FACT SHEET

Final Rules: Enhancements to Regulation S-P

On May 15, 2024, the Securities and Exchange Commission adopted amendments to Regulation S-P, the regulation that governs the treatment of nonpublic personal information about consumers by certain financial institutions. The Commission proposed the amendments on March 15, 2023. The public comment file is available online.

The amendments apply to broker-dealers (including funding portals), investment companies, registered investment advisers, and transfer agents (collectively, "covered institutions") and are designed to modernize and enhance the protection of consumer financial information by:

- Requiring 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;
- Requiring that the response program include procedures for covered institutions to provide timely notification to affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization; and
- Broadening the scope of information covered by Regulation S-P's requirements.

Why This Matters

In 2000, the Commission adopted Regulation S-P, which: (1) broadly requires broker-dealers, investment companies, and registered investment advisers to adopt written policies and procedures to safeguard customer records and information (the "safeguards rule"); (2) requires proper disposal of consumer report information in a manner that protects against unauthorized access to or use of such information (the "disposal rule"); and (3) implemented privacy policy notice and opt out provisions, which Congress subsequently amended in the 2015 Fixing America's Surface Transportation Act ("FAST Act"). Under Regulation Crowdfunding, funding portals must comply with the requirements of Regulation S-P as they apply to brokers.

Since Regulation S-P's adoption, technological developments in how firms obtain, share, and maintain individuals' personal information have corresponded with increased risk of harm to individuals. In addition, the protections afforded customers of covered institutions may vary across different states. The final amendments establish a Federal minimum standard for covered institutions to provide data breach notifications to affected individuals.

What's Required

Incident Response Program

To help protect against harms that may result from a security incident involving customer information, the amendments require covered institutions to adopt an incident response program as part of their written policies and procedures under the safeguards rule. The amendments require an incident response program to be reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information. The incident response program must include procedures to assess the nature and scope of any such incident and to take appropriate steps to contain and control such incidents to prevent further unauthorized access or use. The amendments also require the incident response program to include the establishment, maintenance, and enforcement of written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers.

Customer Notification Requirement

The amendments require covered institutions to notify affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. The amendments require a covered institution to provide the 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, except under certain limited circumstances. The notices must include details about the incident, the breached data, and how affected individuals can respond to the breach to protect themselves. A covered institution is not required to provide the notification if it 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.

The amendments to Regulation S-P also:

- Expand and align the safeguards and disposal rules to cover both nonpublic personal 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;
- Require covered institutions, other than funding portals, to make and maintain written records documenting compliance with the requirements of the safeguards rule and disposal rule;
- Conform Regulation S-P's annual privacy notice delivery provisions to the terms of an exception added by the FAST Act, which provide that covered institutions are not required to deliver an annual privacy notice if certain conditions are met; and
- Extend both the safeguards rule and the disposal rule to transfer agents registered with the Commission or another appropriate regulatory agency.

What's Next

Larger entities will have 18 months after the date of publication in the Federal Register to comply with the amendments, and smaller entities will have 24 months after the date of publication in the Federal Register to comply.