WILMERHALE

# *SEC Modernizes Data Protection Rules for Safeguarding Customer Information*

JUNE 10, 2024

Last month, the Securities and Exchange Commission (the SEC or the Commission) unanimously voted to adopt amendments to Regulation S-P (Reg S-P), which is the SEC's regulation governing the treatment and safeguarding of customers' nonpublic personal information.[1] The amendments apply to broker-dealers, investment companies, registered investment advisers and transfer agents registered with the SEC or with another appropriate regulatory agency (collectively, covered institutions) and cover three main areas, discussed in more detail below: (1) a new requirement to design an "incident response program" to detect, contain and control unauthorized access to or use of customer information; (2) an expanded scope of information and entities covered by Reg S-P's safeguarding and disposal requirements; and (3) new recordkeeping requirements for covered institutions. Covered institutions will be subject to the new rules either 18 months after publication in the Federal Register, if the covered institution is a "larger entity," or 24 months after publication, if the covered institution is a "smaller entity."[2] The amendments were published in the Federal Register on June 3, 2024.

## *Background*

Reg S-P governs the treatment of certain types of information about "consumers" by covered institutions. For purposes of Reg S-P, a consumer is an individual who obtains or has obtained a

[1] Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, 89 Fed. Reg. 47688 (Jun. 3, 2024), available at https://www.federalregister.gov/documents/2024/06/03/2024-11116/regulation-s-p-privacy-of-consumer-financial-information-and-safeguarding-customer-information#citation-411-p47725 (Adopting Release).

[2] The definition of "larger entity" varies by entity type. For investment companies (together with other investment companies in the same group of related investment companies), there must be "net assets of $1 billion or more as of the end of the most recent fiscal year." A registered investment adviser is a "larger entity" if it has "$1.5 billion or more in assets under management." Broker-dealers and transfer agents are "larger entities" if they "are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act."

financial product or service from certain financial institutions that is to be used primarily for personal, family or household purposes, or that individual's legal representative.[3] In addition to its privacy disclosure and "opt-out" rules regarding the use of nonpublic personal information, Reg S-P requires broker-dealers, investment companies and registered investment advisers to adopt written policies and procedures to safeguard certain customer records and information (the Safeguards Rule). Reg S-P also requires proper disposal of consumer report information by transfer agents registered with the Commission, broker-dealers, investment companies and registered investment advisers (the Disposal Rule).

Reg S-P was initially adopted in 2000 under the Gramm-Leach-Bliley Act. In the years since, the Commission and SEC staff have recognized a need to "modernize" Reg S-P to address the increased risk of harm to consumers due to the evolving uses of technology and the increased risks of cybersecurity breaches. In a statement accompanying the final rules, Chair Gary Gensler explained that over "the last 24 years, the nature, scale, and impact of data breaches has transformed substantially."[4] He also noted that complaints about identity theft have more than doubled in just the four years from 2018 to 2022, according to the FBI's Internet Crime Complaint Center.[5] Commissioner Mark Uyeda echoed the sentiment that updates to Reg S-P were overdue, noting that, at the time Reg S-P was adopted, "pagers were still in vogue, and smartphones in their current incarnation did not yet exist."[6]

## *New Incident Response Program Requirement*

New regulation 17 C.F.R. § 248.30(a)(3), (4) and (5) will require covered institutions to implement an incident response program as part of their written procedures if there is a data breach involving certain customer information. The program must address the following areas: (1) assessment, containment and control; (2) notice; and (3) service providers.

***Assessment, Containment and Control.*** Covered institutions must update their written procedures to include a process for assessing the nature and scope of any incident involving unauthorized access to or use of customer information. As part of this process, firms must identify the customer information systems and types of customer information that may have been accessed or used without authorization and take appropriate steps to contain and control the incident to prevent further unauthorized access or use. In the Adopting Release, the Commission explained

---

[3] 17 C.F.R. § 248.3(g).

[4] Chair Gary Gensler, "Statement on Amendments to Regulation S-P," available at https://www.sec.gov/news/statement/gensler-reg-s-p-05162024.

[5] Federal Bureau of Investigation, "Internet Crime Report – 2022," available at https://www.ic3.gov/media/pdf/annualreport/2022_ic3report.pdf.

[6] Commissioner Mark T. Uyeda, "Statement on the Amendments to Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information," available at https://www.sec.gov/news/statement/uyeda-statement-reg-s-p-051624.

that strategies for containing and controlling an incident will vary depending on the type of incident but include, for example, "isolating compromised systems or enhancing the monitoring of intruder activities, searching for additional compromised systems, changing system administrator passwords, rotating private keys, and changing or disabling default user accounts and passwords, among other interventions."[7]

***Notification Requirement to Affected Individuals.*** As part of their incident response programs and written policies and procedures, covered institutions also must notify each affected individual whose "sensitive customer information" was, or was reasonably likely to have been, accessed or used without authorization. Notification, however, is not required if 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. Notably, the final amendments reflect a presumption of notification. Therefore, if a covered institution conducts an investigation and the results are inconclusive, notification is required. Similarly, a covered institution must notify all individuals whose sensitive customer information resides in the customer information system that was, or was reasonably likely to have been, accessed without authorization unless the covered institution reasonably determines that a specific individual's sensitive customer information was not accessed or used without authorization.

As proposed, the final rules define "sensitive customer information" to 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 substantial harm or inconvenience to an individual identified with the information."[8] The Adopting Release acknowledges this definition of "sensitive customer information" is broader than the definition used in some states because it includes identifying information that, in combination with authenticating information (such as a partial Social Security number, access code or mother's maiden name), could "create a substantial risk of harm or inconvenience to the customer because [such information] may be widely used for authentication purposes."[9] There is also no exception for encrypted information, though a covered institution may consider encryption as a factor in determining whether the compromise of customer information could create a reasonably likely harm risk to an individual identified with the information.

The Commission initially proposed to define the phrase "substantial harm or inconvenience" in the definition of "sensitive customer information" to mean all personal injuries, as well as instances of financial loss, expenditure of effort or loss of time when they are "more than trivial." The proposal also included a non-exhaustive list of examples of harms or inconveniences. The final amendments do not include the proposed definition of "substantial harm or inconvenience" or the list of examples, but the Commission did suggest that the list of harms in the proposal may be a "useful

---

[7] Adopting Release, 89 Fed. Reg. at 47694-95.

[8] *Id.* at 47758, 47789.

[9] *Id.* at 47698.

starting point" for an analysis by personnel at the covered institution.[10] In addition, to provide a little more clarity, the rule includes some examples of "sensitive customer information."

With respect to timing, a covered institution must provide a notice "as soon as practicable, but not later than 30 days, after becoming aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred." Notice may be delayed if the US Attorney General determines that the notice required poses a substantial risk to national security or public safety and notifies the Commission of its determination in writing.

***Third-Party Service Providers.*** As noted above, an incident response program must include policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers. Unlike in the proposal, the final rules do not require covered institutions to enter into written contracts with service providers to take certain appropriate measures. Instead, covered institutions have greater flexibility, so long as their policies and procedures are reasonably designed to 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. While there is no formal requirement that a covered institution contractually bind service providers to take certain data security measures, the Commission asks covered institutions in a footnote to "consider whether a written contract that memorializes the expectations of both covered institutions and their service providers is appropriate."[11]

## *Expanded Scope of Safeguards and Disposal Rules*

The amendments also change the scope of the Safeguards Rule and the Disposal Rule in two important respects. First, the amendments redefine and expand the type of information to which the Safeguards Rule and the Disposal Rule apply.[12] Currently, the Disposal Rule applies to "consumer report information," while the Safeguards Rule requires policies and procedures that protect "customer records and information." The amendments broaden these requirements, applying the Safeguards Rule and the Disposal Rule to all "customer information" that a covered institution collects about its own customers and nonpublic personal information it receives from another financial institution about customers of that financial institution. The term "customer information" is a new defined term. For covered institutions other than transfer agents, "customer information" 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

[10] *Id.* at 47701.

[11] *Id.* at 47708 n. 233.

[12] 17 C.F.R. § 248.30(a)(1), (b).

possession of a covered institution or that is handled or maintained by the covered institution or on its behalf."[13]

Second, the amendments expand the scope of entities covered by the rules. The Safeguards Rule currently does not apply to transfer agents, and the Disposal Rule applies to transfer agents only if they are registered with the Commission. The amendments extend the requirements of the Safeguards Rule and the Disposal Rule to any transfer agent registered with the Commission or another appropriate regulatory agency.

In addition to expanding the scope of these rules, the amendments explicitly require covered institutions, other than funding portals,[14] to make and maintain written records documenting compliance with the requirements of the Safeguards Rule and the Disposal Rule.

## *New Recordkeeping Requirements*

Finally, the amendments add recordkeeping requirements for covered institutions and exempt certain institutions from the annual privacy notice requirement.[15] Specifically, covered institutions must make and maintain (1) written policies and procedures to comply with the Safeguards Rule and the Disposal Rule; (2) written documentation of any detected unauthorized access to or use of customer information and any response to such event; (3) written documentation of any investigation and determination made regarding whether customer notification would be required with respect to such an event; and (4) written policies and procedures and contracts regarding service providers. Broker-dealers must maintain records under Exchange Act Rule 17a-4(e) for three years in an easily accessible place.

## *Conclusion*

The Commission and other regulators will expect covered institutions to update their policies and procedures ahead of the compliance date. Covered institutions should begin building an incident response program now so that they are prepared for examinations and inquiries by the compliance date.

---

[13] 17 C.F.R. § 248.30(d)(5).

[14] Under Regulation Crowdfunding, a funding portal must comply with the requirements of Reg S-P as they apply to brokers. 17 C.F.R. § 227.403(b).

[15] The amendments codify a statutory exception to the requirement to provide annual privacy notices if an institution (1) only provides nonpublic personal information to nonaffiliated third parties when an exception to third-party opt-out applies and (2) has not changed its policies and practices with regard to disclosing nonpublic personal information from its most recent disclosure sent to customers. This exception to the annual privacy notice provision was added by the 2015 Fixing America's Surface Transportation Act.

## *Contributors*


**Bruce H. Newman**
PARTNER

bruce.newman@wilmerhale.com
+1 212 230 8835

**Stephanie Nicolas**
PARTNER

stephanie.nicolas@wilmerhale.com
+1 202 663 6825

**Andre E. Owens**
PARTNER

andre.owens@wilmerhale.com
+1 202 663 6350

**Joshua Nathanson**
ASSOCIATE

joshua.nathanson@wilmerhale.com
+1 202 663 6193