
- Supervisory control deficiencies
- Enforcement actions
- Reputational damage and client trust erosion

Regulators will assess not only what decision was made, but whether the decision process was consistent, reasonable, and documented.



WHERE FIRMS ARE MOST EXPOSED

- SEC examination findings
- Required remediation programs
- Supervisory control deficiencies
- Enforcement actions
- Reputational damage and client trust erosion

These gaps don't just slow response, they create exam exposure because the firm can't prove what happened, when, and why.

HOW RADAR PRIVACY™ OPERATIONALIZES REGULATION S-P

STRUCTURED ASSESSMENT WORKFLOW

Guided decisioning aligned to regulatory criteria.

TIMELINE MANAGEMENT

Track awareness date, escalation, and task completion.

VENDOR OVERSIGHT CONTROLS

Centralized intake and documentation of 72-hour notices.

EXAM-READY AUDIT TRAIL

Timestamped decisions, rationale, evidence, and exportable reporting.

BUILT FOR REGULATORY SCRUTINY

Standardized risk assessment tied to Reg S-P

Heat map (risk scoring + "sensitive" data elements)

Heat map scoring and 'sensitive customer information' identification are captured as part of the decision record, supporting Reg S-P documentation and record keeping expectations.

Notification orchestration with proof of execution

Radar tracks notification decisions, owners, due dates, and completion status in one system of record, reducing reliance on email threads and spreadsheets.

CONSISTENT. OPERATIONALIZED. DEFENSIBLE.

SCHEDULE A 20-MINUTE REG S-P WORKFLOW REVIEW

TAKE THE 5-MINUTE REG S-P READINESS ASSESSMENT HERE.