SEC Rulemaking Update
Enhancements to Regulation S-P Final Rulemaking

On May 16, 2024, the SEC adopted amendments to Regulation S-P (***Reg S-P***), the regulation governing the protection and safeguarding of nonpublic information about consumers by financial institutions. The amendments are designed to modernize and enhance the protection of consumer financial information by establishing new requirements for incident response plans and data breach notifications, among other changes. The final rule is effective August 2, 2024. Registered investment advisers with $1.5 billion or more in assets, certain investment companies with $1 billion or more in net assets, as well as certain broker-dealers and transfer agents considered "larger entities" will have an 18-month compliance period (*i.e.*, until February 2, 2026), while smaller entities will have a 24-month compliance period (*i.e.*, until August 2, 2026).

Reg S-P requires "covered institutions" such as registered investment advisers (***RIAs***) to adopt written policies and procedures to protect customer information against unauthorized access and use, including anticipated threats or hazards to the security or integrity of customer information. Reg S-P also requires such institutions to deliver notices to customers initially and annually of their privacy and information-sharing policies informing customers of their rights. A second component of Reg S-P requires financial institutions to properly dispose of consumer report information. A "covered institution" is any broker or dealer, investment company, RIA, or a new covered institution within the final rule, crowdfunding portals. Reg S-P continues to apply to RIAs, but it does not apply to exempt reporting advisers (***ERAs***) or issuers that are excluded from the definition of an investment company under Section 3 of the Investment Company Act of 1940 – such as private funds that are able to rely on Section3(c)(1), or 3(c)(7).

This rulemaking is a first step in updating the SEC's privacy and cybersecurity rulemaking agenda. Two changes from the proposed rule have been perceived as easing some of the regulatory burden for registrants. However, the rule will require advisers to amend existing policies and procedures surrounding information security, privacy, and cybersecurity. Among others, one such change allows either third-party service providers or their RIA counterparts to notify customers of a breach without a written contract between the provider and the adviser, although the final rule also

clarifies that the covered institution, generally the RIA, is ultimately responsible for compliance with rule's provisions on notices to affected individuals, including reasonable investigation, timing, notice contents, and the like. The amendments also expand the recordkeeping requirements of Reg S-P and further require RIAs to have a written incident response policy and procedures for notifying customers in the event sensitive customer information is compromised. In addition, the final rule confirms an existing congressional exception to the annual privacy notice delivery requirement if certain conditions are met. The SEC noted in its press release and factsheet that the amendments to Reg S-P establish a federal minimum standard for providing data breach notifications to affected customers, meaning that it would operate to preempt state requirements to the extent that they are found to conflict with or are broader than the SEC's standards.

In another change to the existing SEC privacy requirements for RIAs, the amendments redefine "customer information" and "consumer information" (formerly "consumer report information") and expand the regulation to extend the safeguards and the disposal rules to both types of information, which is an expansion of the rule to apply to both types of information in certain instances. This expansion of the rule generally puts any customer information in the possession of the covered institution, including such information being handled or maintained on its behalf by a third party, in scope. While the SEC modified the terms "consumer report information" and "consumer information" to effectuate this expansion, it noted that the meaning of the term consumer report information did not change. Previously, Reg S-P defined "customer information" and "consumer report information" separately, making the scope of certain rule obligations potentially limited in their applicability if an adviser determines it has no customers and does not use or maintain consumer report information. Similar to the notice requirements, the SEC clarifies that an RIA's obligations as it relates to privacy include the customer information of any financial institution as discussed in the rule, including nonpublic personal information in any form that the adviser has in its possession or that is being held or used on its behalf.

Incident Response Program

The amended Reg S-P will continue to require RIAs to adopt and implement policies and procedures designed to meet their obligations under both the safeguarding and the disposal rules for customer information, a standalone obligation under the existing and amended rule. Further, the amended rule effectively puts in place a requirement

that advisers adopt and implement a written incident response policy which includes customer notification procedures.

The incident response program may be reasonably designed, but the final rule adds additional and specific requirements that advisers' incident response programs must address. Specifically, it must be 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:

- 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, subject to reasonable investigation

The adviser's incident response policy must also address the notification requirement with specific procedures requiring the assessments and documentation on an incident affecting customer information, to determine if it is sensitive customer information and whether notification is required (as further detailed below).

- **Service Provider Oversight** – The incident response program must include an oversight requirement, including oversight of service providers through due diligence and monitoring. Policies and procedures surrounding service provider oversight may be reasonably tailored to the business, but they must include the specific service provider oversight component.
- **RIA as a Service Provider** - If a covered institution is also acting as a service provider, in addition to its own obligations under rule 248.30, it must provide notification to the other covered institution as required by the policies and procedures required in rule 248.30(a)(5)(i).

Customer Notification Requirements

RIAs will be required to notify customers when "sensitive customer information" was or is reasonably likely to have been accessed or used without authorization, subject to a

reasonable investigation. 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.

The final rule applies to customer information in a covered institution's possession or that is handled or maintained on the covered institution's behalf. This includes information provided to the adviser or its service provider about customers of another financial institution. The final rule modified the notification obligation to avoid duplicate notification obligations, making it the obligation of the covered institution if the breach occurs at the financial institution or at its service provider if the provider is not a covered financial institution. Although the obligation is the adviser's, it may delegate the obligation to its service providers subject to oversight and supervision, including with policies and procedures in the incident response program as discussed above. In addition, RIAs may also be service providers to other financial institutions. Contractual arrangements with all service providers designating the party responsible for sending breach notification as well as notification from the service provider to the adviser are strongly recommended.

Sensitive Customer Information & Harm Assessments

"Sensitive customer information" is a subset of customer information and contains in its definition the potential trigger of a notification obligation if it has been compromised. Whether notification is required in the face of an incident requires a multi-step analysis to determine what was accessed, whether it is customer information, or sensitive customer information, and whether the information was, or is reasonably likely to have been, accessed or used without authorization. Adviser's policies and procedures are expected to track with this framework, and records of determinations should be maintained in the adviser's records. The harm determination is subject to a reasonable investigation, as part of the adviser's incident response process, when compromise occurs.

The final amendments, like the proposed, define the term sensitive customer information to be inclusive of a harm determination, 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 rule does not specify what constitutes "substantial harm or inconvenience," requiring this be determined based on the circumstances surrounding each incident. Similarly, the SEC does not provide a

specific list of data constituting a list of sensitive customer information, but illustrative examples are included as part of the definition. Certain information may be sensitive on its own and others require combination with another piece of customer information to be reasonably likely to create substantial risk. The examples of sensitive information which, by itself, could constitute sensitive customer information given its potential impact are:

- Social Security numbers
- Driver's license or identification number
- Alien registration number
- Government passport number
- Employer or taxpayer identification number
- Biometric records (e.g., fingerprints, iris images)
- A unique electronic identification number (e.g., a student ID)
- Address
- Routing code
- Telecommunication identifying information
- Access device

In addition to one type of information from the list above potentially causing harm, any other customer information, when combined with information from the above list or another piece of customer information, could also create a reasonably likely risk of substantial harm or inconvenience depending on the circumstances, examples of which are noted as an online username plus the authenticating key answer, such as mother's maiden name, birth city, or partial Social Security Number or access code. As with the proposed rule, and in an expansion of nonbinding industry guidance, the SEC notes that other information such as telephone numbers, names, and addresses, can by themselves be sensitive, instead of only in combination with other customer information.

If the information has been compromised, firms are expected to assess potential sensitive customer information based on the circumstances, considering the underlying concepts the rule intends to protect, such as whether the information presents a real or "synthetic" risk to an affected individual of identity theft, fraud, or other harm or inconvenience, and applying various factors applicable to the specific set of circumstances.

Encrypted information presents a unique set of circumstances and is addressed in various parts of the rulemaking. An encryption key or cipher that protects sensitive

personal information's encryption may also be sensitive personal information as may the text of an encrypted file (the cipher). Various factors may affect the determination that such information is sensitive, such as whether it is encrypted at all, whether there is any reason to believe the encryption key has been compromised, has expired, or is outdated compared to industry best practice, or whether, with or without such encryption key, and whether an encrypted file's content (the cipher text) is easily understood by a human being if accessed.

Encrypted information may or may not be sensitive customer information, but it should be used as a factor in a firm's harm assessment, allowing an adviser to determine that the likelihood of substantial harm has been significantly reduced. Data that would otherwise be sensitive customer data, when validly encrypted using the current industry standard best practice encryption may then be classified as customer information. As part of its assessment and reassessment of the harm determination on new facts, the adviser should consider whether there are any facts indicating the encryption has been compromised. For example, if there is reason to believe the encryption key has expired or that the key itself has been accessed, this may create a reasonably likely risk of substantial harm if the underlying information is customer information. The SEC notes in its commentary that it is specifically referring to encryption using "current industry standard best practices" which would be reasonable to use as a factor in determining whether harm is reasonably likely after data has been compromised. It further notes in comments that whether a firm uses best practice standard encryption evolves, such that data encrypted using an outdated standard may not necessarily warrant the determination that data is not sensitive customer data. As noted above, the SEC expects to see a reassessment of this determination if new facts arise, and it follows that firms should also assess whether reliance on current encryption standards continues to be mitigated as industry best practices evolve.

Notice Party, Timing & Form

Notice by the Party Experiencing the Breach or its Service Provider. The rule requires a covered institution to provide notice where unauthorized access to or use of sensitive customer information has occurred at the covered institution or one of the service providers that is not itself a covered institution, as opposed to the covered institution with the customer relationship being the only one with an obligation to send the notice. Further, information pertaining to a covered institution's customers and to customers of other financial institutions that the other institutions have provided to the covered

institution is subject to the safeguards rule under the final amendments, including the incident response program and customer notice requirements. The rule requires notice to all "affected individuals" which is the term used to refer to the adviser's customers and customers of other financial institutions that have provided their customer information to the adviser.

- **30-day Notice Deadline** – Written notice must be provided to the SEC and to affected individuals. The notice period is triggered by awareness of unauthorized use of sensitive customer information, that is either actual or reasonably likely to have occurred, without change from the proposal to the final rule. This awareness marks the beginning of the 30-day outside timeframe.. Firms may delay the written notice if, prior to the 30-day deadline, they have timely requested and been granted a "law enforcement exception" by the US Attorney General (***AG***) in the interest of public safety or national security.
- **Presumption of Notification; Reasonable Investigation** - The SEC notes in its commentary that the written incident response program is generally required to address information security involving any form of customer information, while the notification provisions apply to a smaller subset of customer information, "sensitive customer information." If, after reasonable investigation, results are inconclusive, the SEC expects covered institutions to provide notifications to affected individuals. In the event that it cannot be determined which individual customers' sensitive information was accessed, but access is likely to result in substantial harm or inconvenience, the SEC would expect the notification to be provided to all customers whose information was accessed ("affected individuals"). Thus, the assessments performed under an adviser's incident response program should consider any customer information and whether it has been accessed or used in a manner that would result in substantial harm or inconvenience to the customer. Covered institutions determining that notice is not required must maintain records of the investigation and the basis for the determination.
- **Form and Content** - The notice must contain specified information and be provided clearly and conspicuously in a means designed to ensure the customer can be expected to receive actual notice in writing. Unlike the proposed rule, the final rule does not require covered institutions to detail the steps taken to protect customer information from further unauthorized access

or use. Firms may use their own form of notice (e.g., one that also meets a state's notice requirements) and they may provide additional information, such as the remediation status, but it may not exclude or obscure the rule's proscribed information.

Recordkeeping

The SEC provided additional clarification in the final rule regarding RIA recordkeeping obligations to detailed descriptions of the obligations that are consistent with what was provided for other institutions. Most records relating to the obligations discussed above are required to be created and maintained, some of which will be new for RIAs and since the rule proposal. The required records include: all policies and procedures addressing customer information safeguarding and disposal under the rules, any written delay notice communication to or from the AG, written documentation of any detected unauthorized access or use of customer information, investigation and notification determinations, and service provider contracts and agreements. The amended rules also specify certain information to be created and maintained demonstrating an adviser's incident response policies, such as the steps taken to contain and control incidents and notices provided to affected individuals or records of the adviser's reasonable determination notice was not required. Broadly, required records continue to include records "associated with" the service provider notification requirements, which was not changed substantively from the proposed rule although written contracts with service providers are no longer required. The advisers' records must be maintained for five years, the first two in an easily accessible place.

Annual Privacy Notice Delivery Exception

The final rule amends Regulations S-P, S-ID, and Reg S-AM to adopt the same amendments that were proposed and provide an exception to the annual private notice delivery requirement in certain circumstances, which are generally consistent with an exception adopted by Congress but not included in Reg S-P initially. However, the final rule adds additional details around the timing of an adviser's delivery obligations which have not formally been part of the existing framework for delivery.

The exception to the annual privacy notice requirement is available if the institution (1) only provides non-public personal information to non-affiliated third parties when an exception to third-party opt-out applies and (2) the institution has not changed its policies and practices with regard to disclosing non-public personal information from its most recent disclosure sent to customers. Annual notices are to be provided every

12 months, as per the prior rule. Thus, similar to current practices, advisers are not required to deliver notices to their customers unless they provide customer information to third parties for something other than what is specified in opt-out exemptions, or the adviser amends its policies around disclosing non-public personal information since the most recent disclosure to clients. While current requirements, based on congressional statutes, do not provide a required delivery timeframe within which a notice must be delivered to customers following a change in its non-public information use or policy, the final rule provides that delivery must occur (as an initial notice) within 100 days following the change. The SEC notes that this window might provide advisers an opportunity to include privacy notices with a customer's quarterly statement.

See Final Rule - https://www.sec.gov/rules/2023/03/regulation-s-p-privacy-consumer-financial-information-and-safeguarding-customer#34-100155