New SEC Cybersecurity Compliance Deadlines are Coming: What 5 Things Should Covered Institutions Do to Prepare?

Insights
6.27.25

The SEC's amended Regulation S-P, adopted last year, will soon enhance data privacy protections for broker-dealers, investment companies, registered investment advisors, and transfer agents. The updated rule requires these covered institutions to implement written policies and procedures for an incident response program designed to detect, respond to, and recover from unauthorized access to customer information. Although the compliance deadlines (**December 3, 2025,** for large firms, and **June 3, 2026,** for small firms) might seem far in the distance, it is essential to start acting now to ensure full compliance before the deadlines kick in. Here are five things you should do now to start preparing.

1. Adopt or Update Incident Response Program for Customer Information

Covered Institutions must establish and maintain written policies and procedures to safeguard ***customer information*** through administrative, technical, and physical safeguards. These policies must ensure data security, protect against anticipated threats, and prevent unauthorized access that could harm consumers.

Customer information refers to any nonpublic personal data held by a financial institution or its service providers.

- This includes records tied to individual customers of the institution or customers of other financial entities if the data has been shared.
- For transfer agents, customer information specifically applies to securityholders of issuers they serve.
- Customer information systems are the physical and virtual infrastructures financial institutions use to store, process, and manage customer data, ensuring security, accessibility, and regulatory compliance.

Note: "Customer Information" replaced "Customer records and information" in the updated regulation. The SEC acknowledged that customer records and information was not defined in the GLBA or in Regulation S-P. To align with the information protected by both rules, customer information is now utilized.

2. Develop Additional Measures for Sensitive Customer Information

Institutions must also implement a response program to detect, contain, and recover from unauthorized access, including prompt notification to affected individuals if their ***sensitive customer information*** was compromised.

Sensitive customer information means customer information alone or with any other information, which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information. Other information includes:

- Social Security number
- State- or government-issued driver's license or identification number
- Alien registration number
- Passport number
- Employer or taxpayer identification number
- Biometric record
- Unique electronic identification number, address, or routing code
- Telecommunication identifying information or access device
- Customer information identifying an individual or the individual's account, including their account number, name or online user name, in combination with authenticating information, or in combination with similar information that could be used to gain access to the customer's account such as an access code, a credit card expiration date, a partial Social Security number, a security code, a security question and answer identified with the individual or the individual's account, or the individual's date of birth, place of birth, or mother's maiden name.

3. Create Due Diligence Procedures

Those service providers handling customer data must also follow due diligence procedures, reporting breaches within 72 hours and assisting with customer notifications when required. **Importantly, the 72-hour notice is triggered by unauthorized access to a customer information system maintained by the service provider, *not* the impact to sensitive customer information.** Ultimately, the Covered Institution remains responsible for ensuring proper breach response and consumer notification.

- **Service provider** means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution.

4. Be Ready to Notify Individuals

Covered Institutions must provide a clear and conspicuous notice to each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorized.

- If the Covered Institution is unable to identify which specific individuals' sensitive customer information has been accessed or used without authorization, it must provide notice to all individuals whose sensitive customer information resides in the customer information system that was, or was reasonably likely to have been, accessed or used without authorization.
- The timing of the notice must occur as soon as practicable but not later than **30 days** after becoming aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred.
- **Tip:** The new rule contains specific notice content requirements that need to be included, including general details about the incident; the date or timeframe of the breach, if known; contact information for affected individuals to inquire further; a recommendation that the customer review account statements and immediately report any suspicious activity to the Covered Institution; a fraud alert explanation including how to place a fraud alert; a recommendation to review credit reports and how to obtain a free credit report; and information about the FTC and usa.gov.

What if there isn't any harm to the individual? Notice is not required if the Covered Institution determines that the sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience to the individual after it conducts a reasonable investigation of the facts and circumstances of the incident. The SEC declined to add a safe harbor for encryption into the regulation.

However, the agency emphasizes that proper encryption can mitigate the risk of unauthorized access to customer information. If data is encrypted in a manner that renders it unreadable, Covered Institutions may not be required to notify affected individuals in the event of a breach. This aligns with the broader regulatory approach that considers encryption a key safeguard in protecting consumer financial data. Currently, there is no specific reporting requirement to the SEC as it relates to the amendment.

5. Dispose of Unnecessary Consumer and Customer Records and Maintain Policies and Procedures

Dispose: Covered Institutions, excluding notice-registered broker-dealers, must take reasonable measures to ensure secure disposal of consumer and customer information to prevent unauthorized access. They are required to implement written policies and procedures that outline proper disposal practices. However, these requirements do not override other laws related to record retention or destruction, nor do they impose additional obligations beyond existing legal standards.

Maintain: Covered Institutions must maintain written policies and procedures related to data security, incident response, and breach notification. They must also document unauthorized access incidents, response actions, and notification decisions, including any delays authorized by the US Attorney General. Additionally, records of contracts with service providers and procedures for proper data disposal must be kept. The below chart outlines the retention periods. The takeaway is that the SEC wants Covered Institutions to periodically reassess the effectiveness of their safeguarding and disposal programs.

Covered Institution	**Retention Period**
Covered Institution Registered and Unregistered Investment	Policies and Procedures. A copy of policies and procedures in effect, or that at any time in the past six years were in effect, in an easily accessible place. Other records. Six years, the first two in an easily accessible place.
Registered Investment Advisers	All records for five years, the first two in an easily accessible place.
Broker-Dealers and Transfer Agents	All records for three years, in an easily accessible place.

Special Note: Which Category Do You Fall Into?

- **Small Entities:** The amendments will likely increase operational costs for small Covered Institutions. Developing and maintaining the required written policies and procedures, implementing incident response programs, and conducting periodic risk assessments all require financial resources. Small Covered Institutions operating on tight margins may find these additional costs particularly burdensome.
- **Larger firms** must comply within 18 months (December 3, 2025), while smaller firms have 24 months (June 3, 2026) after the rule's publication. Large firms are defined as:
    - **Investment companies** together with other investment companies in the same group of related investment companies > net assets of $1 billion or more as of the end of the most recent fiscal year.
    - **Registered investment advisers** > $1.5 billion or more in assets under management.
    - **Broker-dealers:** All broker-dealers that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act.
    - **Transfer agents:** All transfer agents that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act.

Conclusion

For further information, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on the firm's Data Protection and Cybersecurity Team and the Consumer Privacy Team. The teams are equipped to help organizations implement the necessary policies and procedures to comply with the upcoming deadlines. Our teams can also assist organizations review existing service provider contracts.

Fisher Phillips will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. You can also visit FP's U.S. Consumer Privacy Hub for additional resources to help you navigate this area.

Related People

Daniel Pepper, CIPP/US
Partner
303.218.3661
Email

Jillian Seifrit, CIPP/US
Associate
610.230.6129
Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

Data Protection and Cybersecurity