Paul, Weiss

Client Memorandum

November 11, 2025

REMINDER: December 3, 2025 Compliance Date for Regulation S-P Amendments

Executive Summary

As a reminder, "Larger Entities," including registered investment advisers with $1.5 billion or more in assets under management, must comply with amended Regulation S-P beginning on December 3, 2025. "Smaller Entities," including registered investment advisers with less than $1.5 billion in assets under management, must comply with amended Regulation S-P beginning on June 3, 2026.

Regulation S-P is a set of privacy rules that govern the treatment of nonpublic personal information about consumers by certain financial institutions, including registered investment advisers ("RIAs").[1] On May 16, 2024, the Securities and Exchange Commission (the "SEC") amended Regulation S-P (the "Amendments"), substantially expanding its requirements.[2] Key changes include requiring RIAs to:

- Establish an incident response program to detect, respond to, and recover from unauthorized access to or use of customer information;
- Establish procedures to notify customers whose sensitive customer information was likely accessed or used without authorization within 30 days;
- Establish procedures to oversee service providers to ensure they protect customer information and notify the RIA within 72 hours of a security breach; and
- Maintain written records documenting compliance with the Amendments.

The Amendments also expand the scope of information subject to Regulation S-P and provide an exception to the annual privacy notice requirement. Below, we describe in more detail the Amendments as they apply to RIAs.

Expanded Scope of Information Covered by Regulation S-P

The Amendments expand the scope of information covered by Regulation S-P. Current Regulation S-P protects only the records and information of individuals who are customers of the particular RIA and not the information of individuals who are customers of another financial institution.[3] By defining "customer information," the Amendments expand the scope of

[1] Amended Regulation S-P also applies to broker-dealers, investment companies, funding portals and transfer agents (together, with registered investment advisers, "covered institutions"). Exempt reporting advisers are not in scope.

[2] *Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information*, Advisers Act Rel. No. IA-6604, May 16, 2024, available here.

[3] The term "financial institution" generally means any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

information covered by Regulation S-P to include information about individuals who may not be customers of RIA. For RIAs, the Amendments define "customer information" as any record containing "nonpublic personal information" about a customer of a financial institution that is in the RIA's possession or that is handled or maintained by the RIA or on its behalf, regardless of whether such information pertains to (a) individuals with whom the RIA has a customer relationship or (b) the customers of other financial institutions where such information has been provided to the RIA.[4]

Incident Response Program

The Amendments require RIAs to develop, implement, and maintain written policies and procedures for an incident response program that is reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information. The Amendments allow flexibility for RIAs to tailor their incident response programs to their particular circumstances, but require such programs to include written policies and procedures to:

1. Assess: Assess the nature and scope of any incident involving unauthorized access to or use of customer information and identify (i) both the "customer information systems"[5] and types of customer information that may have been accessed or used without authorization during an incident, as well as (ii) the specific customers affected;

2. Contain and Control: Take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information; and

3. Notify: Notify each affected individual whose "sensitive customer information" (defined below) was, or is reasonably likely to have been, accessed or used without authorization, unless the RIA 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 RIA or one of its service providers that is not itself subject to Regulation S-P, 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.

The customer notification portion the incident response program is discussed in more detail below.

Customer Notification

Sensitive Customer Information. While the incident response program is generally required to address incidents involving any form of customer information, notification is only required when there has been unauthorized access to or use of "sensitive customer information," a subset of customer information. 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. Examples of sensitive customer information include: Social Security number, driver's license number, employer or taxpayer identification number and other types of information that could be used to authenticate an individual's identity.

Reasonable Investigation. The Amendments establish a rebuttable presumption requiring notice regarding an incident that occurred at the RIA or one of its service providers that is not itself subject to Regulation S-P.[6] However, an RIA is not required to provide notice if it determines, after a reasonable investigation of the facts and circumstances, 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. Whether an investigation is reasonable depends on the particular facts and circumstances of the unauthorized access or use. Information related to the nature and scope of the incident may be relevant to determining the extent of the investigation, such as (i) whether the incident is the result of internal unauthorized access or an external intrusion, (ii) the duration of the incident, (iii) what accounts have been compromised and at what privilege level and (iv) whether and what type of customer information may have been copied, transferred or retrieved without authorization.

---

[4] The term "nonpublic personal information" means (i) personally identifiable financial information; and (ii) 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.

[5] The term "customer information systems" means the information resources owned or used by the RIA, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of customer information to maintain or support the RIA's operations.

[6] If an incident occurs at an RIA's service provider that is itself subject to Regulation S-P, that service provider has its own notification obligations under Regulation S-P and must also provide notification to the RIA. The RIA is not required to separately notify affected individuals of the same incident.

Substantial Harm or Inconvenience. Notably, the Amendments do not define "substantial harm or inconvenience" for purposes of Regulation S-P, explaining that whether a particular harm or inconvenience rises to the level of being substantial is a facts and circumstances determination. The SEC noted that a personal injury, financial loss, expenditure of effort, or loss of time, could each constitute a substantial harm or inconvenience.

Identification of Affected Individuals. In order to comply with the notice requirement, an RIA must first identify the affected individuals. The SEC errs on the side of requiring notification when there is doubt as to whether an individual was affected. For example, if an RIA is unable to identify which specific individuals' sensitive customer information has been accessed or used without authorization, the Amendments require the RIA to 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 without authorization. However, an RIA is not required to provide individual notices if they reasonably determine that a specific individual's sensitive customer information that resides on the customer information system was not accessed or used without authorization.

Method and Content of Notification. The Amendments do not prescribe a notification method, but instead require RIAs to provide a clear and conspicuous notice to each affected individual by a means designed to ensure that the individual can reasonably be expected to receive actual notice in writing. RIAs may contract with service providers to notify affected individuals on the RIA's behalf, although responsibility for compliance with the Amendments ultimately remains with the RIA.

In terms of content, the Amendments are more prescriptive and require that the notices:

1. 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;

2. 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;

3. Include contact information sufficient to permit an affected individual to contact the RIA 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;

4. If the individual has an account with the RIA, recommend that the customer review account statements and immediately report any suspicious activity to the RIA;

5. 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;

6. 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;

7. Explain how the individual may obtain a credit report free of charge; and

8. Include information about the availability of online guidance from the FTC 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 FTC, and include the FTC's website address where individuals may obtain government information about identity theft and report suspected incidents of identity theft.

Timing. The Amendments require that the RIA must provide notice 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 (or is reasonably likely to have) occurred, unless the United States Attorney General determines that such notice poses a substantial risk to national security or public safety, and notifies the SEC of such determination in writing.[7]

[7] In such cases, an RIA may delay delivering the notices for a time period specified by the Attorney General up to 30 days following the date when such notice was otherwise required to be provided; however, the Attorney General may extend such delay if the notice continues to pose a substantial risk to national security or public safety.

Service Provider Oversight

An RIA's incident response program must include the establishment, maintenance, and enforcement of written policies and procedures reasonably designed to require oversight, including through due diligence on and monitoring of service providers. Specifically, an RIA's policies and procedures must be 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 RIA 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. Upon receipt of such notification, the RIA must initiate its incident response program.

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." Since the definition of "service provider" is based on access to information, the definition could extend to affiliates of the RIA and financial counterparties such as brokers, clearing and settlement firms and custodial banks. Service providers may themselves be subject to Regulation S-P.

The Amendments do not require that these measures be provided for in a contract, although the SEC notes that firms "should generally consider whether a written contract that memorializes the expectations of both covered institutions and their service providers is appropriate." Further, the SEC notes that RIAs may wish to consider employing such tools as independent certifications and attestations obtained from the service provider as part of their policies and procedures. In terms of monitoring, the SEC indicates that RIAs should consider reviewing and updating their policies and procedures periodically throughout their relationship with a service provider, including updates designed to address any information learned during the course of their monitoring.

Recordkeeping

The Amendments require that RIAs make and maintain written records documenting compliance with the Amendments including:

- Written policies and procedures to address administrative, technical, and physical safeguards to protect customer information, including the incident response program;
- 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 required by the incident response program;
- Written documentation of any investigation and determination made regarding whether notification to affected individuals is required, including the basis for any determination made and any written documentation from the United States Attorney General related to a delay in notice, as well as a copy of any notice transmitted following such determination;
- Written policies and procedures required as part of service provider oversight;
- Written documentation of any contract entered into pursuant to the service provider oversight requirements; and
- Written policies and procedures addressing the proper disposal of consumer information[8] and customer information.

Annual Privacy Notice Exception

The Amendments provide an exception to the annual privacy notice already required by Regulation S-P if an RIA (i) only provides nonpublic personal information to non-affiliated third parties when an exception to third-party opt-out applies, and (ii) has not changed its policies and practices with regard to disclosing nonpublic personal information from the most recent disclosure sent to customers.

[8] The term "consumer information" means any record about an individual, whether in paper, electronic or other form, that is a consumer report or is derived from a consumer report, or a compilation of such records, that an RIA maintains or otherwise possesses for a business purpose regardless of whether such information pertains to: (A) individuals with whom the RIA has a customer relationship; or (B) to the customers of other financial institutions where such information has been provided to the RIA.

Application to Private Funds

Private funds themselves are not subject to Regulation S-P. However, the new definition of "customer information" in the Amendments captures information about natural person limited partners that a private fund "provides" to its RIA, scoping such information into Regulation S-P, including the customer notification requirements. Private fund advisers may already be subject to breach notification requirements under state law, EU General Data Protection Regulation[9] and the Federal Trade Commission's Safeguards Rule[10] for the natural person investors in the private funds they advise. As a result, we expect that many RIAs will not need to significantly change their practices in order to comply with the Amendments as they apply with regard to private fund limited partners.

Takeaways

As the compliance date for Larger Entities swiftly approaches, RIAs should ensure they are prepared to comply with the Amendments, taking steps including:

- Reviewing and revising applicable policies and procedures, including those related to incident response and vendor oversight;
- Identifying service providers with access to customer information and updating the arrangements with and oversight framework for those service providers;
- Developing a template notification that can be sent to affected individuals in the event that a security breach occurs;
- Training supervised persons on the new obligations under Regulation S-P; and
- Incorporating Regulation S-P compliance into the next annual compliance review and thinking through SEC exam preparedness with respect to demonstrating compliance with the Amendments.

[9] Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.

[10] 16 CFR Part 314.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Kirk Anderson
+1-212-373-3101
kwanderson@paulweiss.com

Brad M. Brown
+1-212-373-3222
bbrown@paulweiss.com

Andrew C. Day
+1-212-373-3554
acday@paulweiss.com

Victoria S. Forrester
+1- 212-373-3595
vforrester@paulweiss.com

Matthew B. Goldstein
+1-212-373-3970
mgoldstein@paulweiss.com

Udi Grofman
+1-212-373-3918
ugrofman@paulweiss.com

Toby M. Karenowski
+44-20-7601-8689
tkarenowski@paulweiss.com

James King
+44-20-7601-8640
jking@paulweiss.com

Jeremy Leggate
+44-20-7601-8734
jleggate@paulweiss.com

Marco V. Masotti
+1-212-373-3034
mmasotti@paulweiss.com

Ted McBride
+1-310-982-4313
tmcbride@paulweiss.com

Caitlin Melchior
+1-212-373-3352
cmelchior@paulweiss.com

Prem Mohan
+44-20-7601-8769
pmohan@paulweiss.com

Ross A. Oliver
+1-212-373-3055
roliver@paulweiss.com

David Pritchett
+44-20-7601-8732
dpritchett@paulweiss.com

Reva Raghavan
+44-20-7601-8751
rraghavan@paulweiss.com

Michael Ronca
+1-212-373-3098
mronca@paulweiss.com

Cameron Roper
+44-20-7601-8775
croper@paulweiss.com

Aaron J. Schlaphoff
+1-212-373-3555
aschlaphoff@paulweiss.com

Jyoti Sharma
+1-212-373-3712
jsharma@paulweiss.com

Marian S. Shin
+1-212-373-3511
mshin@paulweiss.com

Anusha Simha
+1-212-373-3632
asimha@paulweiss.com

Maury Slevin
+1-212-373-3009
mslevin@paulweiss.com

Jennifer Songer
+1-202-223-7467
jsonger@paulweiss.com

Robert D. Tananbaum
+1-212-373-3603
rtananbaum@paulweiss.com

Conrad van Loggerenberg
+1-212-373-3395
cvanloggerenberg@paulweiss.com

Lindsey L. Wiersma
+1-212-373-3777
lwiersma@paulweiss.com

Steve Y. Yoo
+1-310-982-4306
syoo@paulweiss.com

Arik Hirschfeld
+1-212-373-3914
ahirschfeld@paulweiss.com

Associate Ryan Arredondo contributed to this Client Memorandum.