Simpson Thacher

# Regulatory and Enforcement Alert

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

March 17, 2023

In a unanimous 5-0 vote earlier this week, the SEC proposed amendments to Regulation S-P ("Reg. S-P"), which the SEC initially adopted in 2000 pursuant to the Gramm-Leach-Bliley Act (the "GLBA"). The proposed amendments[1] would apply to broker-dealers, investment companies (including business development companies), registered investment advisers and transfer agents (collectively, "Covered Institutions"). If adopted, the amendments will require Covered Institutions to adopt written policies and procedures to respond to incidents of unauthorized access to or use of customer information and to provide affected customers with notification of the breach "as soon as practicable, but not later than 30 days" after becoming aware of the breach.[2] The proposal would also broaden the scope of information subject to Reg. S-P by creating the new defined term "customer information,"[3] and require Covered Institutions' contracts with service providers to include measures to protect against breaches.

Comments regarding the proposal will be due 60 days after publication of the proposal in the Federal Register. The proposed compliance date is 12 months from adoption, which is a short timeframe in light of the content of this proposal and other recent SEC rule proposals that address similar issues.

The SEC's rationale for the proposal is to bring Reg. S-P in line with the substantial technological changes that have occurred since its initial adoption and that, in turn, made it easier for Covered Institutions to maintain individuals' personal information and exacerbated the risk of unauthorized access to such information. While there is consensus for the need to modernize Reg. S-P in light of these technological changes, the Commissioners identified several questions regarding the proposal on which they seek comment. Following is a summary of some noteworthy aspects of this proposal.

- ***The proposal will create a federal minimum standard regarding Covered Institutions' practices for preventing and responding to data breaches.*** The proposing release acknowledges

[1] The SEC published full text of the *Reg S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information* proposal: as well as the *Proposed Enhancements to Regulation S-P Fact Sheet*.

[2] Proposed rule 248.30(b)(4)(iii).

[3] "Customer information" refers to a record containing "nonpublic personal information," which is already used for other components of Reg. S-P.

that all 50 states have enacted laws requiring firms to notify individuals of data breaches. Nonetheless, the SEC contends that because standards differ significantly by state, there is a need to establish a federal minimum standard[4] regarding the nature of breaches that trigger a notification requirement, a firm's duty to investigate a data breach when determining whether notice is required, and the timeline to provide notice, among other matters. The minimum notification standard proposed by Reg. S-P would require a Covered Institution to provide notice, within 30 days of learning of a breach, to individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.[5] If the Reg. S-P amendments do not preempt, or override, state laws, Covered Institutions could face challenges when state and Reg. S-P customer notification requirements do not align, resulting in duplicative notifications that, instead of providing a stronger warning to affected customers, reduce the impact of receiving notification.

- ***The proposal includes burdensome requirements related to service providers.*** Covered Institutions may engage third-party service providers to perform certain business functions ("outsourcing"), such as trading and order management and cloud computer services. These service providers routinely come into possession of sensitive customer information by nature of their services. The proposed amendments would mandate that Covered Institutions' contracts with service providers include measures designed to protect against unauthorized access to or use of Covered Institutions' customer information.[6] Negotiating such agreements with service providers would impose on Covered Institutions substantial time and cost burdens that the SEC, by its own admission, has not quantified in the Reg. S-P proposing release.

- ***Questions about overlap of the Reg. S-P proposal and other SEC proposals.*** Some of Reg. S-P's proposed provisions appear to duplicate or contradict other recent SEC rule proposals. For example, the proposed Reg. S-P amendments and the SEC's *Investment Adviser Outsourcing Proposal*[7] have different definitions of "service provider" and would impose different obligations on registered investment advisers with respect to service providers. Similarly, the Reg. S-P proposing release acknowledges that certain of its proposed revisions require different policies and procedures and impose different disclosure requirements than the SEC's *Investment Management Cybersecurity Proposal*, [8] but asserts—with little

[4] The proposal currently provides for a broader definition of "sensitive customer information" than used by at least 12 states; enacts a 30 day notification deadline which is shorter than what is currently mandated by 15 states; and 32 states do not mandate a notification deadline. These are a few of a handful of examples by which state specific privacy laws differ from each other and what is being proposed.

[5] The Covered Institution would not be required to provide notice if it 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 matter that would result in substantial harm or inconvenience. *See* Proposed rule 248.30(b)(4)(i).

[6] *See* Proposed rule 248.30(b)(5)(i).

[7] Outsourcing by Investment Advisers, IA. Rel. No. 6176 (Oct. 26, 2022).

[8] Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, IA Rel. No. 5956 (Feb. 9, 2022). On March 15, 2023, the SEC issued a release reopening the comment period for the *Investment Management*

analysis—that registered investment advisers could avoid duplicative compliance efforts if both of these proposals were adopted. These potentially duplicative and conflicting obligations between the Reg. S-P proposal and proposed SEC rules would likely exacerbate the costs of complying with the proposed amendments to Reg. S-P.

- ***Exception to Reg. S-P's annual notice requirement in certain circumstances***. Consistent with the GLBA, Reg. S-P currently requires broker-dealers, investment companies and registered investment advisers to provide customers with annual notices regarding their privacy policies. Legislative action in 2015 provided an exception to the annual notice delivery requirements in certain circumstances. The proposed amendments to Reg. S-P would implement this annual notice exception, provided that the Covered Institution only shares non-public information with unaffiliated third parties in certain limited circumstances and has not changed its policies and practices with regard to disclosing non-public personal information in the past year. This change could provide certain entities with welcome-if-limited relief from the otherwise substantial existing and proposed obligations under Reg. S-P.

## Conclusion

The SEC's proposed amendments are intended to modernize Reg. S-P. However, if the proposed Reg. S-P amendments are adopted in their current form, they may have significant negative implications for Covered Institutions and their service providers. Covered Institutions will likely incur significant costs negotiating with service providers to include the required minimum standards regarding incident response and notification. This requirement, combined with the costs associated with the Investment Adviser Outsourcing Proposal and multiple other regulatory initiatives aimed at investment advisers, will likely have a disparate impact on smaller or newer Covered Institutions and may outweigh the intended benefits of increased information protection.

*Cybersecurity Proposal*, for 60 days from the date the release is published in the Federal Register, in light of its substantial overlap with the proposed Reg. S-P amendments. *See* IA Rel. No. 6263 (March 15, 2023).

For further information regarding this Alert, please contact one of the following members of the Firm's Funds Regulatory and Investigations Practice.

WASHINGTON, D.C.

**David W. Blass**
+1-202-636-5863
david.blass@stblaw.com

**David Nicolardi**
+1-202-636-5571
david.nicolardi@stblaw.com

NEW YORK CITY

**Meredith J. Abrams**
+1-212-455-3095
meredith.abrams@stblaw.com

**Manny M. Halberstam**
+1-212-455-2388
manny.halberstam@stblaw.com

**Jeffrey Caretsky**
+1-212-455-7764
jeffrey.caretsky@stblaw.com

**William LeBas**
+1-212-455-2617
william.lebas@stblaw.com

HOUSTON

**Minzala G. Mvula**
+1-713-821-5617
minzala.mvula@stblaw.com