SHARTSIS FRIESE LLP
425 Market Street ♦ Eleventh Floor
San Francisco, California 94105-2496

February 20, 2025

VIA EMAIL

To Our Investment Adviser Clients and Other Friends:

Re: Regulation S-P Amendments Applicable to SEC-Registered Investment Advisers.

New amendments to the SEC's privacy rules of Regulation S-P (the "**Reg S-P Amendments**") will require SEC-registered investment advisers ("**RIAs**") to develop written incident response programs for cybersecurity breaches and to monitor service providers with access to customer information. Large RIAs with $1.5 billion or more in assets under management must comply with the new requirements by December 3, 2025. RIAs under that threshold must comply by June 3, 2026.

Incident Response Programs

The Reg S-P Amendments require RIAs to have an incident response program to (1) assess the scope of any unauthorized data access event and identify compromised information and systems, (2) take steps to contain the breach and prevent further unauthorized access or use of customer information and (3) notify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. RIAs should further tailor their incident response policies and procedures to their particular circumstances.

The Reg S-P Amendments do not specify how an RIA must carry out an incident response, as RIAs may need flexibility to respond appropriately to a breach. Strategies for assessing and responding to a cyber incident may include (a) isolating compromised systems, (b) tracking system use and login attempts, (c) searching for additional compromised systems, (d) changing system administrator passwords, (e) rotating private keys for encrypted information and (f) changing or disabling default user accounts and passwords, among other interventions.

After the initial detection and control process described above, RIAs must assess whether they are required to notify those affected. Such notification is required as soon as practicable, but no later than 30 days after the RIA becomes aware of the breach, unless the RIA determines (after reasonable investigation) 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. A key factor in that assessment may be whether the breached data was encrypted in accordance with current industry standards and if the decryption key remains secure.

The Reg S-P Amendments expand the definition of covered customers, as described below. If the RIA is unable to identify which specific individuals' information was accessed or used without authorization, the Reg S-P Amendments require the RIA to notify all individuals whose sensitive information resides in the information system that was, or was reasonably likely to have been,

accessed without authorization. RIAs must document their decision on whether to send such a notification.

Sensitive customer information includes any customer information that alone or in conjunction with other information could reasonably risk substantial harm or inconvenience to the customer if compromised. This includes a social security number, driver's license number, passport number, account number, taxpayer identification number and any unique electronic identification number, address or routing code.

A breach notification, if required, must clearly describe the nature of the incident, the type of sensitive information involved, the date of the incident, contact details to permit customers to inquire about the incident and recommendations regarding measures to protect against identity theft. Breach notifications may be delayed in limited circumstances, and only if the U.S. Attorney General notifies the SEC that it has determined that the notification poses substantial risk to national security or public safety. RIAs may delegate breach notification responsibility to their service providers. The SEC considers these new notification requirements to be the Federal minimum standard for breach notifications, but state law may still apply, depending on the incident at issue, and could require RIAs to give earlier notifications or use prescribed text.

Oversight of Service Providers

The Reg S-P Amendments require RIAs to oversee service providers with access to customer information, which may include due diligence assessments and ongoing monitoring. RIAs must have policies and procedures reasonably designed to ensure service providers take appropriate measures to:

(1) Protect against unauthorized access to or use of customer information; and

(2) 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 that resulted in unauthorized access to a customer information system maintained by the service provider.

The Reg S-P Amendments do not require the 72-hour notification requirement to be included in a written contract with the service provider; however, practically, a contract provision is an efficient means of complying with the Reg S-P Amendments. As service provider contracts come up for renewal, RIAs may want to prospectively include provisions to cover compliance with the Reg S-P Amendments. An RIA may also confirm that the service provider has internal policies that require a breach notification to be sent to the RIA within the prescribed time period, through periodic diligence or from other certifications and attestations from the service provider.

Other Provisions of the Reg S-P Amendments

The Reg S-P Amendments also amend the Safeguards Rule and Disposal Rule by broadening the information captured by those rules. Those rules now apply to both "customer information" and "consumer information," which includes any nonpublic personal information about a customer of the RIA, or a customer of another financial institution whose information has been provided to the RIA, that is in the RIA's possession.

The Reg S-P Amendments expand RIA recordkeeping requirements. RIAs must make and maintain written records for 5 years documenting: (1) compliance with the Safeguards Rule and Disposal Rule (including the adoption of a written information security policy and an incident response plan), (2) any detection of unauthorized access to or use of customer information and the firm's response, (3) any investigation and decision about whether any customer notification is required with respect to unauthorized access to or use of sensitive customer information, (4) policies and procedures that require oversight, monitoring and diligence of service providers with access to customer information, (5) agreements with service providers relating to customer information and (6) policies and procedures that address the proper disposal of customer information.

Next Steps

RIAs should consult with their IT and cybersecurity professionals to develop an effective and practical incident response plan based on their current information system architecture. RIAs should identify all service providers that handle customer information, review and consider updating the diligence completed on those service providers and consider if service provider contract amendments are appropriate to ensure compliance with service provider oversight requirements. RIAs should review and revise their policies and procedures to address these issues and the recordkeeping requirements in advance of their applicable compliance date for the Reg S-P Amendments.

We encourage all RIAs to review the Reg S-P Amendment requirements carefully and contact one of the Shartsis Friese attorneys in the Investment Funds & Advisers Group if you have questions about your incident response plan or contracts with service providers.

Previous letters to our investment advisory clients and friends and discussions of other topics relevant to private fund managers, investment advisers and private investment funds can be found at our insights page: www.sflaw.com/blog/investment-funds-advisers-insights.

SHARTSIS FRIESE LLP