MARCH 20, 2023

SEC Proposes Enhancements to Regulation S-P: Potential Implications for Private Fund Advisers

Executive Summary

On March 15, 2023, the SEC unanimously proposed amendments to enhance Regulation S-P's provisions requiring registered investment advisers to protect customer (e.g., certain fund limited partners) information (available here) (the "Proposal").

The Proposal would, among other things:

- require SEC-registered investment advisers ("RIAs") to adopt an incident response program to address unauthorized access to or use of customer information;
- require RIAs to provide customer information breach notifications to customers affected by certain types of customer information breaches;
- broaden the scope of information covered by the "safeguards rule" and "disposal rule" (each, as discussed below) to include both nonpublic personal information that an RIA collects about its own customers and nonpublic personal information an RIA receives about customers of other financial institutions;
- conform Regulation S-P's annual privacy notice delivery provisions with a statutory exception provided in 2015; and
- require RIAs to maintain written records documenting compliance with the requirements of Regulation S-P.

Below is a summary of certain aspects of the Proposal, with particular emphasis on its potential implications for private fund advisers.

Background

Regulation S-P currently requires RIAs to, among other things: (1) adopt written policies and procedures to safeguard customer records and information (the "safeguards rule") and (2) properly dispose of consumer report information in a manner that protects against unauthorized access to or use of such information (the "disposal rule"). Importantly, as used in Regulation S-P, the terms "customer" and "consumer" refer to an individual (i.e., natural person). Therefore, a private fund adviser is not required to comply with Regulation S-P with respect to an investor in a private fund that is not a natural person, such as a pension plan. In this memorandum, the term "customer" or "consumer" refers to a natural person that is an investor in a private fund.

Require an Incident Response Program

The Proposal would amend Regulation S-P to require RIAs to adopt a written incident response program reasonably designed to detect, respond to and recover from both unauthorized access to and unauthorized use of customer information (an "incident").

Although the Proposal does not prescribe specific steps an RIA must take when carrying out incident response activities, an RIA's incident response program would be required to include policies and procedures with general elements, which may be tailored to the RIA's facts and circumstances, including policies and procedures to:

- assess the nature and scope of any incident and identify the customer information systems and types of customer information that may have been accessed or used without authorization;
    - e.g., gathering information about the type of access, the extent to which systems or other assets have been affected, the level of privilege attained by any unauthorized persons, the operational or informational impact of the breach and whether any customer information has been lost or exfiltrated;
- take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information;
    - e.g., isolating compromised systems or enhancing the monitoring of intruder activities, searching for additional compromised systems, changing system administrator passwords, rotating private keys, changing or disabling default user accounts and passwords, remediating all infected IT environments (e.g., cloud, operational technology, hybrid, host and network systems) and monitoring for any signs of adversary response to containment activities); and
- notify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization in accordance with the notification obligations discussed below.

Require Customer Information Breach Notifications

An incident response program would also be required to include procedures for notifying affected individuals whose "sensitive customer information"[1] was, or is reasonably likely to have been, accessed or used without authorization, unless the RIA determines, after a reasonable investigation, 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."[2]

- **Affected Individuals**. The RIA would be required to provide notice to each affected individual by a means designed to ensure that the individual can reasonably be expected to receive actual notice in writing (either through paper or electronic means).
- **Timing**. RIAs would be required to notify impacted customers as soon as practicable, but not later than 30 days of becoming aware that an incident has occurred or is reasonably likely to have occurred.
- **Content**. RIAs would be required to include key information with details about the incident, including the breached customer information, what the RIA has done to prevent further incidents, the estimated date or date range of the incident, the RIA's contact information and how affected individuals could respond to the breach to protect themselves.
- **Rebuttal**. RIAs would be permitted to rebut the affirmative presumption of notice based on a reasonable investigation of the facts and circumstances of the incident. Such an investigation would have to provide a sufficient basis for the determination 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.

Although all 50 states have enacted laws in recent years requiring firms to notify individuals of customer information breaches, standards differ by state. The Proposal would establish a Federal minimum standard for RIAs to provide customer information breach notifications to affected individuals.

Expand Requirements Relating to Service Providers

An incident response program would also be required to include written policies and procedures that address the risk of harm posed by security compromises at "service providers"[3] (e.g., providers of trading and order management, information technology functions and cloud computing services) as a result of outsourcing certain business functions or activities to them. Such policies and procedures would require an RIA, pursuant to a written contract between the RIA and its service providers, to require service providers to take appropriate measures that are designed to protect against unauthorized access to or use of customer information. Appropriate measures would include the obligation for a service provider to notify an RIA as soon as possible, but no later than 48 hours after becoming aware of a breach, in the event of any breach in security that results in unauthorized access to a customer information system maintained by the service provider. An RIA would be permitted to enter into a written agreement with its service provider to have the service provider notify affected individuals on its behalf in accordance with the notification obligations discussed above; however, the RIA would remain responsible for any failure to provide a required notice.

The SEC is increasingly focused on the oversight of outsourcing of certain functions by RIAs.[4] Implementing the contractual requirements required under the Proposal would be costly.

Expand the Scope of Information Covered by Regulation S-P

The Proposal would apply the protections of both rules to "customer information," which would mean any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic or other form that is handled or maintained by the RIA. In addition, a new section would provide that both rules apply to both (1) nonpublic personal information that an RIA collects about its own customers and (2) nonpublic personal information it receives from a third party financial institution about that institution's customers.

For example, customer information that an RIA has received from a custodian regarding a former private fund investor's assets would be covered under both rules if the former investor remains a customer of the custodian, even though the individual is no longer an investor in a private fund advised by the RIA.

Include FAST Act Exception from the Annual Privacy Notice Delivery Requirement

Currently, Regulation S-P generally requires an RIA to provide an initial notice of its privacy policies and practices to its customers not later than when the RIA establishes the customer relationship (e.g., in subscription documents) and annually after that for as long as the customer relationship continues. If an RIA chooses to share nonpublic personal information with a nonaffiliated third party other than as disclosed in an initial privacy notice, the RIA must send a revised privacy notice to its customers. Regulation S-P also requires that before an RIA shares nonpublic personal information with nonaffiliated third parties, the RIA must provide the customer with an opportunity to opt out of sharing, except in certain circumstances.[5]

The Proposal would conform Regulation S-P's annual privacy notice delivery provisions to the terms of an exception included in the 2015 Fixing America's Surface Transportation Act, which would provide that an RIA is not required to deliver an annual privacy notice if it satisfies two conditions: (1) an RIA relying on the exception only shares nonpublic personal information to nonaffiliated third parties in a manner that does not trigger the customer's statutory right to opt out and (2) an RIA cannot have changed its policies and practices with regard to disclosing nonpublic personal information from those it most recently disclosed to the customer. In addition, the Proposal would provide timing requirements for delivery of annual privacy notices if an RIA that qualifies for this annual notice exception later changes its policies and practices in such a way that it no longer qualifies for the exception.

Add Recordkeeping Obligations

The Proposal would require RIAs to make and maintain written records documenting compliance with the requirements of Regulation S-P. RIAs would have to preserve the records for five years, the first two years in an appropriate office of the RIA.

Next Steps

If adopted, the SEC is proposing a 12-month transition period for RIAs to come into compliance with the Proposal.

The public comment period will remain open until the date that is 60 days after the publication of the Proposal in the *Federal Register*.

Relatedly, the SEC re-opened the comment period for its proposing release "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies" (available here) so that commenters may consider any effects from the Proposal on such proposing release. The public comment period will remain open until the date that is 60 days after publication of the re-opening release (available here) in the *Federal Register*.

* * *

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:

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

Amran Hussein
+1-212-373-3580
ahussein@paulweiss.com

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

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

Maury Slevin
+1-212-373-3009
mslevin@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

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

[1] "Sensitive customer information" would be defined to mean any component of customer information alone (i.e., Social Security number, government passport number, biometric record of a fingerprint or iris image) or in conjunction with any other information (i.e., name or online user name, in combination with authenticating information such as a partial Social Security number, access code or mother's maiden name), the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information. In determining whether the compromise of customer information could create a reasonably likely harm risk to an individual identified with the information, a covered institution could consider encryption as a factor.

[2] "Substantial harm or inconvenience" would be defined to mean personal injury, or financial loss, expenditure of effort or loss of time that is more than trivial. The definition would also include examples of certain harms.

[3] "Service provider" would be defined to mean any person or entity that is a third party and receives, maintains, processes or otherwise is permitted access to customer information through its provision of services directly to a covered institution. This definition would include affiliates of covered institutions if they are permitted access to this information through their provision of services.

[4] On October 26, 2022, the SEC proposed a new rule and related rule amendments under the Investment Advisers Act of 1940 (available here) that establish a new oversight framework for outsourcing by RIAs.

[5] An RIA is not required to provide customers the opportunity to opt out if the RIA shares nonpublic personal information with nonaffiliated third parties (1) pursuant to a joint marketing arrangement with third party service providers, subject to certain conditions, (2) related to maintaining and servicing customer accounts, securitization, effecting certain transactions, and certain other exceptions and (3) related to protecting against fraud and other liabilities, compliance with certain legal and regulatory requirements, consumer reporting and certain other exceptions.