Salus GRC

Whitepaper

Understanding the Reg. S-P Requirements

A Plain English Guide

Contents

Introduction

Cybersecurity incidents just got a lot more challenging for financial institutions to navigate, thanks in part to recent rule amendments adopted by the U.S. Securities and Exchange Commission on May 15, 2024.

The SEC voted to update Regulation S-P (the “Safeguards Rule”) to provide a consistent framework for responding to cybersecurity incidents relating to the breach of nonpublic personal information. In the following guide, Salus GRC breaks down the rule requirements into plain English and offers practical tips for firms to implement the rule changes in their compliance and cybersecurity programs.

The Four Horsemen

When a cybersecurity incident occurs, it can be a traumatic experience for any organization to both put out the immediate fires and address the crisis afterwards. As amended, Regulation S-P will require firms covered by the rule to bolster their incident response capabilities in four ways. But unlike the Four Horsemen, these four rule requirements aren't intended for cyber incidents to be harbingers of the apocalypse. Rather, these four requirements are designed to improve planning and response actions so that when cybersecurity incidents do happen (and they will happen), your firm will be prepared.

The four pillars of the Safeguards Rule are:

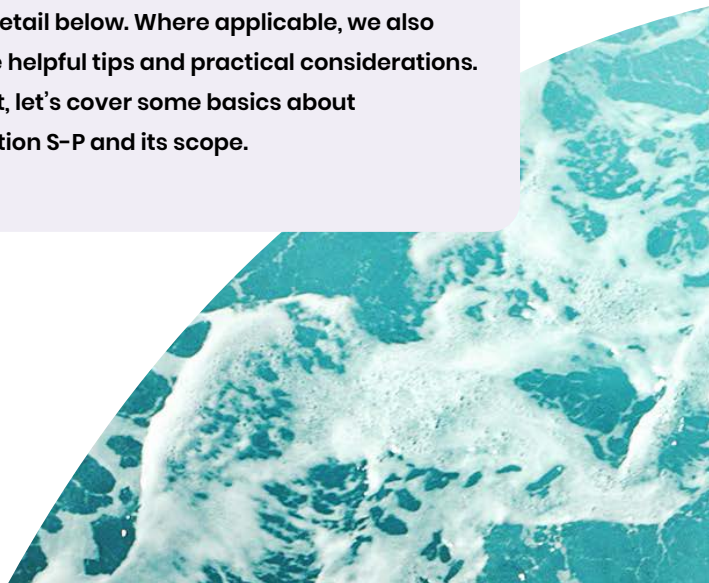
1. Incident Response Program.
Firms must adopt, implement, and maintain a comprehensive, written incident response plan ("IRP"). The IRP must include policies and procedures reasonably designed to help a firm "detect, respond to, and recover from unauthorized access to or use of customer information."

2. Breach Notification.
Firms must "provide notice to individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization," with the notices sent "as soon as practicable, but not later than 30 days, after becoming aware that the incident occurred or is reasonably likely to have occurred."

3. Service Provider Oversight.
Firms must "establish, maintain, and enforce written policies and procedures reasonably designed" to oversee and monitor service providers with access to sensitive customer information.

4. Recordkeeping.
Firms must document and maintain written records to evidence compliance with the Safeguards Rule.

We will describe each of these requirements in more detail below. Where applicable, we also include helpful tips and practical considerations. But first, let's cover some basics about Regulation S-P and its scope.



Who Does the Rule Apply To?

As a threshold matter, Regulation S-P applies to:

1. Investment companies, regardless of whether or not they are required to register with the SEC; consequently, it applies to business development companies (BDC's) as well;

2. Registered investment advisers providing advisory services to natural person customers. This will generally include retail wealth management firms serving high net worth clients and other individuals. It also includes advisers to separately managed accounts (SMAs) for such individuals.

3. Broker-dealers; and

4. Transfer agents registered with the SEC.

On the other hand, the Safeguards Rule does not apply to advisers to private funds who rely on the Investment Company Act Section 3(c)(1) or 3(c)(7) exemptions from registration. This means that advisers to most hedge funds, private equity funds, and other private funds are not subject to Regulation S-P.

Practical Tips:

- Many private fund advisers do maintain policies and procedures in the spirit of Regulation S-P, and they could still be subject to similar requirements under a broad reading of other SEC rules such as Advisers Act Rule 206(4)-7, the adviser's fiduciary duty, or similar expectations for robust incident response plans from institutional investors.

- Because exempt reporting advisers (ERAs) are not required to register with the SEC, ERAs are technically not required to comply with Regulation S-P.

What Information Does the Rule Cover?

Investment advisers and investment companies maintain a significant amount of personally identifiable information (PII) about their clients and investors, either directly or in conjunction with third party service providers, subadvisers, and affiliates. This information can range from names and email addresses to information about investment objectives.

Regulation S-P applies to "customer information in a covered institution's possession or that is handled or maintained on the covered institution's behalf." This means data you collect and share with third parties to help service your customers' accounts is still in scope because that information is maintained on your behalf.

However, breach notification is not required just because any PII is accessed. Notification ultimately depends on what type of PII was involved in a cybersecurity incident. Firms are required to notify customers only when a subset of PII known as *sensitive customer information* is involved.

Definition:

- **Sensitive Customer Information** is "any component of customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information."

Phrased other way, information is considered sensitive customer information if it has a higher risk of substantial harm or inconvenience if exposed because it would increase the risk of fraud, identity theft, or similar harms.

Practical Tips:

- The SEC provides examples of such sensitive customer information. The list is not exhaustive but includes Social Security numbers, driver's license numbers, alien registration numbers, government password numbers, Tax ID numbers, biometric records, a unique electronic identification number, address or routing code, a telecommunication identifying information or an access device. (adopting release, footnote 121)

- Sensitive customer information is broader than the commonly listed types of PII mentioned above. The SEC provides examples of information which, in combination with other data, could be sensitive customer information. These include other information identifying a customer, such as a name or online username, in combination with authenticating information such as a partial Social Security number, access code, or mother's maiden name. (adopting release, footnote 122)

Understanding the Four Pillars of the Safeguards Rule

Now that you have a better sense of who is subject to the rule and what data is in scope, let's dissect the four key requirements applicable to covered firms. Specific citations and footnotes from the adopting release are included where helpful for additional context.

Incident Response Program

Firms are required to "develop, implement, and maintain written policies and procedures for an incident response program" (also known as an incident response plan) that is "reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information." The incident response plan, or IRP, must include procedures "to 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. The IRP must also include procedures for the firm to "take appropriate steps to contain and control the incident to prevent further unauthorized access or use."

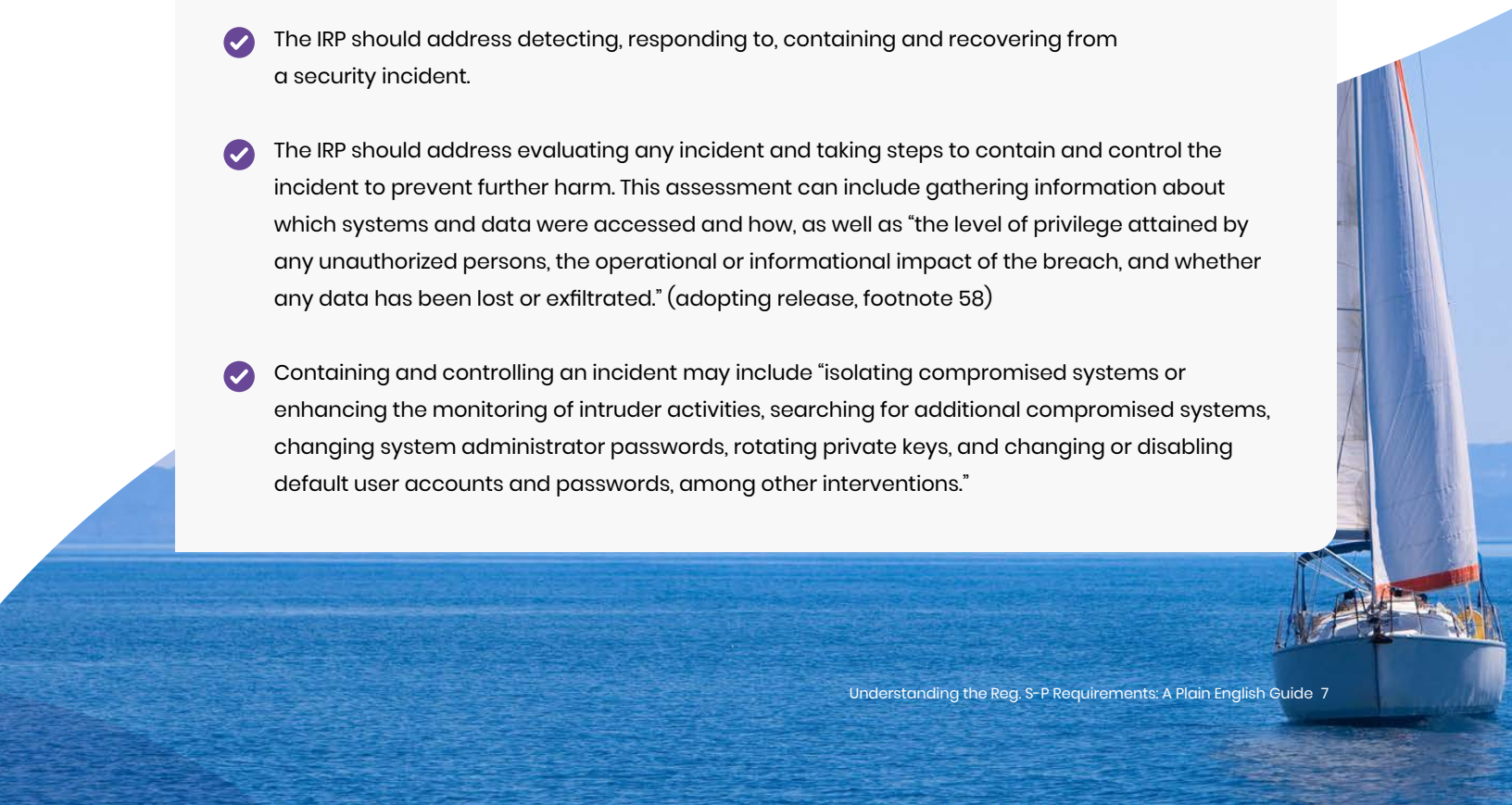
Practical Tips:

- Develop or revise your IRP to define a security incident as including an "incident involving unauthorized access to or use of customer information," and specifically define sensitive customer information to include the definition referenced in Section 248.30(d)(9) of the final rule. This distinction is important because the IRP should address unauthorized access to any customer information as well as other types of incidents, but breach reporting is only required for incidents involving unauthorized access to sensitive customer information.

- The IRP should address detecting, responding to, containing and recovering from a security incident.

- The IRP should address evaluating any incident and taking steps to contain and control the incident to prevent further harm. This assessment can include gathering information about which systems and data were accessed and how, as well as "the level of privilege attained by any unauthorized persons, the operational or informational impact of the breach, and whether any data has been lost or exfiltrated." (adopting release, footnote 58)

- Containing and controlling an incident may include "isolating compromised systems or enhancing the monitoring of intruder activities, searching for additional compromised systems, changing system administrator passwords, rotating private keys, and changing or disabling default user accounts and passwords, among other interventions."



Breach Notification

Firms are required to notify affected individuals whose sensitive customer information "was, or is reasonably likely to have been, accessed or used without authorization" at the firm or at a service provider of the firm who has access to such information. Notice to affected customers must occur "as soon as practicable, but not later than 30 days, after becoming aware that the incident occurred or is reasonably likely to have occurred."

The Reg. S-P definition of sensitive customer information is broader than the definition used by 14 states, but the SEC notes that this is tempered by the harm requirement for notice as well as the ability of firms to rebut the presumption of notice. Notably, the 30-day notice pre-empts any state data breach notification laws with a longer timeframe and requires notification to all such customers regardless of the customers' state of residency.

Regulation S-P includes a strong presumption for notification to customers but includes an exception where the covered institution determines, after an investigation, that the data conclusively "has not been, and is not reasonably likely to be, used in a way that would result in substantial harm or inconvenience." In addition, the 30-day timeframe can be extended in situations where the so-called law enforcement exception has been invoked. The law enforcement exemption provides that when the Attorney General determines that the notification would pose a substantial risk to national security or public safety, the notice period can be delayed.

Practical Tips:

- The IRP should include specific procedures for how the firm will comply with the notice requirement in the event that ransomware renders its systems / data inaccessible. (adopting release, footnote 163)

- "Notice must be provided unless a 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 occurred at the covered institution or one of its service providers that is not itself a covered institution, that 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." (adopting release, footnote 41)

- Firms should assess how they will determine what information and systems were or may have been accessed during an incident. This will likely involve reviewing capabilities to monitor file and folder access and changes, security event logging, log retention periods, and data discovery. Leveraging these will help firms better determine what sensitive customer information, if any, were compromised.

- If a firm can't determine what customer data was accessed, notice must be provided to all customers. The rule presumes that notice is required unless the firm can prove otherwise. As a result, firms should be mindful of implementing security controls using the principle of least privilege in order to minimize greater access to data than is necessary.

- Notification to customers must be clear and conspicuous.

- Notification does not need to be sent by the firm to the SEC.

- **Substantial harm** or inconvenience is not defined in the final rule and is subject to a "facts and circumstances" test. The SEC had initially proposed some examples of what would have constituted "substantial harm or inconvenience" including personal injury, or a substantial financial loss, expenditure of effort, or loss of time. Although the phrase was left undefined in the final rule, the proposed definition provides some helpful guidance for relevant facts and circumstances to consider.

- **Factors for Determining Harm:** Unlike some state data breach regulations, encrypted data is not exempt. Rather, encryption (and in particular, encryption using current industry standard best practices) is one of a number of factors that firms should consider when determining whether the compromise of customer information could create a reasonably likely risk of harm to an individual identified with the information. Compromise of the decryption key or use of weaker encryption methods could be extenuating factors tilting the analysis towards likely risk of harm. As industry standards continue to develop in the future, covered institutions generally should "review and update, as appropriate, their encryption practices." Firms must document their analysis in detail in order to overcome the presumption that notice was required.

Service Provider Oversight

Firms must establish, maintain, and enforce written policies and procedures reasonably designed to oversee certain Service Providers – particularly, those with access to customer information. Other vendors may provide critical services to a firm or otherwise support critical business operations without necessarily having access to or processing such data. While these other providers are not included in the scope of Regulation S-P's vendor oversight requirements, it is still vitally important for firms to assess and monitor the risk of all of their critical vendors through initial and ongoing vendor due diligence.

Definition:

- **Covered Service Provider** as used in the Safeguards Rule refers specifically to "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."

Practical Tips:

- The adopting release lists various types of service providers likely in scope for vendor oversight under the Safeguards Rule. The list includes vendors providing "customer relationship management (CRM), customer billing, portfolio management, customer portals (e,g, customer trading platforms), customer acquisition, tax document preparation, proxy voting, and regulatory compliance (e.g. AML/KYC)" as likely falling within the scope of the due diligence and oversight requirements.

- Other service providers may be in scope, depending upon their level of access or their particular use cases with your firm. For example, cloud-based vendors for email, file storage, and the like, as well as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and IT and other consulting vendors may be set up "to receive, maintain, or process customer information." If any of these vendors are permitted access to customer information, they are within the scope of the rule's vendor oversight provisions.

- Some of these service providers will also be covered institutions in their own right under Regulation S-P.

- Revise the IRP to reference any existing vendor due diligence policy maintained in the WISP or Compliance Manual. If you do not have policies and procedures around vendor due diligence, establish those policies now. Revise monitoring procedures to specifically ensure that the covered service provider provides the breach notice as required.

- **Covered service providers** must provide notification to the covered institution "as soon as possible, but no later than 72 hours after becoming aware of a breach in security that has occurred resulting in unauthorized access to a customer information system maintained by the service provider."

- The 72-hour deadline is a change from the proposed 48 hours. 72 hours aligns Regulation S-P with the reporting deadlines in other rules like NYDFS cybersecurity law and the EU's GDPR.

- Receiving a breach notice from a service provider constitutes the receiving firm "becoming aware," but if the firm independently becomes aware of a breach even before it gets such notice from a vendor, that earlier awareness is what starts the clock for the firm's own incident response plan breach reporting obligations.

- Even if you have contracted with the service provider to provide notice to your customers, your firm ultimately has the responsibility to corroborate that notice was provided to those customers as part of your vendor oversight.

- The final rule does not require firms to include specific terms regarding breach notification and adherence to minimum security standards in vendor contracts. This was done as an accommodation to large vendors like Microsoft and AWS who do not typically negotiate standard terms of contracts with end customers.

- The rule advocates using a risk-based approach to due diligence and suggests that firms "consider employing such tools as independent certifications and attestations obtained from the service provider . . . as part of their policies and procedures to require oversight." Other suggested methods include "confirming with a sample of affected customers that they received such service provider notifications."

- A firm's policies should address the situation where, even though the firm has contracted for the service provider to send notice to customers, if the service provider does not send such notice, the firm must still send notice. While firms are permitted to rely somewhat upon reasonable assurances from vendors that the vendors have implemented adequate security controls, the SEC notes that if a firm has reason to know that certain controls are not in place, the firm cannot rely on such assurances from the vendor. For this reason, a strong vendor due diligence program is critical.

- Firms should consider reviewing and updating their due diligence assessment procedures periodically to ensure that the procedures remain reasonably designed.

Recordkeeping

Similar to many other rules adopted by the SEC, Regulation S-P includes various books and records which must be maintained to evidence compliance with the rule. The specific records are listed on pages 124-125 of the adopting rule release. In general, firms must maintain the following:

- Written incident response plan (IRP) policies and procedures (including redlined versions) addressing the collection, maintenance, sharing, and secure disposal of customer information, as well as policies and procedures for detecting, responding to, containing, and recovering from a security incident.
- Written IRP policies and procedures addressing vendor oversight for Covered Service Providers.
- Written documentation of any contracts or agreements between a covered institution and its service providers.
- Written documentation of any detected unauthorized access to or use of customer information.
- Written records of any firm response to, and recovery from, such unauthorized access to or use of customer information.
- Written documentation of any investigation and determination made regarding whether notification to affected individuals is / was required, including the basis for any determination made, any written documentation from the Attorney General related to a delay in notice, as well as a copy of any notice transmitted following such determination.

For registered investment advisers, these records must be kept for at least five years, the first two in an easily accessible place.

For registered investment companies, the retention period for policies and procedures is six years in an easily accessible place, with other records required to be kept for six years, the first two in an easily accessible place.

Broker-dealers and transfer agents must keep all records under Regulation S-P for three years in an easily accessible place.

Practical Tips:

- Revise the IRP to specifically reference the records which must be maintained to comply with the rule.
- Revise the Compliance Manual policy regarding books and records to also include a reference or cross-reference to any records required to be maintained pursuant to the Safeguards Rule. For example, these records include a copy of any notice of a breach received from a service provider.

Timing and Contents of the Breach Notice

Firms must provide notices to affected individuals "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." Firms can become aware through various means, including through their own monitoring, being informed by a client, or receiving notice of a breach from a service provider.

As stated above, a limited exception applies where that timing can be delayed in what has become known as the law enforcement exception.

The law enforcement exception can be invoked by the Attorney General, who notifies the SEC in writing that national security or public safety interests outweigh the benefits of reporting the incident to customers sooner. In those limited circumstances where the Attorney General has acted to invoke the exception, firms can delay notice to customers up to 30 days from when notice would have been required.

The SEC and the Department of Justice (DOJ) established an inter-agency communication channel for such written notice to be sent from the Attorney General to the SEC to invoke the exception. After invoking it, the DOJ will then notify covered institutions that it has given notice of the national security or public safety exception to the SEC.

The law enforcement exception works by delaying any required breach notice from a covered institution by 30 days. If the national security or public safety issue continues to exist, the Attorney General is authorized to invoke another 30-day delay. In extraordinary circumstances, the Attorney General can impose a final delay of an additional 60 days. Taken together, there are two 30-day delays and one final 60-day delay for a grand total of 120 days that the breach notice can be delayed by the Attorney General.

The DOJ is simply designated as the single point of contact for initiating a delay, but other state and federal agencies can make a request to the DOJ to call for such a delay. The FBI, in coordination with the Department of Justice, has since provided guidance on how firms can request disclosure delays for national security or public safety reasons in connection with the Public Company Cybersecurity Rules. See FBI Guidance to Victims of Cyber Incidents on SEC Reporting Requirements.

Practical Tips:

- The SEC acknowledges that some firms may have to provide notice by day 30, even where additional time investigating concludes that notice would not have been required. The 30-day requirement stems from the SEC balancing timeliness with over-notification concerns, while avoiding the need for firms to have to make a materiality determination. In SEC's view, 30 days is sufficient time to conduct an initial investigation.
- The SEC's 30-day notice requirement takes precedence over less stringent state requirements.
- The SEC also notes that the "becoming aware" standard differs from the public company cybersecurity rules, which require notice within four days of determining that an incident the firm experienced is material. The SEC notes that some incidents involving a limited amount of data or an isolated issue may only take several days to investigate.

Notice Content and Format

The Safeguards Rule sets out specific requirements for the content that must be included in every breach notice. If a firm updates its prior breach notice to a customer, those same minimum elements must be in any subsequent notice.

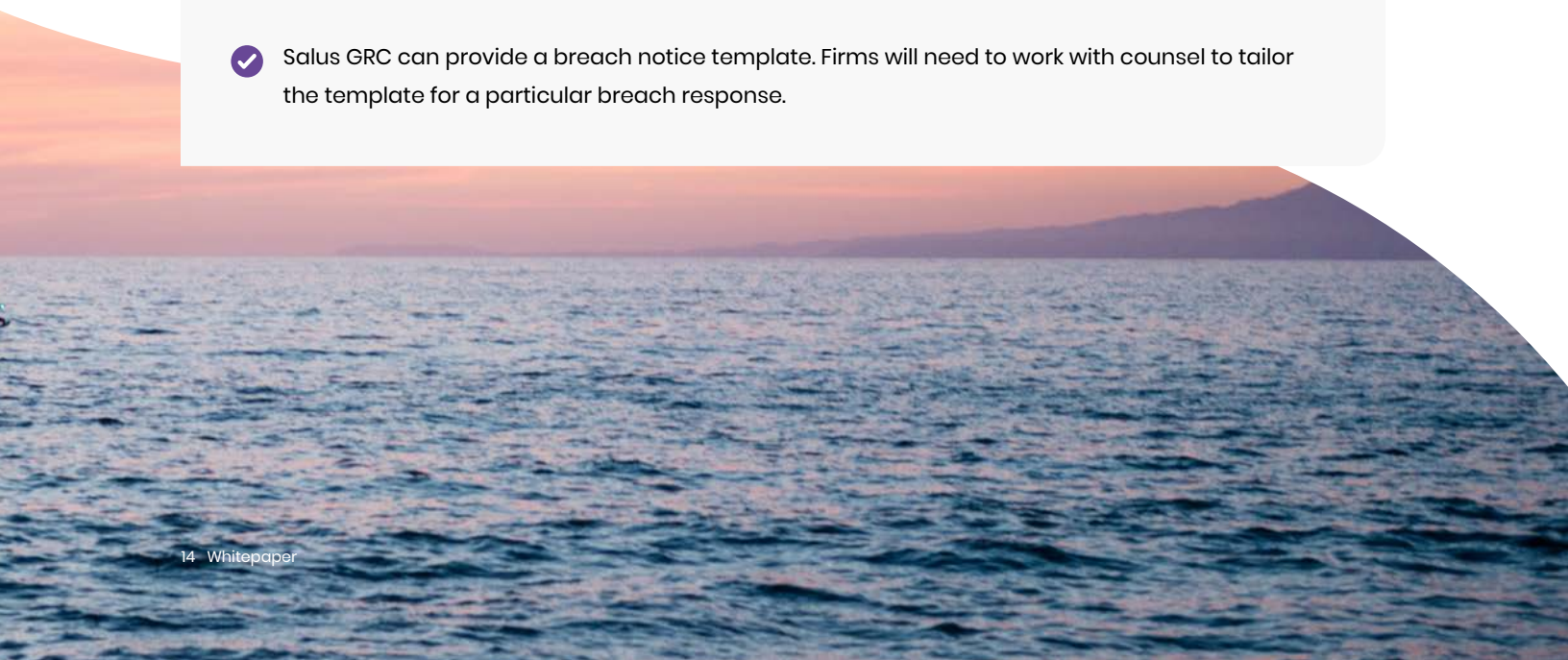
In a change from the proposed rule, the final rule does not require the notice to describe steps the firm has taken to prevent further unauthorized use. This was done in an effort to help firms gather all the information they could possibly need for the notice by day 30 at the latest.

The final rule requires that notices include key information. This includes:

- "details about the incident, the breached data, and how affected individuals can respond to the breach to protect themselves."
- "information regarding a description of the incident and the type of sensitive customer information accessed or used without authorization."
- the date of the incident. In practice, this can be an actual date or even an estimated date of the incident, to the extent this information can reasonably be determined when sending the notice.
- the firm's contact information.
- the name of a specific office or point of contact to enable recipients to get in touch with the firm for additional details. The contact information should include a toll-free number if available, as well as other methods of communication (email, mailing address, etc.).

Practical Tips:

- Notice can be provided by paper mailing or electronically to those customers who have consented to receive such notices electronically. Firms should review their electronic consent to make sure that incident response is specifically listed as a function for which electronic consent is acceptable by the client.
- Salus GRC can provide a breach notice template. Firms will need to work with counsel to tailor the template for a particular breach response.



Compliance Deadlines

The amendments to Regulation S-P are effective August 2, 2024. Similar to recent rules adopted by the SEC, the compliance dates are staggered. Larger firms will have 18 months from the Effective Date and must comply by February 2, 2026, whereas smaller firms will have 24 months from the Effective Date and must comply by August 2, 2026.

Larger firms are defined in the final rule to include registered investment advisers with at least $1.5 billion in assets under management or investment companies with at least $1 billion in net assets as of the most recent fiscal year end.

According to the Regulation S-P adopting release, 77% of registered investment companies are larger entities and will be subject to the 18-month compliance runway. On the other hand, only 23% of registered investment advisers meet the definition of larger entities, giving the vast majority of RIAs a generous 24-month window to get their programs into compliance. The longer compliance timeframe differs from the 12 months for all firms that was initially proposed.

Conclusion

The Regulation S-P amendments provide a federal data breach notification law for financial institutions maintaining customer data. Some state data breach laws are less stringent in terms of data, timing, or exceptions, whereas other states exclude certain entities from their scope entirely. The amended Safeguards Rule provides a "consistent, minimum federal notification standard" for investment companies and registered investment advisers.

Historically, firms have addressed Regulation S-P through a simple privacy notice disclosing information collection and sharing with affiliates, as well as with policies in a Compliance Manual covering requirements to provide natural person customers with an initial privacy notice and an annual privacy notice upon any material changes. Identity theft controls have been noted in firms' Identity Theft Prevention Programs under the existing Regulation S-ID. Additional details about specific administrative, technical, and procedural safeguards were often relegated to a separate Information Security Policy which has grown in length and complexity as cybersecurity regulations continue to expand.

The inclusion of incident response, breach reporting, and vendor due diligence requirements in the amended Regulation S-P rule creates an interesting dilemma. Is Regulation S-P a compliance rule or a cybersecurity rule? Effectively, it is a little of both, as evidenced by books and records requirements on one hand and incident detection and containment controls on the other. In the eyes of the SEC, it is less relevant where firms address the rule requirements and is it more important that they address them.

As this guide illustrates, the requirements imposed by the amended Regulation S-P are extensive. Firms subject to the rules should begin planning now to address the various aspects, as there are a lot of moving parts involved in getting information security controls in place to aid in incident detection as well as closely analyzing vendor contracts, conducting significant vendor due diligence, and coordinating with your compliance and cybersecurity consultants and legal counsel.

For assistance in developing or updating your compliance and cybersecurity policies, conducting incident response testing, and conducting vendor due diligence assessments, contact Salus GRC at inquiry@salusgrc.com for more information about how our team of experts can help.

300 Park Avenue
New York, NY 10022

inquiry@salusgrc.com
salusgrc.com