# CYBERSECURITY LAW ALERT

May 8, 2023

By: Steven J. Kuperschmid, Esq.
Nicole E. Osborne, Esq.
Samantha M. Guido, Esq.

RUSKIN MOSCOU FALTISCHEK P.C.
*Smart Counsel. Straight Talk.*

## THE SEC PROPOSES ENHANCEMENTS TO REGULATION S-P

On March 15, 2023, the Securities and Exchange Commission ("SEC") proposed amendments to Regulation S-P which would require broker-dealers, investment companies, registered investment advisers, and transfer agents ("Covered Institutions") to notify individuals affected by certain types of data breaches (the "Proposed Rule").

Regulation S-P, which was initially adopted by the SEC in July 2000, requires registered broker-dealers, investment companies, and investment advisors to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information." Regulation S-P currently requires (1) broker-dealers, investment companies, and registered investment advisers to adopt written policies and procedures to safeguard customer records and information (the "Safeguards Rule"), and (2) proper disposal of consumer report information in a manner that protects against unauthorized access to or use of such information (the "Disposal Rule").

Since the adoption of Regulation S-P in 2000, "evolving digital communications and information storage tools and other technologies have made it easier for firms to obtain, share, and maintain individuals' personal information."[1] However, the growth of technology has also lead to an increased risk of unauthorized access to or use of customer information. As SEC Chair Gary Gensler stated, "Let's be real. Over the last 24 years, the nature, scale, and impact of data breaches has transformed substantially. Complaints about identify theft have gone up threefold in just the four years from 2017 to 2021, per the FBI's Internet Crime Complaint Center."[2]

Currently, the Safeguards Rule addresses how broker-dealers, investment companies, and registered investment advisers must protect customer information against unauthorized access or use; however, it does it not require those institutions to have policies and procedures for responding to a data breach, nor does it include a requirement that the affected individual be notified of such breach. With the Proposed Rule, the SEC is seeking to fill this gap in the Federal law.

The Proposed Rule "would require covered institutions to develop, implement, and maintain written policies and procedures for an incident response program that is reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information."[3]

First, pursuant to the Proposed Rule, Covered Institutions would be required to adopt an incident response program as part of their written policies and procedures under the Safeguards Rule. The SEC proposed that a Covered Institution be required to create an incident response program that is reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information. Additionally, the SEC would require Covered Institutions to include procedures to assess the nature and scope of any such incident, and contain and control such incidents.

---

[1] *See* Release Nos. 34-97141; IA-6262; IC-34854; File No. S7-05-23. The Proposed Rule can be found at https://www.sec.gov/rules/proposed/2023/34-97141.pdf.

[2] *See https://www.sec.gov/news/statement/gensler-statement-regulation-sp-031523?utm_medium=email&utm_source=govdelivery* for Chair Gary Gensler's full statement on the Proposed Rule.

[3] *See supra* note 1.

Second, the SEC is also seeking to require Covered Institutions to notify affected individuals whose sensitive customer information was or is reasonably likely to have been accessed or used without authorization. Under the Proposed Rule, a Covered Institution would be required to provide the notice as soon as practicable, but not later than 30 days after a Covered Institution becomes aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred. A Covered Institution, pursuant to the Proposed Rule, would not need to provide the notification if the covered institution determines that the sensitive customer information was not actually and is not reasonable likely to be used in a manner that would result in substantial harm or inconvenience.

Third, the Proposed Rule would enhance the protection of customers' nonpublic personal information. The SEC has proposed to apply the Safeguards Rule and the Disposal Rules to "customer information," which is a newly defined term referring to a record containing nonpublic personal information about a customer of a financial institution. The Proposed Rule would apply both rules to both nonpublic personal information that a Covered Institution collects about its own customers and that it receives from a third party financial institution about customers of that financial institution.

Finally, the Proposed Rule would extend the Safeguard Rule and Disposal Rule to transfer agents registered with the SEC or another appropriate regulatory agency.

The comment period for the Proposed Rule will remain open until 60 days of the publication of the proposing release in the Federal Register (unless otherwise extended by the SEC).

This RMF law alert seeks to highlight the key aspects of the Proposed Rule. The material in this blog is meant only to provide general information and is not a substitute nor is it legal advice to you. For more information related to the Proposed Rule, please visit the SEC website at www.sec.gov. If you have any questions or would like to discuss how this applies to your business, please contact:

Steven J. Kuperschmid, Esq.
(516) 663-6686
Skuperschmid@rmfpc.com

Nicole E. Osborne, Esq.
(516) 663-6687
Nosborne@rmfpc.com

Samantha M. Guido, Esq.
(516) 663-6570
sguido@rmfpc.com