May 20, 2024

SEC Adopts Rule Amendments to Regulation S-P to Enhance the Protection of Customer Information

Rule Amendments Will Require Implementation of Incident Response Programs with Broader Notification Requirements, Will Expand the Scope of Safeguards and Disposal Rules, and Will Require Enhanced Recordkeeping

SUMMARY

On May 16, 2024, the Securities and Exchange Commission ("SEC") significantly expanded its consumer information protection framework by adopting rule amendments (the "Final Amendments") to Regulation S-P, which governs the protection of consumer financial information held by broker-dealers, investment companies, registered investment advisers and now transfer agents ("S-P entities"). The SEC originally released its proposed amendments (the "Proposed Amendments") on March 15, 2023, which are discussed in our earlier Memorandum to Clients.[1] The Final Amendments generally follow the Proposed Amendments, with a few changes discussed below, in response to comments received.

Regulation S-P generally requires covered entities to create and maintain written policies and procedures regarding the protection of customer information (the "safeguards rule") and properly dispose of customer information in a manner that protects against the unauthorized access or use of that information (the "disposal rule").[2]

As set forth more specifically below, under the Final Amendments:

- S-P entities will be required to implement incident response programs that include a broad, presumptive notification requirement that applies to instances where sensitive customer information was or was reasonably likely to have been compromised, and to make such notice as soon as practicable but not later than 30 days after an entity becomes aware that an incident has

occurred or is likely to have occurred. The presumption that notification is required may only be overcome where, following a reasonable investigation, it is determined that there is no risk for substantial harm or inconvenience to the affected customers. The Final Amendments also allow for a delay in notification only where there is a substantial risk to national security or public safety as determined by the Attorney General.

- The scope of Regulation S-P, including the safeguards and disposal rules, is expanded to cover all transfer agents, as well as a broader array of customer information, such as customer information received from another financial institution.
- Regulation S-P will require more extensive recordkeeping with respect to customer information and cybersecurity programs.

The Final Amendments will become effective 30 days following publication of the adopting release in the Federal Register. Larger S-P entities will have an 18-month compliance period after the date of publication whereas smaller entities will have a 24-month compliance period.

BACKGROUND

The amendments to Regulation S-P are part of a broader effort by the SEC and other regulatory authorities to expand the scope of their rules and regulations with respect to entities' response to cybersecurity incidents and the collection and protection of customer information. For example:

- In July 2023, the SEC adopted new disclosure rules for public companies on cybersecurity risk management, strategy, governance, and incident disclosure, as discussed in our earlier Memorandum to Clients.[3]
- In October 2023, the SEC filed a complaint against SolarWinds Corporation and its Chief Information Security Officer alleging material misstatements and omissions regarding the company's cybersecurity, as detailed in our earlier Memorandum to Clients.[4] That same month, the Federal Trade Commission adopted amendments to the safeguards rule that require reporting by non-bank financial institutions of certain data breaches.[5]
- Most recently, on May 13, 2024, the SEC and U.S. Department of the Treasury's Financial Crimes Enforcement Network issued a joint notice of proposed rulemaking regarding Customer Identification Programs.[6]

In line with these initiatives, and recognizing the technological advancements and heightened risks that have developed since Regulation S-P was first adopted in the early 2000s, the amendments to Regulation S-P as proposed and adopted are designed to "enhance the protection of customer information" held by broker-dealers, investment companies, registered investment advisers, and transfer agents.[7]

OVERVIEW OF THE FINAL AMENDMENTS

A. INCIDENT RESPONSE PROGRAM

Under the Final Amendments, S-P entities must establish an incident response program that is "reasonably designed to detect, respond to, and recover from both unauthorized access to and unauthorized use of customer information"[8] and that includes notification procedures designed to inform potentially affected

individuals. These programs are intended to ensure a "consistent and systematic response to customer information security incidents and help avoid inadequate responses based on a covered institution's initial impressions of the scope of the information involved in the compromise."[9] The response program must include procedures 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;[10]
- "Take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information;[11]
- "Notify each affected individual whose "sensitive customer information" (as defined below) 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;[12] and
- "Establish, maintain, and enforce written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers."[13]

The scope of the incident response program covers all customer information and is intentionally broader than that of the notification requirement, which only covers "sensitive customer information," as discussed below.[14]

1. Notification Requirement

Under the Final Amendments, S-P entities will be required to notify consumers of the unauthorized access or use of "sensitive customer information," defined 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."[15] Specifically, S-P entities must:

- "[N]otify each affected 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 of the incident, 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."[16]
- Provide such notification "as soon as practicable, but not later than 30 days" after an entity "becomes aware" that an incident has occurred or is likely to have occurred, and provide the notification in a "clear and conspicuous" manner.[17]
- Maintain records of any investigation and related determinations; this requirement applies to all S-P entities except certain funding portals.[18]
- Maintain procedures designed to revisit notification determinations where appropriate in light of new facts or developments.[19]

Importantly, the presumption that notice is required may be rebutted only with evidence that, following a reasonable investigation, there is a determination 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."[20] As noted below, "substantial harm or inconvenience" is undefined in the Final Amendments, and the extent to which S-P entities' investigations were "reasonable" will turn on a facts-and-circumstances analysis of the unauthorized access or use.[21]

2. Service Providers

The Final Amendments include requirements with respect to oversight of service providers, defined 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."[22] Specifically, under the Final Amendments, S-P entities must:

- Establish written policies and procedures that provide oversight measures for service providers and ensure that service providers take steps to protect against unauthorized access to or use of customer information and 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[23] resulting in unauthorized access to a customer information system maintained by the service provider.[24]
- Initiate their own incident response program when notified by a service provider of a breach in security at the service provider.[25]
- Ensure that proper notice is provided to affected customers.[26]

3. Proposed Amendments Versus the Final Amendments

The Final Amendments meaningfully differ from the Proposed Amendments in the following respects:

- The Final Amendments clarify instances where notification would not be required, such as where "a specific individual's sensitive customer information that resides in the customer information system was not accessed or used without authorization."
- With respect to notice requirements for customers across multiple institutions, the Final Amendments require notification only where the unauthorized access or use of sensitive customer information occurred at the entity itself or one of its service providers. Additionally, where two entities would otherwise be required to provide notice to the same affected customers, such notice need only come from one entity to satisfy the obligations of both entities.
- The Final Amendments do not include any definition of "substantial harm or inconvenience." As set forth in the Adopting Release, the meaning of "substantial harm or inconvenience" will depend on the facts and circumstances of the relevant incident.
- Under the Final Amendments, there is no requirement to include in the notice any description of what actions have been taken to mitigate the risk of future unauthorized access or use.
- The "law enforcement exception" to the notice requirements is broadened in the Final Amendments in terms of scope and timing, including by accounting for risks to public safety as well as to national security, and by allowing for additional delays of up to 30 days and, in "extraordinary circumstances," of up to an additional 60 days where the Attorney General determines that a substantial risk to national security or public safety remains. Further delays may be granted by SEC exemptive order or other action. Where a delay is granted, the Final Amendments require the Attorney General to provide this determination in writing to the SEC and

not to the relevant entity, as previously proposed. Through interagency communications, the Attorney General will inform the Department of Justice of any grant of delay and the Department of Justice will be responsible for sharing that information with the relevant entity.

- The Final Amendments eliminate the proposed requirement that S-P entities enter into written agreements with service providers to take appropriate measures to protect customer information.

B. BROADENED SCOPE OF SAFEGUARDS AND DISPOSAL RULES

The Final Amendments broaden the scope of the safeguards and disposal rules to include customer information received by S-P entities from other financial institutions.[27] Specifically, the Final Amendments:

- "Adopt a new definition of 'customer information' defining the scope of information covered by both the safeguards and disposal rules." Specifically, "customer information" is defined as "any record containing nonpublic personal information as defined in section 248.3(t) about a customer of a financial institution, whether in paper, electronic, or other form."[28] "These amendments provide greater specificity regarding what constitutes customer information that must be protected under the safeguards rule. The Final Amendments 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."[29]
- "Provide that customer information protected under both the safeguards and disposal rules includes both customer information in the possession of a covered institution as well as customer information handled or maintained on its behalf."[30]
- "Provide that both customer and consumer information include information that pertains to individuals with whom the covered institution has a customer relationship, as well as to customers of other financial institutions where such information has been provided to the covered institution."[31]

The Final Amendments expand the scope of the safeguards and disposal rules to include all transfer agents regardless of whether they are registered with another regulatory agency that is not the SEC.[32] The Final Amendments also provide a specific definition of "customer" that is applicable only to transfer agents, namely "any natural person who is a securityholder of an issuer for which the transfer agent acts or has acted as a transfer agent."[33]

The Final Amendments maintain the existing exceptions under the safeguards rule and disposal rule for notice-registered broker-dealers.[34]

C. RECORDKEEPING AND ANNUAL NOTICE AMENDMENTS TO SAFEGUARDS AND DISPOSAL RULES

Finally, the Final Amendments include additional recordkeeping requirements regarding compliance with the safeguards and disposal rules.[35] While they largely mirror the Proposed Amendments, the Final Amendments include additional information regarding the scope of certain of the requirements with respect to different S-P entities.

The recordkeeping requirements in the Final Amendments generally cover the following types of records:

- "Written policies and procedures required to be adopted and implemented pursuant to final rule 248.30(a)(1), which requires policies and procedures to address administrative, technical, and physical safeguards for the protection of customer information;
- "Written documentation of any detected unauthorized access to or use of customer information, as well as any response to, and recovery from such unauthorized access to or use of customer information required by final rule 248.30(a)(3);
- "Written documentation of any investigation and determination made regarding whether notification to affected individuals is required pursuant to final rule 248.30(a)(4), including the basis for any determination made, any written documentation from the Attorney General related to a delay in notice, as well as a copy of any notice transmitted following such determination;
- "Written policies and procedures required to be adopted and implemented pursuant to final rule 248.30(a)(5)(i), which requires policies and procedures to oversee, monitor, and conduct due diligence on service providers, including to ensure that the covered institution is notified when a breach in security has occurred at the service provider;
- "Written documentation of any contract or agreement between a covered institution and a service provider entered into pursuant to final rule 248.30(a)(5)(ii); and
- "Written policies and procedures required to be adopted and implemented pursuant to final rule 248.30(b)(2), which requires policies and procedures to address the proper disposal of consumer information and customer information."[36]

The Final Amendments adopt an exception to the annual privacy notice requirement provided that certain conditions are met. Namely, 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."[37]

IMPLICATIONS

As previewed in our Memorandum to Clients on the Proposed Rules, the new notice requirements may be challenging to meet in certain circumstances. For instance, the prescriptive 30-day deadline for providing notice to affected consumers may be challenging to meet given that it can be a complex exercise to assess the nature and extent of a data breach and any consumer information that has been compromised, including assessing whether customer information may be used in a manner that would result in substantial harm or inconvenience. Moreover, the notice provision as adopted is significantly broader than analogous notice requirements under various state laws and other regulatory regimes, which adds to the complexity that S-P entities may face in responding to a data breach.

Finally, these Regulation S-P amendments are the first to have been adopted in a series of proposed amendments to the SEC's cybersecurity regulatory framework, including amendments to Regulation SCI and proposed cybersecurity rules for market entities.[38] It remains to be seen what effect the adoption of these amendments will have on the future adoption of the other proposed changes.

* * *

Copyright © Sullivan & Cromwell LLP 2024

ENDNOTES

1 *See* our publication, dated March 22, 2023, *available at* https://www.sullcrom.com/insights/memo/2023/March/SEC-Proposes-New-Cybersecurity-Rule-and-Regulation-S-P-and-SCI-Amendments.

2 Fact Sheet, Final Rules: Enhancements to Regulation S-P (May 16, 2024), https://www.sec.gov/files/34-100155-fact-sheet.pdf.

3 *See* our publication, dated July 28, 2023, *available at https://www.sullcrom.com/SullivanCromwell/_Assets/PDFs/Memos/sc-publication-sec-adopts-new-cybersecurity-disclosure-rules-public-companies.pdf.*

4 *See* our publication, dated November 6, 2023, *available at https://www.sullcrom.com/insights/memo/2023/November/SEC-Brings-Novel-Cybersecurity-Charges-Against-SolarWinds-and-Its-CISO.*

5 *See* our publication, dated November 1, 2023, *available at* https://www.sullcrom.com/insights/memo/2023/November/FTC-Requires-Non-Bank-Financial-Institutions-to-Report-Certain-Data-Breaches.

6 *See* 31 C.F.R. 1032, 17 C.F.R. 275.

7 Press Release, Securities and Exchange Commission, SEC Proposes Changes to Reg S-P to Enhance Protection of Customer Information (Mar. 15, 2023), https://www.sec.gov/news/press-release/2023-51; Press Release, Securities and Exchange Commission, SEC Adopts Rule Amendments to Regulation S-P to Enhance Protection of Customer Information (May 16, 2024), https://www.sec.gov/news/press-release/2024-58.

8 Adopting Release, at 16.

9 Adopting Release, at 17.

10 The SEC did not receive any comments directed toward the assessment provisions of the incident response program and, as such, the amendments were adopted as proposed. Adopting Release, at 21.

11 The SEC did not receive any comments directed toward the containment and control provisions of the incident response program and, as such, the amendments were adopted as proposed. Adopting Release, at 22.

12 Adopting Release, at 18

13 Adopting Release, at 18.

14 Adopting Release, at 20.

15 Adopting Release, at 39-40. The SEC acknowledged commenters' suggestions that the final rule include an exception for encrypted information but concluded that the text of the rule already addresses encrypted information and S-P entities can consider the extent to which information was encrypted when determining the risk underlying any compromise of such information. Adopting Release, at 44.

16 Adopting Release, at 24.

17 Id.

18 Adopting Release, at 27.

19 Adopting Release, at 36.

ENDNOTES (CONTINUED)

20 Adopting Release, at 26-27.

21 Adopting Release, at 26.

22 Adopting Release, at 70.

23 The Final Amendments expanded the timing of the notification requirement for service providers to allow a 72-hour period of time as opposed to the proposed 48-hour period.

24 Adopting Release, at 69.

25 Id.

26 Adopting Release, at 70.

27 Adopting Release, at 92.

28 Adopting Release, at 94.

29 While substantively the same as proposed, the definition of consumer information appearing in the final amendments was reorganized to contain all the requirements for customer information and consumer information that were previously provided in a separate paragraph defining scope. Adopting Release, at 96.

30 While substantively the same as proposed, the restructured definition reflects that both rules are applicable regardless of whether the information derives from a customer of the institution or another institution where such information was shared. Adopting Release, at 98.

31 Adopting Release, at 93.

32 Adopting Release, at 100-101.

33 While the definition was adopted generally as it was originally proposed, the SEC clarified the limited applicability of this definition in the Adopting Release, noting that it "applies for purposes of section 248, meaning that it does not apply to any other rules, including those specific to transfer agents codified at 17 C.F.R. 240.17Ad. Adopting Release, at 111.

34 The SEC received no comments regarding the treatment of notice-registered broker-dealers and, as such, the amendments were adopted as proposed. Adopting Release, at 119-121.

35 Adopting Release, at 121-122. *See* Table 1: Recordkeeping Requirements, Adopting Release, at 122-123.

36 Adopting Release, at 124-125.

37 Adopting Release, at 127.

38 Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, SEC Release Nos. 33-11028; 34-94197; IA-5956; IC-34497 (Feb. 9, 2022) (the "Release"); SEC Fact Sheet: Cybersecurity Risk Management (Feb. 9, 2022), available at https://www.sec.gov/files/33-11028-fact-sheet.pdf; Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major SecurityBased Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, SecurityBased Swap Dealers, and Transfer Agents, SEC Release No. 34-97142 (Mar. 15, 2023) (the "Rule 10 Release"), at 1; Press Release, Securities and Exchange Commission, SEC Proposes New Requirements to Address Cybersecurity Risks to the U.S. Securities Markets (Mar. 15, 2023), https://www.sec.gov/news/press-release/2023-52.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 900 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.