March 21, 2023

SEC Proposes to Amend Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information

On March 15, 2023, the SEC issued a release (the "Release") containing proposed amendments to Regulation S-P[1] (the "Proposals") that, if adopted, would require broker-dealers, registered investment companies (with business development companies, "registered funds") and investment advisers to adopt written policies and procedures creating an incident response program to deal with unauthorized access to customer information, including procedures for notifying persons affected by the incident within 30 days. The Proposals would be in addition to the SEC's other pending cybersecurity regulations. The Proposals would also:

- Require response programs to include written policies and procedures that address the risk of harm posed by security compromises at a covered institution's service providers, including mandatory contract provisions with the service providers;
- Include transfer agents among the covered institutions that are subject to the safeguards rule (described below) and response program requirements;
- Require covered institutions to adopt and implement written policies and procedures to address the disposal of customer information;
- Require covered institutions to maintain written records documenting compliance with the Proposals; and
- Conform Regulation S-P's annual privacy notice delivery provisions to include an exception required by a 2015 statutory amendment to the Gramm-Leach-Bliley Act (the "GLBA").

The Proposals are described in detail below.

Background

Regulation S-P was adopted by the SEC in 2000. Currently, Regulation S-P's provisions include, among other requirements, Rule 248.30(a) (the "safeguards rule"), requiring broker-dealers, registered funds and investment advisers to adopt written policies and procedures covering safeguards that protect customer records and information.

- Currently, there are no SEC rules that require broker-dealers, registered funds, investment advisers or transfer agents to have policies and procedures for responding to data breach incidents or to notify customers of those breaches.[2]
- The safeguards rule does not currently apply to transfer agents.

Another provision of Regulation S-P, Rule 248.30(b) (the "disposal rule"), which applies to transfer agents registered with the SEC and entities covered by the safeguards rule, requires proper disposal of "consumer report information."

---

[1] 17 C.F.R. § 248.1 *et seq*.

[2] The Release acknowledges that all states have laws that require notification to state residents of data breaches, but these state laws "are not consistent and exclude some entities from certain requirements." Accordingly, the Proposals would establish "a Federal minimum standard for providing notification to all customers . . . affected by a data breach (regardless of state residency) and providing consistent disclosure of important information to help affected customers respond."

Required Response Programs for Unauthorized Access to or Use of Customer Information

The Proposals would amend the safeguards rule to require that broker-dealers,[3] registered funds and investment advisers ("covered institutions") have safeguards policies and procedures that include a response program for unauthorized access to or use of customer information. The Proposals also would amend Regulation S-P's safeguards rule to require that transfer agents (also, "covered institutions") have safeguards policies and procedures, including a response program.

- The Release clarifies that the provisions of Regulation S-P relating to safeguarding apply directly to investment advisers that manage solely private funds, even though such advisers' clients are the funds, not the natural-person investors in the funds. Although many private funds themselves would continue to fall under the Federal Trade Commission's implementation of the GLBA (which is similar to Regulation S-P), the Proposals would implement the same provisions of the GLBA through Regulation S-P and would regulate all customer and consumer information that a covered institution possesses "regardless of whether such information pertains to individuals with whom the covered institution has a customer relationship."

Specifically, the Proposals would require covered institutions' safeguards policies and procedures to include a "response program reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including customer notification procedures."

The 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 (an "incident") 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"[4] was, or is reasonably likely to have been, accessed or used without authorization, unless the covered institution reasonably investigates the incident and determines 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."[5]

The Proposals would thus establish a rebuttable presumption of notice (*i.e.*, a covered institution would not be required to provide the notification if it determines that the sensitive customer information was not, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience).

---

[3] The Proposals would not affect the Regulation S-P treatment of so-called "notice-registered broker-dealers," which are futures commission merchants and introducing brokers registered with the CFTC that are permitted, pursuant to Section 15(b)(11) of the Exchange Act, to register as broker-dealers by filing a notice with the SEC for the limited purpose of effecting transactions in security futures products.

[4] The Proposals would define "sensitive customer information" 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 proposed definition provides examples of sensitive customer information, including a Social Security number, an official state or government issued driver's license or identification number, an alien registration number, a government passport number and an employer or taxpayer identification number.

[5] The Proposals would define "substantial harm or inconvenience" as personal injury, financial loss, expenditure of effort or loss of time that is more than trivial, and provides examples, including theft, fraud, impersonation, and impaired eligibility for credit.

Notably, the Proposals would cover a particularly broad and relatively unique class of "sensitive customer information" including any "unique electronic identification number, address, or routing code" and certain authenticating information, such as an individual's date of birth, place of birth, mother's maiden name, or partial Social Security number, when present in combination with a customer's name, online user name or individual account number.

Service Providers and Response Programs. The Proposals would amend the safeguards rule to require that a covered institution's incident response program has written policies and procedures that address the risk of harm posed by security compromises at its "service providers."[6] Therefore, a response program would be required to include written policies and procedures that require each covered institution to have a written contract with each of its services providers.

- The mandated contract must require the service provider to take appropriate measures designed to protect against incidents, including notification to the covered institution within 48 hours after the service provider becomes aware of any breach in security resulting in unauthorized access to a customer information system maintained by the service provider.

Contents of Notice to Affected Individuals. As described above, the Proposals would require a covered institution to provide notice to individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization, although the Proposals would not require the provision of credit monitoring.[7] The Proposals would require the notice:

- To be clear and conspicuous and transmitted by a means designed to ensure that each affected individual can reasonably be expected to receive actual notice in writing;
- To be provided as soon as practicable but within no more than 30 days after the covered institution becomes aware that unauthorized access to or use of sensitive customer information has occurred or is reasonably likely to have occurred, unless the Attorney General of the United States informs the covered institution in writing that the required notice poses a substantial risk to national security;[8]
- To contain or include the following:
    - A description of the incident in general terms and the type of sensitive customer information that was or is reasonably believed to have been accessed or used without authorization;
    - A description of what has been done to protect the sensitive customer information from further unauthorized access or use;
    - If the information is reasonably possible to determine at the time the notice is provided, any of the following (i) the date of the incident, (ii) the estimated date of the incident and (iii) the date range within which the incident occurred;

[6] The Proposals would define "service provider" as 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.

[7] As noted above, Proposals would not require a notice, if the Covered Institution reasonably investigates the incident and determines 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.

[8] The Proposals would provide, if the Attorney General provides such a notice, that a covered institution may delay notice for a period specified by the Attorney General but not longer than 15 days (the notice may be delayed for an additional period of up to 15 days if the Attorney General determines that the notice continues to pose a substantial risk to national security).

- Contact information that would permit an affected individual to contact the covered institution with questions about the incident, including (i) a telephone number (which should be a toll-free number, if available), (ii) an email address or equivalent method or means of communication, (iii) a postal address and (iv) the name of a specific office to contact for further information and assistance;

- If the affected individual has an account with the covered institution, a recommendation that the customer review account statements and immediately report any suspicious activity;

- An explanation of what a fraud alert is and how an individual may place a fraud alert in the affected individual's credit reports to put the individual's creditors on notice that the individual may be a victim of fraud, including identity theft;

- A recommendation that the affected individual periodically obtain credit reports from each nationwide credit reporting company and have information relating to fraudulent transactions deleted;

- An explanation of how the affected individual may obtain a credit report free of charge; and

- Information about the availability of online guidance from the Federal Trade Commission (the "FTC") and usa.gov regarding steps an individual can take to protect against identity theft, a statement encouraging the individual to report any incidents of identity theft to the FTC and the FTC's website address at which individuals may obtain government information about identity theft and report suspected incidents of identity theft.

Service Providers Used for Notices. The Proposals would permit a covered institution to enter into a written agreement with a service provider to provide required notices to affected individuals. However, the covered institution would remain responsible for any failure to provide a notice that the Proposals would require.

Aligning Definitions Under the Safeguards Rule and the Disposal Rule

Currently, Regulation S-P's safeguards rule mandates written policies and procedures to protect "customer records and information," which is not defined in Regulation S-P. Regulation S-P's disposal rule requires every covered institution to properly dispose of "consumer report information," a different term, which Regulation S-P defines.

To better align the information protected by both rules, the Proposals would amend Rule 248.30 by (i) replacing the term "customer records and information" in the safeguards rule with a newly defined term "customer information" and (ii) adding customer information to the coverage of the disposal rule. Thus, the Proposals would make "customer information" the relevant term under both rules, which would be defined as follows:

- For any covered institution, except any transfer agent, any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic or other form, that is handled or maintained by the covered institution or on its behalf; and

- For any transfer agent, any record containing nonpublic personal information 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 handled or maintained by the transfer agent or on its behalf.

The Release explains that the different definitions arise from the fact that transfer agents typically do not have consumers or customers for the purposes of Regulation S-P. Transfer agents' clients are usually not individuals but, instead, the issuers in which the individual securityholders invest. Nonetheless, underscoring their access to nonpublic personal

information, the Release states, transfer agents "maintain extensive securityholder records in connection with performing various processing, recordkeeping, and other services on behalf of their issuer clients."

Disposal Rule Written Procedures

The Proposals would amend the disposal rule to require covered institutions to adopt and implement written policies and procedures under the disposal rule that address the proper disposal of consumer information and customer information according to a standard of taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal (*i.e.*, the same standard under the existing disposal rule).

Exception from the Annual Notice Delivery Requirement

In the 2015 Fixing America's Surface Transportation Act, Congress amended the GLBA by adding a new section containing an exception to the annual notice delivery requirements for a financial institution that meets certain requirements. As described below, the Release would amend Regulation S-P's annual notice provision to include the exception.

In general, Regulation S-P requires broker-dealers, registered funds and investment advisers ("financial institutions") to provide their customers (i) an annual notice of their privacy policies and practices and (ii) subject to certain exceptions,[9] an opportunity to opt out before these entities share nonpublic personal information with unaffiliated third parties.

Section 248.5 of Regulation S-P prescribes the requirements for an annual privacy notice, including delivery. The Proposals would add a new paragraph (e) to this section to provide an exception the annual notice requirement. To qualify for the new exception, financial institutions would be required to satisfy two conditions:

1. The financial institution must share nonpublic personal information only in accordance with the pre-existing Regulation S-P exceptions to the general requirement of providing customers an opportunity to opt out of the financial institution's information sharing with unaffiliated third parties;[10] and

2. The financial institution relying on the new exception cannot have changed its policies and practices with regard to disclosing nonpublic personal information from those that were disclosed in the most recent annual notice sent to customers.

Proposed paragraph 248.5(e) also specifies when a financial institution would be required to resume delivering annual privacy notices if the financial institution no longer satisfies the two conditions above.

Recordkeeping

The Proposals would require covered institutions to make and maintain written records documenting compliance with the requirements of the amended safeguards rule and disposal rule. The Proposal would amend Rules 31a-1(b) and 31a-2(a) under the 1940 Act, Rule 204-2 under the Advisers Act, Rule 17a-4 under the Exchange Act for broker-dealers and Rule 17Ad-7 under the Exchange Act for transfer agents. In each case, the Proposals would require the covered institution to maintain written records documenting the covered institution's compliance with the requirements set forth in the safeguards rule and the disposal rule, as amended.

---

[9] *See* Regulation S-P §§ 248.13, 248.14 and 248.15. In general, these sections provide that a financial institution is not required to provide customers the opportunity to opt out if it shares nonpublic personal information with unaffiliated third parties (i) pursuant to a joint marketing arrangement with third party service providers, (ii) in connection with maintaining and servicing customer accounts and effecting certain transactions and (iii) in situations related to protecting against fraud, complying with certain legal and regulatory requirements and required consumer reporting.

[10] *See id*.

Comment Deadline

Comments on the Proposals should be received by the SEC no later than 60 days following the publication of the Release in the *Federal Register*. As of the date of this Alert, the Release has not been published therein.

Interactions with 2022 Investment Management Cybersecurity Proposals

On the same day as the Release, the SEC issued separate releases proposing updating and expanding Regulation Systems Compliance and Integrity (Regulation SCI) (here) and cybersecurity risk management requirements for various entities (including broker-dealers and transfer agents) to address their cybersecurity risks (here).

The SEC recognized the interactions among the three March 15, 2023 releases and the SEC's 2022 release titled, "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies" (the "Investment Management Cybersecurity Release") (described in this February 2022 Ropes & Gray Alert).

Accordingly, on March 15, 2023, the SEC issued a release reopening the comment period on the Investment Management Cybersecurity Release, with comments due no later than 60 days following the date of publication of the release announcing the reopening in the *Federal Register*.

* * *

If you would like to learn more about the issues in this Alert, please contact your usual Ropes & Gray attorney contacts.