The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 35189

March 16, 2023

SEC Publishes Proposed Revisions to Regulation S-P That, In Part, Will Require Breach Notices

[35189]

March 16, 2023

TO: Privacy Issues Working Group
Transfer Agent Advisory Committee RE: SEC Publishes Proposed Revisions to Regulation S-P That, In Part, Will Require Breach Notices

Yesterday, the SEC published for comment proposed revisions to Rule 248.30 in Regulation S-P.[1] This is the section of the regulation that requires the safeguarding of customer records and information and the disposal of consumer report information. The proposed revisions are summarized below. Comments on the proposal will be due 60 days after it is published in the Federal Register.

In the near term, the ICI will be scheduling calls of the Privacy Issues Working Group and the Transfer Agent Advisory Committee to get your input on this proposal to assist us in drafting our comment letter. If you will be able to join us for the call, in anticipation of it, please familiarize yourself with the proposal.

Current Law; Proposed Changes

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 proposed, the above subsection (a) would become subsection (b) of this Rule. A new subsection (a) would be added to define the "scope of information" covered by Rule 248.30. No longer would this provision reference brokers, dealers, investment companies, and

investment advisers. Instead, these institutions would be referred to as "covered institutions" and the definition of "covered institutions" would include transfer agents, even those not registered with the SEC.

New subsection (a) would also add to the rule's current scope (i.e., customer records and information) "all customer information in the possession of a covered institution, and all consumer information that a covered institution maintains or otherwise possesses for a business purpose" regardless of whether the information relates to a customer of the institution. As such, information about an individual that has been provided to the covered institution by another institution would be within the scope of the revised rule even if such person is not a customer of the covered institution.

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

The provisions of the current rule governing the required policies and procedures will be found in Rule 248.30(b)(1) and (2). These sections of the rule are substantively identical to Rule 248.30(a).

NEW Rule 248.30(b)(3): Response Programs for Unauthorized Access

Added to the existing requirements, is a new provision, subsection (b)(3), requiring the existing 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 (b)(4).

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

This new provision is divided into four subdivisions:

- Subdivision 248.30(b)(4)(i) – Notice. This subdivision requires the covered institution, after conducting a reasonable investigation of the facts and circumstances, to provide a clear and conspicuous written notice (which can be electronic) to each individual whose sensitive information was, or is reasonably likely to have been, accessed or used without authorization.
- Subdivision 248.30(b)(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.
- Subdivision 248.30(b)(4)(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.
- Subdivision 248.30(b)(4)(iv) – Notice Contents. According to this provision, the notice must include the following:

    - A general description of the intrusion;
    - What has been done to protect sensitive customer information from further unauthorized access or use;

- 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.

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

"Service Provider" is defined in the proposal to mean "any person or entity that is a third party and receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution." (See proposed Rule 248.30(e)(10).) This portion of the rule would require the covered institution's response program (required by Rule 248.30(b)(3)) to "include written policies and procedures requiring the institution pursuant to a written contact ... to require the service providers to take appropriate measures that are designed to protect against unauthorized access to or use of customer information, including notification to the covered institution as soon as possible, but no later than 48 hours after becoming aware of a breach" if the breach results in unauthorized access to a customer information system maintained by the service provider. [Emphasis added.] This notice is to enable the covered institution to implement its response program. The rule additionally provides that, as part of the institution's response program, it "may enter into a written agreement with its service provider to notify affected individuals on its behalf" in accordance with the requirements of new Section 248.30(b)(4).

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

Currently, Rule 248.30(c) requires brokers, dealers, investment advisers, investment companies, and transfer agents to properly dispose of consumer report information and records. This provision would be revised to: (1) require policies and procedures addressing the proper disposal of consumer information customer information and (2) expand the scope of this provision to include any "consumer information" in addition to the current "consumer report information."

NEW Rule 249.30(d): Recordkeeping

A new subsection (d) would be added to the rule requiring a covered institution to maintain records documenting compliance with the rule. These records would need to be maintained for 6 years, the first two in an easily accessible place.

NEW Rule 248.30(e): Definitions

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

- Consumer information;[2]

- Consumer report;
- Covered institution;
- Customer;
- Customer information;
- Customer information systems;
- Disposal; and
- Sensitive customer information;[3]
- Service provider;
- Substantial harm or inconvenience;[4] and
- Transfer agent.

Tamara K. Salmon
Associate General Counsel

Notes

[1] See 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 "Release"), which is available at: https://www.sec.gov/rules/proposed/2023/34-97141.pdf.

[2] This term would mean any record containing nonpublic personal information as defined in Reg. S-P.

[3] This term would mean any "component of customer information alone or in conjunction with any other information the compromise of which could create a reasonably likely risk of harm or inconvenience to an individual identified with the information." The rule would include examples of this information.

[4] This term would mean "personal injury, or financial loss, expenditure of effort or loss of time that is more than trivial, including theft, fraud, harassment, physical harm, impersonation, intimidation, damaged reputation, impaired eligibility for credit, or the misuse of the information ... to obtain a financial product or service, or to access, log into, effect a transaction in, or otherwise misuse the individual's account."