troutman pepper locke

Checklist: What Small Firms Must Have in Place by June 3, 2026

1. Written, Risk-Based Incident Response Program

Small firms must adopt written policies and procedures reasonably designed to:

- ❑ **Detect** unauthorized access to or use of customer information.
- ❑ **Contain** and control such incidents.
- ❑ **Assess** the nature and scope of any incident.
- ❑ **Recover** and restore systems and data.
- ❑ **Notify** affected individuals where required.
- ❑ **Oversee service providers** involved in the incident or relevant systems.

For smaller firms, this program should be tailored to:

- ❑ Firm size and staffing.
- ❑ Number and type of systems and applications.
- ❑ Use of third-party service providers and cloud platforms.
- ❑ Nature and volume of customer information.

Securities and Exchange Commission (SEC) staff have indicated that they will look for evidence that the incident response program is actually implemented and tested.

2. Customer Breach Notification Process

Covered institutions must provide notice to customers:

- ❑ As soon as possible, but no later than 30 days after becoming aware of unauthorized access to or use of customer information involving sensitive customer information, unless the firm determines that the incident is not reasonably likely to result in harm.
- ❑ Any determination that notification is not required must be based on a reasonable investigation and reached within that 30-day window.

To meet this standard, small firms should:

- ❑ Establish a clear internal escalation path when a potential incident is detected.
- ❑ Define roles and responsibilities for IT, compliance, legal, and senior management.

3. Risk Register or Risk Matrix Tailored to the Firm

The SEC has indicated it expects firms to maintain a risk register or matrix that:

- ❑ **Identifies Risks**
  - ❑ Based on the firm's network footprint (on-premises, cloud, hybrid).
  - ❑ Types of customer information held.
  - ❑ Business lines and products.
  - ❑ Use of mobile devices and remote work.

- **Assesses Risks**
  - Using a structured scale (*e.g.*, critical/high/medium/low or numerical scoring).
  - Taking into account likelihood and impact.
- **Mitigates Risks**
  - By documenting whether the firm will avoid, reduce, transfer, or accept each risk.
  - Describing specific controls (technical, administrative, contractual) for higher risk areas.

4. Robust Oversight of Third-Party Service Providers

Smaller firms often rely heavily on IT vendors, cloud providers, and outsourced compliance or cybersecurity support.

The SEC has stressed that:

- Regulation S-P obligations ultimately remain with the firm, not the vendor.
- Firms must conduct due diligence on service providers both at onboarding and on an ongoing basis.

By June 3, 2026, small firms should:

- Inventory all vendors that access, store, or process customer information.
- Ensure written agreements with these vendors address, at a minimum:
  - Safeguarding and disposal obligations consistent with amended Reg S-P.
  - Incident detection, reporting timelines, and cooperation requirements.
  - Notification obligations in the event of a breach affecting the firm's customers.
  - Rights to obtain logs, reports, and other evidence necessary for incident investigation.
- Document vendor oversight activities, such as:
  - Reviewing audits.
  - Requesting security questionnaires or attestations.
  - Holding periodic meetings to discuss cybersecurity and data protection.

5. Updated Policies, Procedures, and Training

The Reg S-P amendments require that policies and procedures reflect enhanced safeguards, disposal, and incident response requirements, and that firms can demonstrate that they have implemented them.

Small firms should:

- **Update Written Policies and Procedures**
  - Privacy notices and GLBA policies.
  - Safeguards and information security policies.
  - Data retention and secure disposal procedures.
  - Incident response plan and breach notification procedures.
  - Vendor management and oversight policies.

- ❑ **Train Personnel**
  - ❑ Provide training to all staff on:
    - ❑ The importance of protecting customer information.
    - ❑ How to recognize and escalate potential incidents.
    - ❑ Their roles under the incident response plan.
  - ❑ Conduct more targeted training for IT, compliance, and management on the new requirements.
- ❑ **Conform Privacy Notices to the FAST Act**
  - ❑ Determine whether the firm meets conditions that allow it to forego annual privacy notices.
  - ❑ If so, update processes accordingly while still ensuring customers are informed, consistent with Reg S-P.

6. Prepare for the SEC Examination Lifecycle

- ❑ Understand the firm environment
  - ❑ Number and locations of offices.
  - ❑ Whether and how you use hybrid or remote work.
  - ❑ Where customer information resides (on-premises, cloud, third-party systems).
  - ❑ How data flows into, through, and out of the firm's systems.
- ❑ Review Documentation
  - ❑ Incident response plan and any incident logs or reports.
  - ❑ Risk register or risk matrix.
  - ❑ Data mapping diagrams or descriptions.
  - ❑ Vendor contracts and due diligence materials.
  - ❑ Other policies and procedures.
  - ❑ Evidence of training and tabletop exercises.
- ❑ Conduct Interviews
  - ❑ With the firm's executive leadership and any outside IT provider.
  - ❑ Test whether day-to-day practices match written policies.