Published on *The National Law Review* https://natlawreview.com

SEC Finalizes Amendments to Regulation S-P

Article By:

Richard F. Kerr

Sasha Burstein

Brian Doyle-Wenger

On 16 May 2024, the Securities and Exchange Commission (SEC) adopted amendments (amendments) to Regulation S-P representing the first major changes to Regulation S-P since its initial adoption in 2000. Although the amendments do not change the substantive privacy policy provisions of the rule, they do impose significant new privacy-related protections and obligations including:

Adoption of Incident Response Program

Requiring brokers and dealers, investment companies, registered investment advisers, funding portals, and transfer agents registered with the SEC or another appropriate regulatory agency (collectively, covered institutions) as defined in the Securities Exchange Act of 1934 (Exchange Act) to adopt written incident response program policies and procedures to address unauthorized access to or use of customer information, including procedures for providing timely notification to individuals affected by an incident involving sensitive customer information.

Expansion of Scope to All Transfer Agents

Expanding the applicability of the safeguards rule[1] to include transfer agents and the disposal rules[2] to include all transfer agents including those that are not SEC registered.

Broadening Scope of Covered Information

Broadening the scope of information covered by the safeguards and disposal rules.

Imposing Recordkeeping Requirements

Imposing requirements to maintain written records documenting compliance with the amended rules.

Codify Exception to Privacy Policy Delivery Obligation

Creating an exception to the delivery provisions for the annual privacy notice consistent with a statutory amendment to the Gramm-Leach-Bliley Act (GLBA).[3]

INCIDENT RESPONSE PROGRAM

In an effort to address the expanded use of technology and the corresponding risks, the amendments require covered institutions to adopt incident response program policies and procedures that address unauthorized access to or use of customer information, including customer notification procedures. For purposes of Regulation S-P, a customer is a consumer that has a customer relationship with the covered institution. A consumer is an individual who obtains or has obtained a financial product or service that is to be used primarily for personal, family, or household purposes, or that individual's legal representative. With respect to transfer agents, the amendments define a customer as any natural person who is a securityholder of an issuer for which the transfer agent acts or has acted as a transfer agent. Although the amendments do not dictate the specific steps that a covered institution must take when carrying out its incident response program, each covered institution’s incident response program must have written policies and procedures that:

- 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 in accordance with the notification obligations, 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.

Assessment

The amendments require each covered institution’s incident response program to include procedures for: (1) assessing the nature and scope of any incident involving unauthorized access to or use of customer information and (2) identifying the customer information systems and types of customer information that may have been accessed or used without authorization. The assessment requirement is designed to identify both the customer information systems (i.e., information resources owned or used by a covered institution, including physical or virtual infrastructure) and types of customer information that may have been accessed or used without authorization during the incident, as well as the specific customers affected, which is necessary to fulfill the amendments’ notification requirements.

Containment and Control

An incident response program must have 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, such as 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.

Notification

Covered institutions must notify each 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, 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.

What Is Sensitive Customer Information?

While the incident response program is generally required to address information security incidents involving any form of customer information, notification to customers is only required when there has been unauthorized access to or use of sensitive customer information, a subset of customer information.

Sensitive customer information is defined to be any component of customer information that the compromise of which, alone or in conjunction with any other information, could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information. Examples of sensitive customer information include social security numbers and other types of identifying information that can be used alone to authenticate an individual's identity, such as a driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, biometric records, a unique electronic identification number, address, routing code, or telecommunication identifying information or access device.[4] It is worth noting that whether or not access to or use of particular customer information rises to a level that it presents a "reasonably likely risk of substantial harm or inconvenience to a individual identified with the information" is an subjective standard and firms may differ in their interpretations. As such, covered institutions may want to establish criteria for this standard in their policies and procedures.

Timing, Contents, and Format Requirements for Notifications

The amendments require covered institutions to provide notice as soon as a practicable but no later than 30 days after a covered institution becomes aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred. The amount of time that constitutes "as soon as practicable" may vary based on several factors, such as the time required to assess, contain, and control the incident. Moreover, the adopting release provides that notice will not be required if "after a reasonable investigation of the facts and circumstances," the covered institution determines that access to customer information has not occurred or is not reasonably likely to have occurred. However, the rule does not provide parameters or any time limits on the manner of investigation that is necessary. As such, covered institutions may vary in their investigation requirements and standard for determining when access or use of customer information is "reasonably likely" to have occurred.

If notice is required, it must contain key information in a clear and conspicuous manner and by means designed to ensure the customer can reasonably be expected to receive actual notice in writing including:

- Details about the incident, breached data, and how individuals can respond to protect themselves;
- Contact information sufficient to permit an individual to contact the covered institution about the incident, including a telephone number, an email address, a postal address, and the name of a specific office to contact for further information or assistance, including information of a

third-party service provider that has been engaged by the covered institution to provide specialized information or assistance about the incident on behalf of the covered institution;
- The date of the incident or the estimated date or date range within which the incident occurred;

Due Diligence and Monitoring of Service Providers

In addition to the above requirements, each incident response program must include policies and procedures reasonably designed to require oversight, including through due diligence on and monitoring, of service providers. The amendments broadly define a service provider 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.

Rather than requiring each covered institution to enter into a written contract with its service providers, as initially proposed, the amendments require that a covered institution's policies and procedures ensure service providers take appropriate measures to: (1) protect against unauthorized access to or use of customer information and (2) provide notification to the covered institution as soon as possible, but no later than 72 hours after becoming aware that a breach in security has occurred resulting in unauthorized access to a customer information system maintained by the service provider.

Covered institutions, as part of their incident response programs, may enter into a written agreement with their service providers to notify affected individuals on the covered institution's behalf but remain responsible to ensure that affected individuals are notified.

SCOPE OF INFORMATION PROTECTED

The amendments broaden and more closely align the scope of both the safeguards rule and the disposal rule by applying the requirements of those rules to the information of not only a covered institution's own customers, but also the information of customers of other financial institutions that has been made available to the covered institution, including information handled or maintained on behalf of a covered institution.

Definition of Customer Information

Currently, Regulation S-P's protections under the safeguards rule and disposal rule apply to different, and at times overlapping, sets of information. Specifically, as required under GLBA, currently, the safeguards rule requires broker-dealers, investment companies, and registered investment advisers (but not transfer agents) to maintain written policies and procedures to protect "customer records and information," which is not defined in GLBA or in Regulation S-P. Whereas, the disposal rule requires every covered institution to properly dispose of "consumer report information," a different term that Regulation S-P defines consistently with Fair and Accurate Credit Transactions Act of 2003 (FACT Act) provisions.

To more closely align the information protected by both rules, the amendments replace the term "customer records and information" in the safeguards rule with a newly defined term "customer information" which is defined as any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, and includes information in the possession of or that is handled or maintained by the covered institution.

Safeguards Rule and Disposal Rule Coverage of Customer Information

The amendments also require that both the safeguards rule and the disposal rule apply to the information specified in those definitions regardless of whether such information pertains to (1) individuals with whom the covered institution has a customer relationship or (2) the customers of other financial institutions where such information has been provided to the covered institution. This contrasts with the current requirement in Regulation S-P to protect only the information of "a consumer who has a customer relationship with you."

EXTENDING THE SCOPE OF THE SAFEGUARDS RULE AND THE DISPOSAL RULE TO COVER ALL TRANSFER AGENTS

In acknowledging the sensitive and detailed information maintained by transfer agents, the amendments extend both the safeguards rule and the disposal rule to any transfer agent registered with the SEC or another appropriate regulatory agency. Although the SEC received several comments opposing this change, including that it would exceed the SEC's authority and would result in regulatory confusion, the SEC asserted that the expansion was necessary to comply with GLBA and the FACT Act.

Definition of a Transfer Agent's Customer

The amendments include a definition of "customer" that is specific to transfer agents and solely for purposes of the amendments. For a transfer agent, a "customer" is defined to be any natural person who is a securityholder of an issuer for which the transfer agent acts or has acted as a transfer agent.

Maintaining the Current Regulatory Framework for Notice-Registered Broker-Dealers

The amendments contain a number of amendments to Regulation S-P that result in the continuation of the same regulatory treatment for notice-registered broker-dealers[5] as they were subject to under the existing safeguards rule and disposal rule. Specifically, notice-registered broker-dealers are explicitly excluded from the scope of the disposal rule, but subject to the safeguards rule.

RECORDKEEPING

The amendments require covered institutions to make and maintain written records documenting compliance with the requirements of the safeguards rule and the disposal rule as outlined in the table below.

Covered Institution	Retention Period
Registered Investment Companies and BDCs	*Policies and Procedures.* A copy of policies and procedures in effect, or that at any time in the past six years were in effect, in an easily accessible place. *Other records.* Six years, the first two in an easily accessible place.
Registered Investment Advisers	All records for five years, the first two in an easily accessible place.

Covered Institution	Retention Period
Broker-Dealers and Transfer Agents	All records for three years, in an easily accessible place.

EXCEPTION FROM REQUIREMENT TO DELIVER ANNUAL PRIVACY NOTICE

Currently, Regulation S-P generally requires broker-dealers, investment companies, and registered investment advisers to provide customers with annual notices informing them about the institutions' privacy practices. The amendments conform Regulation S-P to the requirements of the FAST Act, which provides an exception to the annual privacy notice required by Regulation S-P, provided certain requirements are met. Specifically, an institution is exempt from providing annual notices if (1) it 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.

EFFECTIVE DATE

The effective date for the amendments will be 60 days after publication in the Federal Register, with compliance dates of 18 months for investment companies with net assets of US$1 billion or more, registered investment advisers with assets under management of US$1.5 billion or more, and broker-dealers and transfer agents that are not small entities under the Exchange Act. Other covered institutions will have 24 months after publication in the Federal Register to comply.

RECOMMENDED NEXT STEPS FOR COVERED INSTITUTIONS

In light of the amendments, covered institutions may wish to consider, among other things, doing the following to determine where they are with respect to compliance with the amendments:

- Review existing policies and procedures to identify gaps that will need to be addressed prior to the effective date of the amendments. Among other things, consider changes necessary to conform with the new definitions included in the amendments described above;
- Identify and evaluate information received from third parties to determine where the covered institution receives information that would be deemed to be protected under the amendments and consider whether it is necessary to receive such information. To the extent it is necessary, review policies and procedures to confirm that such information may be adequately protected under them; and
- Review contracts for third party services where customer information is provided to the third party to confirm compliance with the amendments and whether modification to such contracts is necessary.

The foregoing are just some of the areas that the amendments may result in changes for covered institutions. As such, covered institutions should effectively use the compliance period to review their practices and determine where modification is necessary.

[1] The "safeguards rule" currently requires that brokers, dealers, investment companies and investment advisers adopt and implement written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and

information.

[2] The “disposal rule” currently requires that brokers and dealers (other than notice-registered broker-dealers), investment companies, investment advisers and transfer agents registered with the SEC that maintain or otherwise possess consumer report information for a business purpose 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.

[3] As discussed further below, under an amendment added as part of the Fixing America’s Surface Transportation Act (FAST Act), covered financial institutions are not required to deliver an annual privacy notice if certain conditions are met. The amendments codify that exemption in SEC rule.

[4] Although requested by multiple commenters, the amendments do not include an exception or safe harbor for encrypted information. However, the SEC acknowledged 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.

[5] Notice-registered broker-dealers are futures commission merchants and introducing brokers registered with the CFTC that are permitted to register as broker-dealers by filing a notice with the SEC for the limited purpose of effecting transactions in security futures products. As discussed on page 119 of the adopting release, the amendments are designed to result in the continuation of the same regulatory treatment for notice-registered broker-dealers as they were subject to under the existing safeguards rule and disposal rule.

National Law Review, Volume XIV, Number 162