



RIA Lawyers

TRUSTED COUNSEL FOR INVESTMENT ADVISERS

Recent Amendments to Regulation S-P; the Now-Delayed AML Rule; and Hot Exam Topic

Max Schatzow
RIA Lawyers, LLC

Agenda

- ▶ Amendments to Regulation S-P
- ▶ FinCEN's Now-delayed AML Rule for Investment Advisers
- ▶ SEC Examination Hot Topic
 - ▶ Share Class Selection

Amendments to Regulation S-P

May 16, 2024 - Final Rule Adopted

August 3, 2024 - Effective Date (60 days after publication on June 3, 2024)

Split Compliance Period

Larger Entities - 18 months -
December 3, 2025

Smaller Entities - 24 months - June
3, 2026

Amendments to Regulation S-P

Entity	Qualification to be considered a "larger entity"
Investment companies together with other investment companies in the same group of related investment companies	Net assets of \$1 billion or more as of the end of the most recent fiscal year.
Registered investment advisers	\$1.5 billion or more in assets under management.
Broker-dealers	All broker-dealers that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act.
Transfer agents	All transfer agents that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act.




Amendments to Regulation S-P

- ▶ When do you measure assets under management for purposes of the \$1.5B small/large entity cut-off?
 - ▶ As of your last annual updating amendment?
 - ▶ As of the compliance date or effective date of the rule? (i.e., August 3, 2024)
 - ▶ From the effective date on forward?



Amendments to Regulation S-P

- ▶ Who does it apply to?
 - ▶ The amendments to Regulation S-P only apply to investment advisers registered with the U.S. Securities and Exchange Commission.
 - ▶ The Federal Trade Commission (“FTC”) has privacy jurisdiction over investment advisers not registered with the SEC.
 - ▶ Gramm-Leach-Bliley Act (compliance required in 2001)
 - ▶ Comparable privacy regime prior to the recent amendments
- 

Amendments to Regulation S-P

- ▶ What did Regulation S-P **previously** require?
 - ▶ Notice to *customers* about privacy policies and practices
 - ▶ Describe conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties
 - ▶ Provide a method for consumers to prevent a financial institution from disclosing information to nonaffiliated third parties by “opting out” (subject to exceptions)

Amendments to Regulation S-P

- ▶ What did Regulation S-P **previously** require?
 - ▶ Section 30(a) - Required written policies and procedures that address administrative, technical, and physical **safeguards** for the protection of customer records and information. Reasonably designed to..
 - ▶ Insure the security and confidentiality of customer records and information;
 - ▶ Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
 - ▶ Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.
 - ▶ Section 30(b) - Every...investment company, and every investment adviser ...registered with the Commission, that maintains or otherwise possesses consumer report information for a business purpose must properly **dispose** of the information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

Amendments to Regulation S-P

► What does Regulation S-P NOW require?

► Section 30 was amended to enhance the safeguard and disposal rules.

1. Incident Response Program
 - Notification Requirement
2. Service Provider Oversight
3. Increased Scope
4. Recordkeeping Amendments

Amendments to Regulation S-P Incident Response Program

Written policies and procedures...**reasonably designed** to detect, respond to, and recover from unauthorized access to or use of customer information, including customer notification procedures. This response program must include procedures for the covered institution to:

...



Amendments to Regulation S-P Incident Response Program



(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;



Amendments to Regulation S-P Incident Response Program



(ii) Take **appropriate steps** to contain and control the incident to prevent further unauthorized access to or use of customer information; and

Amendments to Regulation S-P Incident Response Program

(iii) Notify each those whose *sensitive customer information* 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 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.

Amendments to Regulation S-P Notification Requirements

- Clear and conspicuous notice to each individual
- What if you can't determine whose information has been accessed or used?
 - Notify all whose sensitive customer information resides in the information system that was accessed
 - Can exclude specific individuals if...

Amendments to Regulation S-P Notification Requirements

Timing for Notification

- As soon as practicable...
- but not later than 30 days, after becoming aware of the breach unless...
 - the US Attorney General determines that the notice required under this rule poses a substantial risk to national security or public safety and notifies the Commission in writing (30 additional days)...
 - Subject to another 30-day extension by AG
 - Subject to a final 60-day extension by AG
 - Subject to specific request by AG and approval by SEC

Amendments to Regulation S-P Notification Requirements

Contents of Notification

- Describe the incident and the type information that was accessed or used
- Include the date of the incident or an estimate
- Contact information
- Recommendation to review account statements and report suspicious activity
- Explain what a fraud alert is and how an individual may place a fraud alert
- Recommendation to periodically obtain credit reports and have fraudulent transactions deleted
- Explain how the individual may obtain a free credit report
- Include info about the availability of online gov't guidance



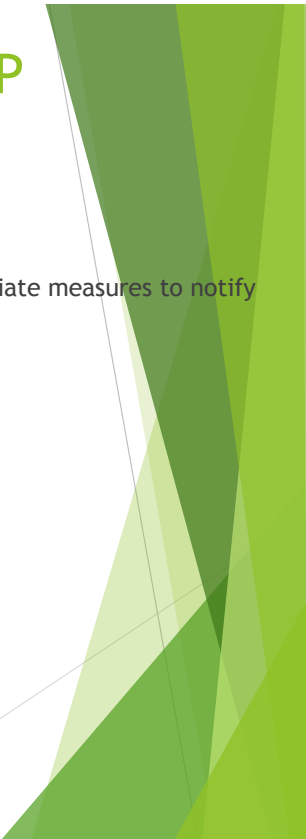
Amendments to Regulation S-P Service Provider Oversight

The policies and procedures must be reasonably designed to ensure service providers take appropriate measures to:

- (A) Protect against unauthorized access or use of customer info (Due diligence); and
 - (B) Provide notice ASAP, but no later than 72 hours after becoming aware of breach. FI must then initiate its incident response program.
- ▶ Can contractually delegate notice to provider, but FI remains responsible




Amendments to Regulation S-P Service Provider Oversight

- ▶ How do you reasonably ensure a service provider takes appropriate measures to notify you within 72 hours of discovering a breach?
 - ▶ A question asked and answered during the interview process?
 - ▶ A written email to the service provider?
 - ▶ A contractual representation?
 - ▶ “Reasonable assurances”?
 - ▶ Insufficient if assurance is known to be inaccurate
 - ▶ Ongoing review process?
- 




Amendments to Regulation S-P Increased Scope

“Customer information” means any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic or other form, that is in the possession of a covered institution or that is handled or maintained by the covered institution or on its behalf regardless of whether such information pertains to: (A) Individuals with whom the covered institution has a customer relationship; or (B) To the customers of other financial institutions where such information has been provided to the covered institution.



Amendments to Regulation S-P Increased Scope

“Sensitive customer information” means 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.



Amendments to Regulation S-P Increased Scope

Examples of sensitive customer information include:

Customer information uniquely identified with an individual that has a reasonably likely use as a means of authenticating the individual's identity, including:

- (1) SSN, driver's license or ID number, passport number, EIN or TIN;
- (2) A biometric record;
- (3) A unique electronic identification number, address, or routing code;
- (4) Telecommunication identifying information or access device; or

Customer information identifying an individual or the individual's account, including the individual's account number, name or user name, in combination with authenticating information, or in combination with similar information that could be used to gain access to the customer's account such as an access code, a credit card expiration date, a partial Social Security number, a security code, a security question and answer identified with the individual or the individual's account, or the individual's DOB, place of birth, or mother's maiden name.

Amendments to Regulation S-P Recordkeeping Amendments

- ▶ P&P required pursuant to the Safeguards Rule
- ▶ 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
- ▶ The written documentation of any investigation and determination made regarding whether notification is required, including the basis for any determination made, any written documentation from the US Attorney General related to a delay in notice
- ▶ P&P relating to due diligence and monitoring of service providers
- ▶ Contracts or agreements entered with a Service Provider
- ▶ Written P&P required to be adopted and implemented pursuant to the Disposal Rule

Knowledge Check - Question 1

- ▶ Under the amendments to Regulation S-P, an Investment Adviser must do all of the following EXCEPT:
- ▶ a. Notify affected individuals of unauthorized access
- ▶ b. Notify affected individuals within 30 days
- ▶ c. Provide free credit monitoring
- ▶ d. Perform due diligence of service providers

FinCEN's Final AML Rule Update

- ▶ January 1, 2026 - Previous Effective Date
- ▶ January 1, 2028 - Updated Effective Date (July 21, 2025)
- ▶ What should Investment Advisers be Doing?
 - ▶ Calendar reminder
 - ▶ Monitor
 - ▶ Prepare and Implement?
- ▶ Final rule applies only to SEC-registered IAs and ERAs
- ▶ Rule may require:
 - ▶ Written AML/CFT programs
 - ▶ Compliance officer designation
 - ▶ SAR and Currency Transaction Reporting
 - ▶ Ongoing training, internal controls, independent testing

SEC Examination Hot Topic Share Class Selection

- ▶ Data Sources
 - ▶ DERA - Division of Economic and Risk Analysis
 - ▶ Custodial Request
 - ▶ Routine Exam Request
- ▶ Less expensive vs most appropriate
- ▶ Delta in cost between less expensive and current holdings
- ▶ Remediation?
- ▶ Push back?

Knowledge Check - Question 2

- ▶ What sources does the SEC Examinations Staff use to determine whether an investment adviser is holding any inappropriate mutual fund share classes?
- ▶ a. EDGAR
- ▶ b. DERA
- ▶ c. Custodians
- ▶ d. A & C
- ▶ e. B & C

Questions?

- ▶ Max Schatzow
- ▶ RIA Lawyers, LLC
- ▶ www.RIALawyers.com
- ▶ Contact@RIALawyers.com
- ▶ Thank you!

