

# 4 Compliance Challenges With Amended Regulation S-P



The deadline for Amended Regulation S-P (“Amended Reg S-P”) is quickly approaching, and unlike many recent rules, the SEC [made it clear](#) that this one will stay the course.

Below are 4 key challenges advisers are facing with regards to complying with Amended Reg S-P. Understanding these challenges (and how to navigate them) may help both larger and smaller entities (who must comply by Dec. 3, 2025, and June 3, 2026, respectively) to anticipate and navigate some of the trickiest aspects of the new rule.



## 4 Compliance Challenges for RIAs

### 1 Ensuring 72-hour Service Provider Notification

Under Amended Reg S-P, a covered institution’s incident response program must include written policies and procedures to ensure service providers provide notification to the covered institution as soon as possible, but no later than 72 hours after becoming aware that a breach in security has occurred, resulting in unauthorized access to a customer information system maintained by the service provider. It is this notification that alerts a covered institution to initiate its incident response program for breaches of systems outside of the covered institution’s control.

The proposed rule required covered institutions to enter into a written contract with service providers to take appropriate measures to comply with Amended Reg S-P, including agreeing to provide notice of a breach to the covered institution. The final rule softened this stance, and written contracts covering Amended Reg S-P are not required. The SEC staff that participated in the SEC’s Compliance Outreach [Webinar](#) on Amended Regulation S-P for Large Firms, emphasized this change in the final rule.

Firms are not required to enter into written agreements to provide notice, however, the challenge is that firms must ensure that service providers provide notice.



#### *Considerations*

If you can amend your contract with a service provider, treat the notification of a breach within 72 hours as a non-negotiable provision. The firm bears all of the compliance risk, and without a contractual obligation, it is challenging to ensure the service provider will provide such notice within the first 72 hours.

For service providers that will not amend existing contracts, perform advanced due diligence, incorporate attestation, acknowledgments, or any other method to evidence your attempts to ensure notice is provided. It is also a best practice to keep a pulse on breaches occurring in the industry, in case one of your service providers experiences a breach and is delayed in notifying or unable to notify you.

## 2 Customer Information is Broad

Under Amended Reg S-P, customer information is “any record containing nonpublic personal information” about a customer of a financial institution that is handled or maintained by the covered institution or on its behalf. The scope is very broad. Information is included in the definition regardless of whether such information pertains to customers of the covered institution, or “to customers of other financial institutions where such information has been provided to the covered institution.” This broad scope was also emphasized by SEC staff at the Compliance Outreach Webinar. Both nonpublic information about your customers’ information *and* any nonpublic information about customers of other institutions.

Nonpublic personal information is further defined as personally identifiable financial information and any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is *not* publicly available information. In the adopting release, the SEC staff responded to a commenter questioning the broad scope of customer information, and indicated the broad scope was intentional to ensure all information covered by the requirements of the Gramm-Leach-Bliley Act is safeguarded and sufficiently assessed.

A compliant incident response program must have written policies and procedures to:

- i. Assess the nature and scope of any incident involving unauthorized access to or use of *customer information* and identify the *customer information systems* and types of *customer information* that may have been accessed or used without authorization;
- ii. Take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of *customer information*; and
- iii. Notify each affected individual whose *sensitive customer information* was, or is reasonably likely to have been, accessed or used without authorization in accordance with the notification obligations discussed below, unless the covered institution determines, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of *sensitive customer information*, 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. (*emphasis added*)

Understandably, this has created a lot of confusion for advisers as they work to determine which vendors must be included in their vendor management programs under Amended Regulation S-P.

### Considerations

While covered institutions must assess customer information and systems containing it and must take appropriate steps to contain and control unauthorized access of customer information, the third requirement to notify affected individuals has a higher standard. Notification is for *sensitive* customer information.

To determine if an incident likely accessed sensitive customer information, a covered institution must be aware of all customer information:

- **Step 1** – Understand where ALL customer information is located. Map out all systems that handle or maintain customer information and do the same for any service providers. This is not an easy task, so start now.
- **Step 2** – If a ransomware attack locks you out of a system, you will not be able to see what information is there. Detail the nature of customer information in each system. This must be completed proactively.
- **Step 3** – Maintain this customer information map and repeat this process as systems, service providers, and your business changes. With a current customer information map, you will be able to determine if sensitive customer information was or is reasonably likely to have been accessed.

### 3 For Shared Information, Which Covered Institution Must Send Notification?

Since the definition of customer information includes information pertaining to your customers and the customers of other financial institutions where you have no preexisting customer relationship, this raises the question: Which covered institution is obligated to send notice?

In the proposed rule, multiple covered institutions could have been required to notify the same affected individuals about the same incident. Commenters pointed to this outcome as duplicative and burdensome, and confusing to customers. Commenters argued that covered institutions might not even have the contact information for customers of another covered institution. For these reasons, the SEC staff made an adjustment in the final rule.



#### **Considerations**

Under the final rule, a covered institution must provide notice where unauthorized access to or use of sensitive customer information has occurred at the covered institution or one of its service providers that is not itself a covered institution. In the staff's view, since the incident occurred at the covered institution or one of its service providers, that covered institution has the most information about the incident to properly notify affected individuals. A few examples under the final rule:

- An incident occurs in the systems of X, a covered institution, which affects X's customers.
  - X must notify X's customers within 30 days.
- An incident occurs in the systems of X, a covered institution, which affects customers of X and of Y, another covered institution that did not experience the breach.
  - X must notify the customers of both X and Y within 30 days.
- A service provider of X experiences an incident affecting X's customers.
  - X must ensure the service provider, which is not a covered institution, notifies X within 72 hours of such a breach, and X must notify X's customers within 30 days.
- A service provider of X, but not of Y, experiences an incident affecting customers of both X and Y.
  - X must ensure the service provider, which is not a covered institution, notifies X within 72 hours of such a breach, and X must notify the customers of both X and Y within 30 days.

The staff "appreciated" that a covered institution may not have access to the contact information for some customers, but indicated that the covered institution can coordinate with the other covered institutions that do have a customer relationship to receive contact information as needed. Furthermore, under the rule, covered institutions must either provide notice or ensure such notice is provided. This means that you could coordinate with another covered institution or a third party and have them provided notice, so long as you could ensure it satisfied the rule and the rule's timing requirements. Compliance programs will have to work carefully through this added layer of complication when responding to an incident.

## 4 Government Shutdown

Another challenge for large entities to comply by the December 3rd deadline is the confusion and loss of urgency prompted by the government shutdown. The SEC's Compliance Outreach [Webinar](#) on Regulation S-P for Large Firms was held just before the government shutdown. It was the first of three planned sessions, though it is anyone's guess when those additional sessions will occur.

### Considerations

**Remember: Just because the government has shutdown does not mean you can ignore your compliance obligations.**

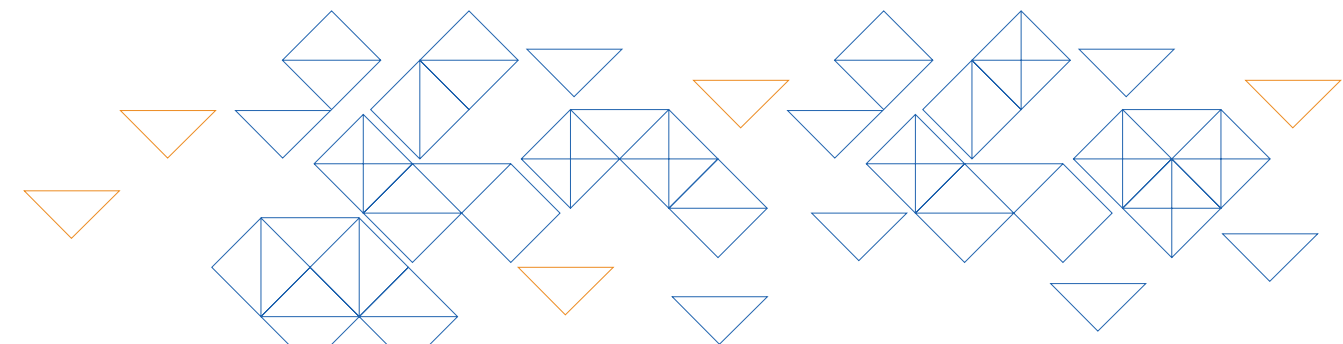
Now, as in past government shutdowns, all deadlines are still live. The first SEC examinations on Amended Reg S-P will look back to the deadlines of the final rule. SEC Examiners will check for the adoption of written policies and procedures, records of compliance activities, and responses to any incidents. The 2025 Examination Priorities published by the SEC mention Amended Reg S-P, and the new rule will continue to be a priority for the near future. This rule has always had bipartisan support, passed with a unanimous 5-0 vote by the commission, and fits into the cyber examination process the Division of Examinations has followed for over ten years.

The SEC has been steadfast in its approach to this rule. Compliance programs must rise to meet these challenges.



### We're here to help.

Fairview's cyber team offers full support for complying with Amended Regulation S-P, including written policies and procedures for Incident Response Plans, development and maintenance of Vendor Management Programs, and more. If you have questions or need help, [let us know](#).



### About Fairview

Founded in 2005, Fairview<sup>®</sup>, LLC provides a full range of back-office support services for investment advisers and other financial institutions.

For more information, visit [FairviewInvest.com](https://FairviewInvest.com).

