Simpson Thacher

Regulatory and Enforcement Update

Regulation S-P Amendments: Practical Points for Private Fund Advisers

August 25, 2025

Private fund advisers should start taking steps now to prepare for compliance with the amendments to Regulation S-P (the "Amendments") that were adopted by the U.S. Securities and Exchange Commission (the "SEC") in May 2024.[1] Unless the SEC delays the dates, registered investment advisers, including advisers to private funds, with at least $1.5 billion in assets under management ("AUM") must meet the ***December 3, 2025*** compliance date for "large" advisers, while smaller registered investment advisers must be in compliance by ***June 3, 2026***. The Amendments will also be applicable to investment companies, broker-dealers, and transfer agents (together with registered investment advisers, "covered institutions").[2] The Amendments set forth new policy requirements—including establishing an incident response program, breach notification procedures, and vendor oversight procedures—as well as new recordkeeping procedures, among other things, as detailed below.

While there has been industry advocacy calling for the SEC to extend the compliance dates,[3] the SEC, to date, has not announced an intention to modify the compliance dates for the Amendments. We will closely be monitoring for any updates to the compliance timeline. In the meantime, this article is meant to serve as a practical overview for private fund advisers as they endeavor to update their policies and modify their practices to achieve compliance with the Amendments by the fast-approaching deadlines (or by any extended deadlines). Especially given that some elements of the Amendments may require significant change or implementation efforts, private fund advisers would be well-advised to dedicate sufficient time and resources to operationalize compliance with the Amendments well in advance of the relevant compliance date.

I. Advisers Must Implement Policies and Procedures Across Four General Areas Related to Safeguarding Customer Information.

The SEC's stated goal in adopting the Amendments was to modernize and enhance the protections afforded to investors to keep pace with the expanded use of technology. Intended to further that purpose, the Amendments

[1] *See* Sec. & Exch. Comm'n, Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer information, Advisers Act Rel. No. 6604 (May 16, 2024) (hereinafter Adopting Release), available here; Press Release, Sec. & Exch. Comm'n, SEC Adopts Rule Amendments to Regulation S-P to Enhance Protection of Customer Information (May 16, 2024), available here; Sec. & Exch. Comm'n, Fact Sheet Final Rules: Enhancements to Regulation S-P, available here. For Simpson Thacher's discussion of the adoption of the Amendments, please see our article: *SEC Adopts Significant Amendments to Regulation S-P Requiring Notification of Sensitive Customer Information Breaches, Service Provider Oversight* (May 22, 2024), available here.

[2] The AUM thresholds are not uniform across all covered institutions. *See* Adopting Release, *supra* note 1, at 129, Table 3: Designation of Larger Entities, for additional context.

[3] *See, e.g.*, Letter from Investment Adviser Assoc. to the Hon. Paul S. Atkins, Chairman, Sec. & Exch. Comm'n (July 30, 2025), available here.

set forth various policy requirements related to safeguarding customer information that private fund advisers may not have in their existing policies and procedures: (i) general requirements pertaining to the security of customer information; (ii) incident response programs; (iii) breach notification requirements; and (iv) service provider oversight.[4]

As background, "customers" are defined to mean consumers who have a continuing relationship with the covered institution where the covered institution provides one or more financial products or services to the consumer for personal use.[5] Accordingly, "customers" of a private fund adviser can generally be understood to be limited partners in the private funds.

Additionally, "customer information" is defined to mean any record containing nonpublic personal information about a customer of a financial institution where the record is in the possession of the covered institution or being handled or maintained on its behalf.[6] Notably, this definition includes both the information of individuals who have a customer relationship with the covered institution as well as customers of *other* financial institutions where the information has been provided to the covered institution.

A. GENERAL REQUIREMENTS: ADVISERS MUST IMPLEMENT POLICIES AND PROCEDURES TO ADDRESS *ADMINISTRATIVE*, *TECHNICAL*, AND *PHYSICAL* SAFEGUARDS.

The general requirements of the policy provisions mandate that covered institutions have policies and procedures that address "administrative, technical, and physical safeguards for the protection of customer information."[7] The policies and procedures must be reasonably designed with three objectives in mind: (i) ensure the security and confidentiality of customer information; (ii) protect against any anticipated threats or hazards to the security or integrity of customer information; and (iii) protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.[8]

Many private fund advisers likely already have adequate policies and procedures to meet these requirements, but all advisers should review their policies and procedures to determine if any updates are needed.

[4] *See* 17 CFR § 248.30(a)(5).

[5] *See* 17 CFR § 248.30(d)(4)(i) (citing 17 CFR § 248.3(j)). Note that customer is defined differently for transfer agents under the Amendments.

[6] *See* 17 CFR § 248.30(d)(5). Note that customer information is defined differently for transfer agents under the Amendments.

[7] *See* 17 CFR § 248.30(a)(1).

[8] *See* 17 CFR § 248.30(a)(2).

B. INCIDENT RESPONSE PROGRAM: ADVISERS MUST IMPLEMENT AN INCIDENT RESPONSE PROGRAM DESIGNED TO *DETECT*, *RESPOND TO*, AND *RECOVER FROM* UNAUTHORIZED ACCESS TO OR USE OF CUSTOMER INFORMATION.

The Amendments specifically require that incident response programs are reasonably designed to *detect*, *respond to*, and *recover from* unauthorized access to or use of customer information.[9]

The Amendments detail three required categories of procedures that must be included in such incident response programs in the event an incident has been detected—generally, (i) assess, (ii) contain and control, and (iii) notify affected individuals.

First, there must be procedures for the private fund adviser to take steps to assess the nature and scope of any incident. The private fund adviser must identify the customer information systems[10] and types of customer information that may have been accessed or used without authorization. As a starting point, private fund advisers should be aware of the extent of its infrastructure that contains customer information and should track the types of customer information across different customer information systems. Private fund advisers may also consider limiting where customer information is housed, to the extent practicable, as well as who has access to such customer information.

Second, the incident response program must include appropriate steps for the adviser to take to contain and control the incident to prevent further unauthorized access or use of customer information. The Amendments do not include specific steps that covered institutions must take but rather allow flexibility for covered institutions to determine the appropriate containment steps, though such steps should be commercially reasonable and in line with industry practices.

Third, the incident response program must also include procedures for the covered institution to notify each affected individual whose "sensitive customer information" (as defined) was, or is reasonably likely to have been, accessed or used without authorization, unless the covered institution determines, after a reasonable investigation of the facts and circumstances, that the sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would cause substantial harm or inconvenience. These requirements are discussed in more detail in the next section. As noted below, private fund advisers should review their breach notification procedures in particular for compliance with the Amendments, while also keeping in mind that any particular incident could also trigger breach notification requirements under additional laws and regulations in the U.S. and foreign jurisdictions.

[9] *See* 17 CFR § 248.30(a)(3).

[10] The Amendments define customer information systems as "the information resources owned or used by a covered institution, including physical or virtual infrastructure controlled by such information resources, or components thereof, organizing for the collection, processing, maintenance, use, sharing, dissemination, or disposition of customer information to maintain or support the covered institution's operations." *See* 17 CFR § 248.30(d)(6).

The three categories of procedures set forth above generally will not implicate private fund adviser employees beyond those in compliance, IT, and similar roles. But private fund advisers should ensure that all employees are trained on the incident response program, including, but not limited to, in connection with initial detection of an incident and promptly reporting it to compliance (or otherwise as directed by policy).

C. BREACH NOTIFICATION: ADVISERS MUST TIMELY NOTIFY AFFECTED INDIVIDUALS IN THE EVENT OF A BREACH (SUBJECT TO LIMITED EXCEPTIONS).

The Amendments impose a notification requirement on covered institutions to provide "clear and conspicuous" notice to affected individuals of unauthorized access or use of sensitive customer information.[11] The notification is triggered in connection with incidents at either the covered institution or one of its service providers (where the service provider is not itself a covered institution, in which case such service provider is instead potentially responsible for making such notifications directly to the affected individuals).

"Sensitive customer information" is defined as "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."[12] The Amendments provide illustrative examples of sensitive customer information: (i) Social Security number, official State- or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (ii) biometric record; (iii) unique electronic identification number, address, or routing code; (iv) telecommunication identifying information or access device; or (v) customer information identifying an individual or the individual's account (such as account number, name, or online user name) in combination with authenticating information or similar information that could be used to gain access to the customer's account.

As previewed in the prior section above, covered institutions should conduct a reasonable investigation of the facts and circumstances of any incident. If such investigation determines 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 to the affected individual, the covered institution does not need to provide notice under Regulation S-P. Private fund advisers should be prepared to take immediate steps to conduct a reasonable investigation. Additionally, while the SEC declined to define the term "substantial harm or inconvenience,"[13] private fund advisers should consider adopting factors or analytical frameworks to have at the ready to determine if particular information is or is not reasonably likely to cause substantial harm or inconvenience.

In the absence of negative findings from an investigation, covered institutions must notify affected individuals as soon as possible, but ***no later than 30 days after becoming aware*** that sensitive customer information

[11] *See* 17 CFR § 248.30(a)(4)(i). Note that this requirement applies regardless of, and is in addition to, any individual state's applicable requirements for data breaches.

[12] *See* 17 CFR § 248.30(d)(9)(i).

[13] *See* Adopting Release, *supra* note 143, at 46-49. In the Adopting Release, the SEC indicated a desire to take a consistent approach with the banking agencies and to avoid both under- and over- notification.

was, or is reasonably likely to have been, accessed or used without authorization. The rapid notice timing is intended to give affected individuals the opportunity to mitigate the risk of substantial harm or inconvenience arising from the incident (such as by monitoring credit reports for unauthorized activity, placing fraud alerts on relevant accounts, or changing passwords). The Amendments have a narrow exception to the 30-day notification rule in the case of national security concerns.[14] Notably, the Amendments do *not* permit an extension of the 30-day notice window to allow for more time to conduct an investigation.

As to the means of transmittal, notice must be transmitted by a means designed to ensure that each affected individual can reasonably be expected to receive actual notice in writing. Therefore, practically speaking, if a private fund investor has opted to receive updates electronically, notification can also be provided electronically.

Importantly, if the covered institution is not able to identify which *specific* individual's sensitive customer information may have been accessed or used, notice must be provided to *all* individuals whose sensitive customer information resides in the relevant customer information system. This requirement underscores the importance of private fund advisers having an understanding of where particular customer information resides.

The notice must include the following content criteria:

- Describe in general terms the incident and the type of sensitive customer information that was or is reasonably believed to have been accessed or used without authorization;
- Include, if the information is reasonably possible to determine at the time the notice is provided, any of the following: the date of the incident, the estimated date of the incident, or the date range within which the incident occurred;
- Include contact information sufficient to permit an affected individual to contact the covered institution to inquire about the incident, including the following: a telephone number (which should be a toll-free number if available), an email address or equivalent method or means, a postal address, and the name of a specific office to contact for further information and assistance;
- If the individual has an account with the covered institution, recommend that the customer review account statements and immediately report any suspicious activity to the covered institution;
- Explain what a fraud alert is and how an individual may place a fraud alert in the individual's credit reports to put the individual's creditors on notice that the individual may be a victim of fraud, including identity theft;
- Recommend that the individual periodically obtain credit reports from each nationwide credit reporting company and that the individual have information relating to fraudulent transactions deleted;

[14] *See* 17 CFR § 248.30(a)(4)(iii). Covered institutions will be permitted to delay notification by an additional 30 days by providing notice to the SEC upon written notification from the U.S. Attorney General that notification would pose substantial risk to national security or public safety.

- Explain how the individual may obtain a credit report free of charge; and
- Include information about the availability of online guidance from the Federal Trade Commission and *usa.gov* regarding steps an individual can take to protect against identity theft, a statement encouraging the individual to report any incidents of identity theft to the Federal Trade Commission, and include the Federal Trade Commission's website address where individuals may obtain government information about identity theft and report suspected incidents of identity theft.[15]

Covered Institutions are permitted to include additional context in the notice as dictated by the facts and circumstances, but they may *not* omit any of the prescribed information set forth above.

The Amendments carry a presumption of detailed notification in the event of an incident. But not all incidents will require notification. As noted above, in the case where the incident does not involve *sensitive* customer information or where a reasonable investigation determines 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 to the customer. It therefore will serve private fund advisers well to have adequate procedures in place and frameworks for making and documenting (as further discussed below) such decisions.

D. SERVICE PROVIDER OVERSIGHT: ADVISERS MUST ADOPT POLICIES AND PROCEDURES TO ENSURE SERVICE PROVIDERS TAKE CERTAIN APPROPRIATE MEASURES.

The policy provisions of the Amendments also impose a requirement for covered institutions to implement written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers.[16] The Amendments define "service provider" as 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.[17]

Specifically, covered advisers must have policies that are reasonably designed to ensure service providers take appropriate measures to (i) protect against unauthorized access to or use of customer information; and (ii) provide notification to the covered institution as soon as possible, but no later than 72 hours, after becoming aware of a breach in security resulting in unauthorized access to a customer information system maintained by the service provider. Upon receipt of such notification from the service provider, the covered institution must initiate its incident response program.

This requirement related to the oversight of service providers may represent a significant operational challenge for many private fund advisers. Private fund advisers likely do not want to be in the business of requesting, reviewing,

[15] *See* 17 CFR § 248.30(a)(4)(iv)(H).

[16] *See* 17 CFR § 248.30(a)(5)(i).

[17] *See* 17 CFR § 248.30(d)(10). The Regulation S-P Adopting Release indicated that "service provider" can include affiliates of a covered institution, *see* Adopting Release, *supra* note 1, at 70.

and opining on the adequacy of third-party service provider customer information policies. While private fund advisers could contract with service providers to provide relevant representations,[18] service providers may not agree to such contractual representations—including but not limited to in the case of longstanding relationships (and contracts) with service providers. In the alternative, private fund advisers might consider seeking other assurances that service providers are taking appropriate measures to protect customer information and will provide the private fund adviser with the required timely notice. For instance, private fund advisers may seek periodic attestations or otherwise seek assurances through initial and periodic due diligence for their relevant service providers.

It bears noting that the Amendments allow a covered institution to enter into a written contract with the service provider to notify affected individuals on the covered institution's behalf in the event of an incident at the service provider. However, in such a case, the Amendments are clear that the covered institution nonetheless remains responsible for ensuring such notification to individuals occurs in the prescribed manner. Accordingly, some advisers may opt to handle the notice to affected individuals themselves to ensure that the notice is timely and sufficient under the Amendments.

At a high level, private fund advisers should be aware of which of their vendors qualify as service providers under the Amendments. Private fund advisers should be aware what customer information systems and types of customer information such service providers have access to, and if the access and extent of access is in fact needed.

II. Advisers Must Comply With Additional Requirements.

Beyond the policy requirements, the Amendments set forth additional provisions, as summarized below.

A. ENHANCED RECORD-KEEPING: ADVISERS MUST COMPLY WITH SPECIFIC RECORD-KEEPING REQUIREMENTS RELATED TO POLICIES AND PROCEDURES, BREACHES, AND INVESTIGATIONS.

Private fund advisers should be mindful of the expanded recordkeeping obligations in the Amendments. In particular, private fund advisers will be expected to maintain records including, but not limited to, the following: (i) policies and procedures designed to safeguard customer information; (ii) written documentation of any detected unauthorized access to or use of customer information, as well as any response to, and recovery from, such unauthorized access to or use of customer information; and (iii) written documentation of any investigation and determination made regarding whether notification is required, including the basis for any determination made.[19]

[18] *See* Adopting Release, *supra* note 1, at 69 (referencing a modification from the proposed amendments, which would have required policies and procedures requiring the covered institution to enter into written contracts with its service providers to take appropriate measures).

[19] *See* 17 CFR § 248.30(c).

The retention period for private fund advisers is to maintain all records for five years, the first two in an easily accessible place.[20]

B. DISPOSAL: ADVISERS MUST TAKE MEASURES TO PROPERLY DISPOSE OF CUSTOMER INFORMATION; IMPROPER DISPOSAL MAY TRIGGER BREACH NOTIFICATION REQUIREMENTS.

The Amendments also address the proper disposal of information by requiring that covered institutions adopt reasonable measures to protect against unauthorized access to or use of information in connection with its disposal.[21] Notably, the Amendments expand the scope of information covered to now encompass both consumer and customer information. Covered institutions should ensure their disposal policies and procedures cover customer information (not only consumer information). Each covered institution will need to adopt policies and procedures aligned with their specific disposal practices.

Improper disposal can trigger the breach notification requirements discussed above. As an example noted in the adopting release, "a covered institution whose employee leaves un-shredded customer files containing sensitive customer information in a dumpster accessible to the public would be required to notify affected customers, unless the institution has determined 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."[22]

C. PRIVACY NOTICE: ADVISERS MAY AVOID DELIVERING ANNUAL INVESTOR PRIVACY NOTICES TO THEIR CUSTOMERS IN CERTAIN CIRCUMSTANCES.

The Amendments incorporate an existing statutory exemption to the requirement to deliver an annual investor privacy notice to a covered institution's customers.[23] A covered institution can rely on this exemption if it has not changed its policies and practices regarding the disclosure of nonpublic personal information from those it most recently provided to the customer in privacy notices.

In practice, it will be important to consider this exemption against necessary compliance with applicable state or foreign data privacy laws that may require the provision of privacy notices (and updates to same).

III. The SEC Has Given Recent Commentary About Regulation S-P Amendments Outreach.

The SEC Staff have expressed their intention to conduct outreach related to the Amendments.

[20] *See* Adopting Release, *supra* note 1, at 122, Table 1: Recordkeeping Requirements.

[21] *See* 17 CFR § 248.30(b). Note that this requirement does not apply to notice-registered broker-dealers.

[22] *See* Adopting Release, *supra* note 1, at 25, n. 68.

[23] *See* 17 CFR § 248.5(a)(1).

For instance, earlier this year in May, Keith Cassidy, the Acting Director of the Division of Examinations previewed a future series of three outreach events related to the Amendments.[24] At the annual SEC Speaks program also in May, Alexis Hall, Acting National Associate Director of the Technology Controls Program of the Division of Examinations, also discussed the intended outreach events that are intended to help promote readiness for implementing the Amendments. Consistent with this commentary, the 2025 Exam Priorities, which highlighted Regulation S-P as one of the risk areas impacting various market participants, had previewed the Staff's intention to conduct targeted industry outreach regarding Regulation S-P.[25]

Acting Director Cassidy also stated that, in advance of the compliance dates, "registrants should not be surprised if examiners inquire about their preparations to ensure compliance following the compliance date." He assured that such inquiries "are not directed at citing registrants for potential non-compliance with requirements that are not yet in effect but are intended to inform the Commission of where registrants are in the process of implementation," and compared such approach to the approach taken before the transition to the T+1 settlement cycle.[26]

IV. Conclusion: Advisers Should Take Steps to Comply and Monitor for Updates.

We will closely monitor for SEC updates related to the Amendments, including for any outreach events or any extensions to the compliance dates.

In the meantime, private fund advisers should consider the steps they need to take to comply with the Amendments. As is typical following the compliance date for any new rule, the SEC Staff will likely test compliance with the Amendments during SEC examinations.

Private fund advisers will be well served by beginning to update policies and practices, in advance of the compliance dates, to allow sufficient time to work through operational challenges. Note that private fund advisers need to be mindful that if they officially adopt policies *in advance* of the relevant compliance date (whether as currently set or if delayed), they must comply with those policies in full in advance of the compliance date. By analogy, the Staff issued deficiencies to advisers who early adopted policies pursuant to the amended marketing rule and did not comply with such policies.

---

[24] *See* Keith Cassidy, Acting Dir., Div. of Examinations, Sec. & Exch. Comm'n, Speech, Regulation S-P – Back to the Future, Washington D.C. (May 14, 2025) (hereinafter Cassidy Speech), available here.

[25] *See* SEC. & EXCH. COMM'N, EXAMINATION PRIORITIES: FISCAL YEAR 2025 (Oct. 21, 2024), available here. For Simpson Thacher's discussion of the SEC's 2025 Examination Priorities in general, please see our article: *SEC Division of Examinations Announces 2025 Examination Priorities (Registered Funds* Regulatory Update) (Jan. 6, 2025), available here.

[26] *See* Cassidy Speech, *supra* note 24, § V; *see also* EXAMINATION PRIORITIES 2025, *supra* note 25, at 13 ("In preparation for the compliance date of the Commission's amendments to Regulation S-P, the Division will engage with firms during examinations about their progress in preparing to establish incident response programs reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information.").

Drafting (but not necessarily implementing) policies and procedures in advance of the compliance date may allow private fund advisers to better consider potential gaps or issues related to the practical implementation of procedures and compliance with the Amendments. As the Amendments may require significant changes to procedures and practices, thinking practically through issues and testing systems sufficiently in advance of the compliance date may ease the implementation process when the compliance dates arrive.

Even if the compliance dates are extended, it seems clear that the Regulation S-P Amendments will stay top of mind for the SEC. Acting Director Cassidy stated that, "should the Commission choose to extend the compliance date, the Division will adjust our timeline, as necessary, but our approach to promoting compliance with the new requirements will remain the same. With the Commission's clear statement of the importance of this issue, registrants shouldn't be surprised if Regulation S-P is the subject of a thematic initiative in the coming fiscal years."[27] The topics in the Amendments thus should be a focus area for private fund advisers in the coming years.

For further information regarding this Update, please contact one of the following authors:

WASHINGTON, D.C.

David W. Blass
+1-202-636-5863
david.blass@stblaw.com

Meaghan A. Kelly
+1-202-636-5542
mkelly@stblaw.com

NEW YORK CITY

Lori E. Lesser
+1-212-455-3393
llesser@stblaw.com

Jeffrey Caretsky
+1-212-455-7764
jeffrey.caretsky@stblaw.com

Raymond F. Jensen
+1-212-455-6820
raymond.jensen@stblaw.com

PALO ALTO

Corina Holland
+1-650-251-5073
corina.holland@stblaw.com

[27] *See* Cassidy Speech, *supra* note 24, § V.