DINSMORE COMPLIANCE SERVICES

AN AFFILIATE OF DINSMORE & SHOHL LLP

Special Alert

January 13, 2025

Summary of Regulation S-P Revisions Applicable to Investment Advisers

On May 15, 2024 the SEC issued Release Nos. 34-100155; IA-6604 (the "Adopting Release") providing for amendments to the safeguards and disposal rules of Regulation S-P (the "Amendments"). The compliance dates for the Amendments are December 31, 2025 for "large" investment advisers (those with $1.5 billion or more in assets under management) and June 3, 2026 for "small" investment advisers (those with less than $1.5 billion in assets under management.

The safeguards rule requires investment advisers (and other Covered Institutions - broker-dealers, investment companies and transfer agents) to adopt written policies and procedures that address administrative, technical and physical safeguards to protect customer records and information ("Customer Information"). The disposal rule requires investment advisers (and other Covered Institutions) to ensure the proper disposal of Consumer Report information, and pursuant to the Amendments, Customer Information. This alert summarizes the Amendments as applicable to investment advisers.

The principal elements of the Amendments are as follows:

- Requiring Covered Institutions to establish and maintain written incident response programs designed to detect, respond to, and recover from unauthorized access to or use of Customer Information;
- Requiring Covered Institutions to notify individuals whose Sensitive Customer Information was, or is likely to have been, accessed or used without authorization;
- Requiring Covered Institutions to establish and maintain policies and procedures reasonably designed for oversight of Service Providers;
- Expanding the application of the safeguards and disposal rules to the newly defined term "Customer Information;"
- Requiring Covered Institutions to make and maintain written records documenting compliance with the safeguards and disposal rules; and
- Codifying the exemption applicable to the annual delivery of privacy notices.

Pursuant to the Amendments, Customer Information refers to any record with nonpublic personal information about a financial institution's customers. This includes information a Covered Institution possess, handles, or maintains – whether it relates to the Covered Institution's owner customers or those of other financial institutions that shared the information. Regulation S-P defines nonpublic personal information as personally identifiable financial information and 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.

Incident Response Program

The Amendments require Covered Institutions to establish and maintain an incident response program for unauthorized access to, or use of, Customer Information. A Covered Institution's incident response program will be required to include written policies and procedures to:

- 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;
- Take appropriate steps to contain and control the incident to prevent further unauthorized access to, or use of, Customer Information; and

- Notify each affected individual 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, 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 to the customer.

Covered Institutions should tailor their incident response programs to their individual facts and circumstances.

Assessment

The Amendments require that the incident response program include procedures for:

- Assessing the nature and scope of any incident involving unauthorized access to, or use of, Customer Information; and
- Identifying the Customer Information Systems and types of Customer Information that may have been accessed or used without authorization.

While a Covered Institution's assessment will be driven by the applicable facts and circumstances, the SEC states in the Adopting Release that an assessment may include 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 data has been lost or exfiltrated. In addition, the SEC says in the Adopting Release that the assessment process may also be helpful for identifying and evaluating existing vulnerabilities that could benefit from remediation in order to prevent such vulnerabilities from being exploited in the future.

Containment and Control

The Amendments require the response program to include procedures for taking appropriate steps to contain and control a security incident, in order to prevent further unauthorized access to, or use of, Customer Information. While the steps for containing and controlling an incident will be driven by the applicable facts and circumstances, the SEC provides the following examples in the Adopting Release:

- Isolating compromised systems or enhancing the monitoring of intruder activities;
- Searching for additional compromised systems;
- Changing system administrator passwords;
- Rotating private keys; and
- Changing or disabling default user accounts and passwords

Notice to Affected Individuals

The Amendments require Covered Institutions to provide clear and conspicuous notice to each affected individual whose Sensitive Customer Information was, or was reasonably likely to have been, accessed or used without authorization, unless the Covered Institution has determined, after a reasonable investigation of the incident, 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 individual. The notice must be provided as soon as practicable, but not later than 30 days after the Covered Institution becomes aware that unauthorized access to, or use of, Customer Information has occurred or is reasonably likely to have occurred.

Standard for Providing Notice and Identification of Affected Individuals

Pursuant to the Amendments, if an incident has occurred but a Covered Institution is unable to identify which specific individuals' sensitive Customer Information has been accessed or used without authorization, the Covered Institution must 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. While incident response programs are generally required to address security 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.

What Constitutes a Reasonable Investigation

As referenced above, the Amendments require notifying affected individuals unless the Covered Institution determines, after a 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 to an individual. In the Adopting Release, the SEC provides that whether an investigation is reasonable will depend on the particular facts and circumstances of the unauthorized access or use. The SEC further states that information relating to the nature and scope of the incident may be relevant to determining the extent of the investigation, such as:

- Whether the incident was the result of internal unauthorized access or use of Sensitive Customer Information or an external intrusion;
- The duration of the incident;
- What accounts have been compromised and at what privilege level; and
- Whether and what type of Customer Information may have been copied, transferred or retrieved without authorization

A Covered Institution cannot avoid its notification obligations in cases where an investigation's results are inconclusive. Instead, the notification requirement is excused only where a reasonable investigation

supports a 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. Under the Amendments, for any determination that a Covered Institution makes that notice is not required, the Covered Institution will be required to maintain a record of the investigation and the basis for its determination.

The Adopting Releases addresses system protections in relation to whether a Covered Institution's reasonable investigation supports a 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. Specifically, the Adopting Release states that a Covered Institution may consider encryption as a factor in determining whether the compromise of Customer Information could create a reasonably likely harm to an individual identified with the information. The SEC acknowledges that encryption of information using current industry standard best practices is a reasonable factor for a Covered Institution to consider in making such determination. To the extent encryption minimizes the likelihood that the cipher text could be decrypted, it would also reduce the likelihood that the cipher's text compromise could create a risk of harm, as long as the associated decryption key is secure. In addition, the SEC provides in the Adopting Release that relatedly, and for the same reasons, when information that would otherwise constitute Sensitive Customer Information is encrypted, the Covered Institution may consider the security provided by that encryption in determining whether the cipher text (i.e. the data rendered in a format not understood by people or machines without an encryption key) is Sensitive Customer Information.

Notification Requirements Relating to Service Providers, Other Third Parties and Information Received from Third Parties

The Amendments apply to Customer Information in a Covered Institution's possession or that is handled or maintained on the Covered Institution's behalf, regardless of whether such information pertains to individuals with whom the Covered Institution has a customer relationship or to the customers of other financial institutions where such information has been provided to the Covered Institution. The Amendments do not require multiple Covered Institutions to notify the same affected individuals about a given incident. The Amendments only require a Covered Institution to provide notice when an incident occurs at the Covered Institution or one of its Service Providers that is not itself a Covered Institution. When a Service Provider (that is not itself a Covered Institution) provides notice to a Covered Institution that a breach in security has occurred resulting in unauthorized access to a Customer Information System maintained by the Service Provider, that Covered Institution will be required to initiate its incident response program and if applicable, provide notice to affected individuals. Furthermore, a Covered Institution is permitted to enter into a written agreement with its Service Provider to notify affected individuals in accordance with the requirements of the Amendments. Finally, where an incident occurs affecting two Covered Institutions' customers, although the Covered Institution experiencing the incident is

responsible for the notification, the two Covered Institutions can coordinate with each other as to which Covered Institution will send the notice.

Relation to State Notification Obligations

State law notification standards may vary from the notification standards contained in the Amendments. In the Adopting Release, the SEC acknowledges these variations and says Covered Institutions may provide one notice, as long as one notice includes all of the information required under the Amendments and applicable state law.

Substantial Harm or Inconvenience

Substantial harm or inconvenience is not defined in the Amendments. Whether a harm rises to the level of a substantial harm, or substantial inconvenience, depends upon the particular facts and circumstances surrounding an incident. In reference to the proposed Amendments, the SEC provides that a personal injury, financial loss, expenditure of effort or loss of time, each could constitute a substantial harm or inconvenience. In addition, the SEC provides the following examples:

- Theft;
- Fraud;
- Harassment;
- Physical harm;
- Impersonation;
- Intimidation;
- Damaged reputation;
- Impaired eligibility for credit; and
- Misuse of information identified with an individual to obtain a financial product or service, or to access, log into, effect a transaction in or otherwise misuse the individual's account.

Timing Requirements

The Amendments require notice to be provided 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 occurred or is reasonably likely to have occurred. What constitutes "as soon as practicable" may vary based on several factors, such as the time required to assess, contain and control the incident. As an example in the Adopting Release, the SEC provides that an incident of unauthorized access by a single employee to a limited set of Sensitive Customer Information may take only a few days to assess, remediate and investigate. In those circumstances a Covered Institution generally should provide notices to affected

individuals at the conclusion of the tasks and as soon as the notices have been prepared. In addition, the SEC provides that the outside timeframe does not begin from the time that the Covered Institution determines that an incident involved "Sensitive Customer Information." If so, the SEC views this as likely delaying the notification because Covered Institutions may require significant time to determine whether an incident involved Sensitive Customer Information. This delay could extend beyond the allowable timeframe, further postponing any potential notice to affected individuals.

A Covered Institution may delay notices where the disclosure would pose a substantial risk to national security and public safety. The Amendments explain that a delay in this instance will only be provided upon the Attorney General of the United States making that determination and communicating such to the SEC in writing.

Notice Contents and Format

The Amendments require that notices include the following information.

- Key information about the incident, with details regarding:
  - the incident (description of the incident):
  - the breached data (type of Sensitive Customer Information accessed or used without authorization);
  - how affected individuals can respond to the breach to protect themselves; and
  - the date of the incident, the estimated date of the incident or the date range within which the incident occurred, if such information is reasonably possible to determine at the time the notice is provided.

- Contact information sufficient to permit an affected individual to contact the Covered Institution about the incident, including:
  - a telephone number (which should be toll-free 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.

- Information to assist affected individuals in evaluating how they should respond to the incident. If the affected individual has an account with the Covered Institution, the notice must include a recommendation that the customer review account statements and immediately report any suspicious activity to the Covered Institution.
- An explanation of a fraud alert and how an affected individual may place a fraud alert in credit reports.

- A recommendation that the affected individual periodically obtain credit reports from each nationwide credit reporting company and that the individual have information relating to fraudulent transactions deleted.
- An explanation on how a credit report can be obtained free of charge.
- Information regarding the Federal Trade Commission ("FTC") and usa.gov guidance on steps an affected individual can take to protect against identity theft, a statement encouraging the individual to report any incidents of theft to the FTC and the FTC's website address.

Additional information can be included in a notice. However, the SEC provides in the Adopting Release that the inclusion of any additional information may not prevent the required information from being presented in a clear and conspicuous manner. Notices can be provided electronically, through means consistent with current SEC guidance on the electronic delivery of documents.

Finally, the Amendments do not prescribe any specific format for the notice.

Service Providers

Incident Response Program Obligations Regarding Service Providers

The Amendments require that a Covered Institution's incident response program include the establishment, maintenance and enforcement of written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of the Covered Institution's Service Providers. Through these policies and procedures, a Covered Institution must ensure that any Service Provider takes appropriate measures to:

- Protect against unauthorized access to, or use of, Customer Information; and
- Provide breach notification to the Covered Institution as required by the Amendments.

The Amendments do not require a written contract between a Covered Institution and a Service Provider. However, the SEC provides in the Adopting Release that Covered Institutions should generally consider whether a written contract that memorializes the expectations of both the Covered Institution and its Service Providers is appropriate.

In seeking to ensure compliance with these requirements, the SEC states in the Adopting Release that a Covered Institution may receive "reasonable assurances" from its Service Providers that they have taken appropriate measures to both protect Customer Information and provide timely notification to the Covered Institution in the event of a relevant breach of the Service Provider's Customer Information Systems. The SEC further provides that reliance solely on assurances may be insufficient depending on the facts and circumstances. The Amendments provide for a "risk based" approach. Consistent with this "risk based"

approach, the SEC provides that Covered Institutions may wish to consider employing such tools as independent certifications and attestations obtained from the Service Provider, as part of their policies and procedures. Ultimately, whether a Covered Institution meets its due diligence and monitoring obligations relating to Service Providers is a facts and circumstances determination.

The Amendments provide that upon the receipt of a Service Provider's notification, the Covered Institutions must initiate its incident response program. In addition, a Covered Institution must initiate its incident response program where the Covered Institution has otherwise independently detected an incident of unauthorized access to or use of Customer Information at the Service Provider.

Deadline for Service Provider Notice to Covered Institutions and Notice Trigger

The Amendments require that a Covered Institution's policies and procedures be reasonably designed to ensure Service Providers take appropriate measures to provide Covered Institution's with notice as soon as possible, but no later than 72 hours after becoming aware of the occurrence of a breach in security resulting in unauthorized access to a Customer Information System maintained by the Service Provider.

Delegation of Notice and Covered Institution's Customer Notification Obligation

The Amendments permit Covered Institutions, as part of their incident response programs, to enter into a written agreement with their Service Providers to notify affected individuals on the Covered Institution's behalf. The Amendments additionally provide that notwithstanding any Covered Institution's use of a Service Provider, the Covered Institution's obligation to ensure that affected individuals are notified in accordance with the Amendments rests with the Covered Institution. Therefore, where a Covered Institution has entered into a written agreement with its Service Provider to provide notice on the Covered Institution's behalf, the Covered Institution must ensure that the Service Provider has satisfied the customer notification obligations.

In addressing such situations, the SEC provides in the Adopting Release that Covered Institutions should consider including steps for conducting reasonable due diligence to confirm that the Service Provider has provided notice to affected customers. Effective due diligence might include obtaining confirmation of delivery of such notification in the form of attestations or certifications made by the Service Provider and/or confirming with a sample of affected customers that they received the Service Provider notification. The executed due diligence should be timely to permit the Covered Institution to remedy the matter in advance of the delivery deadline set forth in the Amendments, and the Covered Institution's policies and procedures should generally be designed to address these instances. Finally, pursuant to its recordkeeping obligations, the Covered Institution should maintain a copy of any notice transmitted to affected individuals by the Service Provider on the Covered Institution's behalf.

Service Provider Definition

A "Service Provider" is defined 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. The definition includes affiliates of Covered Institutions if they are permitted access to this information through the provision of services. As a note, the definition references "Customer Information" and not "Sensitive Customer Information," thereby expanding the scope of entities subject to the Service Provider definition.

In the Adopting Release, the SEC discussed the request of commenters to clarify the scope of what is included within the Service Provider definition, including whether Service Providers include financial counterparties such as brokers, clearing and settlement firms and custodial banks. The SEC adds that Covered Institutions should make this determination based on the facts and circumstances about the substance of the relationship with the Service Provider, rather than the form of the entity in question. The SEC goes on to state that where financial counterparties receive, maintain or otherwise are permitted access to Customer Information through the provision of services directly to the Covered Institution, they meet the Service Provider definition as adopted.

Definition of Consumer Information, Consumer Report, Sensitive Customer Information and Customer Information System

Consumer Information

Consumer Information is defined as any record about an individual that is a Consumer Report, is derived from a Consumer Report or a compilation of such records, that a Covered Institution maintains or otherwise possesses for a business purpose regardless of whether such information pertains to individuals with whom the Covered Institution has a customer relationship, or to the customers of other financial institutions where such information has been provided to the Covered Institution.

Consumer Report

The Amendments did not revise the definition of Consumer Report found in Regulation S-P. Regulation S-P defines Consumer Report by reference to section 603(d) of the Fair Credit Reporting Act ("FCRA"). The FCRA defines a Consumer Report as any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's

eligibility for credit, insurance, employment or other related purposes. The FCRA provides exceptions to the definition of Consumer Report, including, but not limited to, any report containing information solely as to transactions or experiences between the consumer and the person making the report.

Sensitive Customer Information

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. The definition is meant to include types of information that, if exposed, could put affected individuals at a higher risk of suffering substantial harm or inconvenience through, for example, fraud or identity theft enabled by the unauthorized access to or use of information. The Amendments provide examples of the types of information that will be considered Sensitive Customer Information. These examples include certain Customer Information identified with an individual that, without any other identifying information, could create a substantial risk of harm or inconvenience to an individual identified with the information, along with examples of combinations of identifying information and authenticating information that could create such a risk to an individual identified with the information. Examples of standalone information include:

- Social security number:
- Driver's license number;
- Alien registration number;
- Government passport number;
- Employer or taxpayer identification number;
- Biometric records;
- A unique electronic identification number, address, or routing code; and
- Telecommunication identifying information or access device.

The Amendments highlight information identifying a customer, such as name or online user name, in combination with authenticating information such as a partial Social Security Number, access code, or mother's maiden name as an example of combinations of identifying information and authenticating information.

Customer Information System

Customer Information System is defined as the information resources owned or used by a Covered Institution, 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 Covered Institution's operations.

Scope of Safeguards Rule and Disposal Rule

The Amendments revised the scope of information covered by the safeguards and disposal rules. Specifically, the Amendments:

- Adopt a new definition of "Customer Information" defining the scope of information covered by both the safeguards and disposal rules;
- Expand the scope of the disposal rule, which before the Amendments applied only to Consumer Information (defined as "Consumer Report Information" prior to the Amendments) so that it applies to both Customer Information and Consumer Information;
- Provide that Customer Information protected under both the safeguards and disposal rules includes both Customer Information in the possession of a Covered Institution as well as Customer Information handled or maintained on its behalf; and
- Provide that both Customer Information and Consumer Information include information that pertains to individuals with whom the Covered Institution has a customer relationship, as well as to the customers of other financial institutions where such information has been provided to the Covered Institution.

Recordkeeping

The Amendments provide revisions to the Advisers Act recordkeeping requirements relating to the safeguards and disposal rules. Specifically, the following records are required to be maintained:

- Written policies and procedures required to be adopted and implemented which address administrative, technical and physical safeguards for the protection of Customer Information;
- 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;
- Written documentation of any investigation and determination made regarding whether notification to affected individuals is required, including the basis for any determination made, any written documentation from the 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 to be adopted and implemented which address the oversight, monitoring and conduct of due diligence on Service Providers, including ensuring that the Covered Institution is notified when a breach in security has occurred at the Service Provider;
- Written documentation of any contract or agreement between a Covered Institution and a Service Provider; and
- Written policies and procedures required to be adopted and implemented which address the proper disposal of Consumer Information and Customer Information.

Exception from the Requirement to Deliver Annual Privacy Notice

The Amendments conform Regulation S-P to the previously adopted statutory exception to the annual privacy notice delivery required by Regulation S-P. Specifically, the Amendments provide that delivery of an annual privacy notice is not required if the Covered Institution:

- Only provides non-public personal information to non-affiliated third parties when an exception to the third-party opt out applies; and
- That Covered Institution has not changed its policies and practices with regard to disclosing non-public personal information from its most recent disclosure sent to customers.

Questions? Contact the DCS Team

Dinsmore Compliance Services (DCS), an affiliate of Dinsmore & Shohl LLP, offers compliance solutions for investment managers and municipal advisers. DCS will help you develop and maintain high-quality compliance programs customized to your particular business demands and operational realities. We offer these services, all as an affiliate of a coast-to-coast, full-service law fim.

Kevin Woodard
President
(513) 977-8646
Kevin.woodard@dinsmorecomplianceservices.com

Jeff Chapman
Director of Client Relations
(513) 977-8647
Jeff.chapman@dinsmorecomplianceservices.com

dinsmorecomplianceservices.com