The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 35718

May 23, 2024

SEC Adopts Amendments to Regulation S-P

[35718]

May 23, 2024

TO: ICI Members
Chief Compliance Officer Committee
Chief Information Security Officer Committee
Closed-End Investment Company Committee
Compliance Advisory Committee
Investment Advisers Committee
Operations Committee
Privacy Issues Working Group
SEC Rules Committee
Small Funds Committee
Technology Committee
Transfer Agent Advisory Committee
Unit Investment Trust Committee RE: SEC Adopts Amendments to Regulation S-P

On May 16, 2024, the SEC unanimously adopted amendments to Rule 248.30 in Regulation S-P (the "amendments").[1] Since its adoption in 2000, Regulation S-P has required the safeguarding of customer records and information and the disposal of consumer report information. In recognition of technological advancements over the past 20 years, the amendments are intended to enhance consumer financial information protection and establish a minimum standard to provide data breach notifications for brokers, dealers, investment companies, registered investment advisers and transfer agents ("covered institutions") at the federal level. We briefly summarize the amendments (Section I), then detail changes from current law and the Proposal (Section II), below. The amendments will become effective 60 days after publication in the Federal Register. Larger entities will have 18 months after the date of publication in the Federal Register to comply with the amendments, and smaller entities will have 24 months after the date of publication in the Federal Register to comply.[2]

I. Summary

The Commission adopted the amendments substantially as proposed, with some changes in response to comments. The amendments in particular update the requirements of the "safeguards" and "disposal" rules. The safeguards rule requires covered institutions to

adopt written policies and procedures that address administrative, technical, and physical safeguards to protect customer records and information. The disposal rule, which applies to every covered institution, other than notice-registered broker-dealers, requires proper disposal of consumer report information.

The principal elements of the amendments are as follows:

Incident Response Program. As proposed, the safeguards rule now requires covered institutions to develop, implement, and maintain written policies and procedures for an incident response program that is reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information.[3] The amendments require that a response program include: 1) procedures to assess the nature and scope of any incident, including identifying the customer information systems and types of customer information that may have been accessed or used without authorization and 2) to take appropriate steps to contain and control the incident to prevent further unauthorized access or use. The amendments do not prescribe specific steps a covered institution must undertake when carrying out incident response activities. Instead, the Adopting Release provides that covered institutions can create policies and procedures best suited to their particular circumstances.[4]

30-day Customer Notification Requirement.[5] The amendments also require that covered institutions provide a notification to affected individuals whose sensitive customer information[6] was, or is reasonably likely to have been, accessed or used without authorization. The Commission will not require notice if a 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.

Under the amendments, a customer notice must be clear and conspicuous and provided by a means designed to ensure that each affected individual can reasonably be expected to receive it. This notice must be provided as soon as reasonably practicable, but not later than 30 days, after the covered institution becomes aware that unauthorized access to or use of customer information has, or is reasonably likely to have, occurred. Further, the amendments will permit covered institutions to delay providing notice if the Commission receives a written request from the Attorney General that this notice poses a substantial risk to national security or public safety.[7]

Service Provider Oversight. The amendments to the safeguards rule include new provisions that address the use of service providers by covered institutions.[8] Under these provisions, covered institutions will be required to establish, maintain, and enforce written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring of service providers, including to ensure that affected individuals receive any required notices. The amendments make clear that while covered institutions may use service providers to provide any required notice, covered institutions will retain the obligation to ensure that affected individuals are notified in accordance with the notice requirements.

Scope of the Safeguards and Disposal Rules. The amendments will more closely align the information protected under the safeguards rule and the disposal rule by applying the protections of both rules to "customer information," a newly defined term. The amendments will also broaden the group of customers whose information is protected

under both rules. Also, transfer agents will be required to comply with the safeguards rule.

Recordkeeping and Annual Notice Amendments. The amendments will add requirements for covered institutions, other than funding portals,[9] to make and maintain written records documenting compliance with the requirements of the safeguards rule and the disposal rule. Further, the amendments amend the existing requirement to provide annual privacy notices to codify a statutory exception provided that certain conditions are met. Specifically, an entity can be exempted if it "(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."[10]

II. Changes to Current Law and Changes from the Proposal

Rule 248.30(a)

Currently, Rule 248.30(a) requires every broker, dealer, investment company, and investment adviser registered with the Commission to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. Such policies and procedures must be reasonably designed to ensure the security and integrity of customer records and information; protect such records and information from anticipated threats or hazards; and protect them against unauthorized access that could result in any harm or inconvenience to the customer.

As amended, the above subsection (a) no longer references brokers, dealers, investment companies, and investment advisers. Instead, these institutions would be referred to as "covered institutions" and the definition of "covered institutions" includes transfer agents, even those not registered with the SEC.[11]

Rule 248.30(a)(1) and (2): Required Policies and Procedures

The provisions of the current rule governing the required policies and procedures are substantively identical to amended Rule 248.30(a). The Commission did not receive comments on these provisions and have adopted them as proposed.

NEW Rule 248.30(a)(3): Response Programs for Unauthorized Access to or Use of Customer Information

The Commission adopted this requirement substantially as proposed, with some changes in response to comments. Added to the existing requirements, is a new provision, subsection (a)(3), requiring policies and procedures to include "a response program for unauthorized access to or use of customer information." These policies and procedures would be required to govern "a program reasonably designed to detect, respond to, and recover from unauthorized access to our use of customer information." Among other things, they must include provisions to "notify each affected individual whose sensitive customer information was, or is, reasonably likely to have been accessed or used without authorization . . .". The notification details are set forth in new subsection (a)(4).

NEW Rule 248.30(a)(4): Notifying Affected Individuals of Unauthorized Access or Use

This new provision is divided into four subdivisions:

- Subdivision 248.30(a)(4)(i) – Notification Obligation. This subdivision requires the covered institution, after conducting a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information that occurred at the covered institution or one of its service providers that is not itself a covered institution, to provide a clear and conspicuous written notice (which can be electronic), or to ensure notice is provided, to each affected individual whose sensitive information was, or is reasonably likely to have been, accessed or used without authorization.
- Subdivision 248.30(a)(4)(ii) – Affected Individuals. This provision would specify that, if the covered institution cannot identify specific individuals harmed by the intrusion, it must notify all individuals whose information was or was reasonably likely to have been accessed or used without authorization. To address commenters concerns, in a change from the Proposal, the amendments explicitly provide that, in cases where a covered institution reasonably determines that a specific individual's sensitive customer information that resides in the customer information system was not accessed or used without authorization, the covered institution need not provide notice to that individual.
- Subdivision 248.30(a)(3)(iii) – Timing. This provision specifies that the written notice must be provided as soon as practicable but not later than 30 days after becoming aware of the intrusion. The only exception to this is if the US Attorney General delays the notification due to national security interests. As explained in footnote 7 above, in a modification from the Proposal, the amendments provide for an incrementally longer period of time than the Proposal for a covered institution to delay providing notice to affected individuals in cases where the Attorney General has determined that providing the notice would pose a substantial risk to national security or public safety.
- Subdivision 248.30(a)(4)(iv) – Notice Contents. According to this provision, the notice must include the following:
    - A general description of the intrusion;
    - Information about when the incident occurred;
    - Information on who to contact for further information and assistance;
    - Advice that any customer of the institution review account statements and report any suspicious activity;
    - An explanation of fraud alerts and how to place one on a credit report;
    - A recommendation that the individual periodically obtain credit reports from each nationwide credit reporting agency and have information related to fraudulent transactions deleted;
    - An explanation of how the individual may obtain a credit report free of charge; and
    - Information about the online guidance available from the Federal Trade Commission on usa.gov about identify theft protections.

The amendments, consistent with the Proposal, require that notices include key information with details about the incident, the breached data, and how affected individuals can respond to the breach to protect themselves. In a modification from the Proposal, however, the amendments will not require the notice to "[d]escribe what has been done to protect the sensitive customer information from further unauthorized access or use."

In the ICI Letter, ICI urged the Commission to remove the requirement for covered institutions to provide "the date of the incident, the estimated date of the incident, or the date range," asserting that this specific information is not required by the Banking Agencies' Incident Response Guidance and should not be included in an amended

Regulation S-P. The Commission, however, did not modify the proposed requirement for covered institutions to provide information about the date of the incident, as suggested. As the Adopting Release explains, "[p]roviding this information to affected individuals, to the extent the information is reasonably possible to determine, can help affected individuals identify the point in time in which their sensitive customer information was compromised, thus providing critical details that affected individuals can use to take targeted protective measures (e.g., review account statements) to mitigate the potential harm that could result from the unauthorized access to or use of their sensitive customer information. For this reason, we disagree with the commenter that stated firms should not be required to provide this information in their notice."[12]

NEW Rule 248.30(a)(5): Service Providers

"Service Provider" is defined in the amendments to mean "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." (See Rule 248.30(d)(10).) The Commission revised the definition of service provider from the Proposal to remove reference to third parties to incorporate into rule text the Commission's intended scope of the "service provider" definition and make clear that the definition can include affiliates of a covered institution.

This portion of the rule would require the covered institution's response program (required by Rule 248.30(a)(3)) to "include the establishment, maintenance, and enforcement of written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers, including to ensure that the covered institution notifies affected individuals as set forth in paragraph (a)(4) of [the amendments]."

In a change from the Proposal, rather than requiring written policies and procedures requiring the covered institution to enter into a written contract with its service providers to take certain appropriate measures, the amendments require policies and procedures to be reasonably designed to ensure service providers take appropriate measures to: (A) protect against unauthorized access to or use of customer information; and (B) provide notification to the covered institution as soon as possible, but no later than 72 hours after becoming aware of a breach in security has occurred resulting in unauthorized access to a customer information system maintained by the service provider. In another modification from the Proposal, upon receipt of such notification, a covered institution must initiate its incident response program pursuant to Rule 248.30(a)(3). Therefore, as the Adopting Release explains, the amendments modify the Proposal by removing the written contract requirement and shifting the notification deadline for the service provider's notification of the covered institution from 48 to 72 hours, while retaining the notice trigger of the service provider "becoming aware of" a breach in security resulting in unauthorized access to a customer information system maintained by the service provider.[13]

However, even though the Commission removed the proposed written contract provision, the amendments provide that a covered institution, as part of its incident response program, may enter into a written agreement with its service provider to notify affected individuals on the covered institution's behalf in accordance with paragraph (a)(4) of the amendments.[14] The amendments also add new language which clarify that even where a covered institution uses a service provider in accordance with paragraphs (a)(5)(i) and (ii) of the amendments, the obligation to ensure that affected individuals are notified in accordance with paragraph (a)(4) of the amendments rests with the covered institution.

Revised Rule 248.30(b): Disposal of Consumer and Customer Information

Currently, Rule 248.30(b) requires brokers, dealers, investment advisers, investment companies, and transfer agents to properly dispose of consumer report information and records. This provision would be revised, and is adopted substantially as proposed, to require the following: "Every covered institution, other than notice-registered broker-dealers, must properly dispose of consumer information and customer information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal." The amendments adopt a new definition of "customer information" defining the scope of information covered by both the safeguards and disposal rules. These amendments provide greater specificity regarding what constitutes customer information that must be protected under the safeguards rule. They also expand the scope of the disposal rule, which currently applies only to consumer information (defined as "consumer report information" in the current rule) so that it applies to both customer and consumer information.[15]

NEW Rule 248.30(c): Recordkeeping

A new subsection (c) would be added to the rule requiring a covered institution to maintain records documenting compliance with the rule. The Commission adopted these amendments substantially as proposed, but, in response to a comment, with modifications designed to provide additional specificity to the scope of certain of the recordkeeping requirements. These records would need to be maintained for 6 years, the first two in an easily accessible place for registered investment companies. ICI supported these recordkeeping requirements in the Proposal.

NEW Rule 248.30(d): Definitions

A new definitions section would be added to the rule to define the following terms, among others:

- Consumer information;[16]
- Consumer report;
- Covered institution;
- Customer;
- Customer information;[17]
- Customer information systems;
- Disposal; and
- Sensitive customer information;[18]
- Service provider; and
- Transfer agent.

Upon the compliance date, the Commission may withdraw or rescind certain staff letters and other staff statements addressing Regulation S-P and other matters covered by the final amendments in connection with this adoption.

Mitra Surrell
Associate General Counsel, Markets, SMAs, & CITs

Notes

[1] See Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, SEC Release Nos. 34-100155, IA-6604, and IC-35193 (May 16, 2024) (the "Adopting Release"), available at: https://www.sec.gov/files/rules/final/2024/34-100155.pdf. See also Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, SEC Release Nos. 34-97141, IA-6262, and IC-34854 (March 15, 2023) (the "Proposal"), available at: https://www.sec.gov/rules/proposed/2023/34-97141.pdf. See also Letter from Tamara K. Salmon, Senior Associate Counsel, ICI, to Vanessa Countryman, Secretary, SEC, dated May 23, 2023, available at https://www.sec.gov/comments/s7-05-23/s70523-193259-384202.pdf ("ICI Letter"). ICI supported the amendments in the Proposal and was pleased that the Commission's approach strove to be consistent with the Interagency Guidelines Establishing Standards for Safeguarding Customer Information (the "Interagency Guidelines") adopted by the federal banking regulators (66 FED. REG. 8816 (February 1, 2001)). In the ICI Letter, ICI only recommended a few tweaks to the Proposal to be more consistent with the Interagency Guidelines.

[2] The original compliance date proposed was 12-months for all covered institutions, regardless of asset size. ICI advocated for a 24-month compliance period in the ICI Letter.

[3] 17 CFR § 248.30(a)(3). "Customer information" is a newly defined term, see footnote 16 below discussing the full definition of "customer information."

[4] Adopting Release at p. 18. See also the discussion on pp. 10-20 regarding flexibility and a facts and circumstances approach.

[5] 17 CFR § 248.30(a)(3)(iii) and 17 CFR § 248.30(a)(4).

[6] See footnote 17 below discussing the definition of "sensitive customer information."

[7] 17 CFR § 248.30(a)(4)(iii). In the ICI Letter, ICI advocated that the Commission revise the timing of the breach notices to accommodate law enforcement investigations. ICI commented that it is unclear what process would be followed to obtain written direction from the US Attorney General. Delays in breach notices should be permitted if such delays are requested by any law enforcement agency. That approach would align with the Commission's prior position and well established requirements in the Interagency Guidelines and state laws. However, the amendments maintained the narrow exception of determination from the US Attorney General, as proposed, and revised that notification may be delayed for up to 30 days (60 days in extraordinary circumstances) for either national security or public safety concerns rather than the proposed 15 days.

[8] See discussion below regarding new Rule 248.30(a)(5) and the definition of service provider.

[9] "Funding portals act as intermediaries in facilitating securities-based crowdfunding transactions that are subject to Regulation Crowdfunding." See Adopting Release at 187.

[10] Adopting Release at p 127. The amendments also, as proposed, provide the timing for when an institution must resume providing annual privacy notices if the institution changes its policies and practices such that the exception no longer applies. ICI, as provided in the ICI Letter, supported the proposed exception and timing requirements.

[11] In the ICI Letter, ICI supported extending these rules to all transfer agents.

[12] Adopting Release at pp. 67-68.

[13] Adopting Release at pp. 69-70. Although not adopted by the Commission, as noted in the ICI Letter, ICI did not oppose the written contractual requirement in Section 248.30(b)(5) because of its very narrow scope. Further, ICI did not oppose the 48 hour notice trigger.

[14] In the ICI Letter, ICI supported the Commission permitting covered institutions to have their service providers send breach notices to affected individuals on their behalf, stating that it is a common practice today for investment companies to have their transfer agents assume responsibility for sending affected customers breach notices.

[15] Adopting Release at p. 93.

[16] Modified from the Proposal, this term would mean any record about an individual, whether in paper, electronic or other form, that is a consumer report or 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 (i) individuals with whom the covered institution has a customer relationship, or (ii) to the customers of other financial institutions where such information has been provided to the covered institution. Consumer information does not include information that does not identify individuals, such as aggregate information or blind data.

[17] Modified from the Proposal, this term for any covered institution other than a transfer agent registered with the Commission or another appropriate regulatory agency (ARA) means any record containing nonpublic personal information as defined in § 248.3(t) about a customer of a financial institution, whether in paper, electronic or other form, that is in the possession of a covered institution or that is handled or maintained by the covered institution or on its behalf regardless of whether such information pertains to (a) individuals with whom the covered institution has a customer relationship, or (b) to the customers of other financial institutions where such information has been provided to the covered institution. With respect to a transfer agent registered with the Commission or another ARA, customer information means any record containing nonpublic personal information as defined in § 248.3(t) identified with any natural person, who is a securityholder of an issuer for which the transfer agent acts or has acted as transfer agent, that is in the possession of a transfer agent or that is handled or maintained by the transfer agent or on its behalf, regardless of whether such information pertains to individuals with whom the transfer agent has a customer relationship, or pertains to the customers of other financial institutions and has been provided to the transfer agent.

[18] This term means any "means 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 amendments provides examples of sensitive customer information which include: (1) Customer information uniquely identified with an individual that has a reasonably likely use as a means of authenticating the individual's identity, such as a Social Security number, official State- or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, a biometric record, a unique electronic identification number, address, or routing code, telecommunication identifying information or access device (as

defined in 18 U.S.C. 1029(e)); or (2) customer information identifying an individual or the individual's account, including the individual's account number, name or online user name, in combination with authenticating information that could be used to gain access to the customer's account such as an access code, a credit card expiration date, a partial Social Security number, a security code, a security question and answer identified with the individual or the individual's account, or the individual's date of birth, place of birth, or mother's maiden name.

In the ICI Letter, ICI recommended that the Commission revise the proposed definition of "sensitive customer information" to better align with the definition of this term in the Interagency Guidelines, however the Commission adopted the definition as proposed.
