Published on *The National Law Review* https://natlawreview.com

Understanding the Enhanced Regulation S-P Requirements

Article By:

Thomas Kellerman

Securities Practice Group at Stark and Stark

On May 16, 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 amendments apply to broker-dealers, investment companies, and registered investment advisers (collectively, "covered institutions") and are designed to modernize and enhance the protection of consumer financial information. Regulation S-P continues to require covered institutions to implement written polices and procedures to safeguard customer records and information (the "safeguards rule"), properly dispose of consumer information to protect against unauthorized use (the "disposal rule"), and implementation of a privacy policy notice containing an opt out option. Registered investment advisers with over $1.5 billion in assets under management will have until November 16, 2025 (18 months) to comply, those entities with less will have until May 16, 2026 (24 months) to comply.

Incident Response Program

Covered institutions will have to implement an Incident Response Program (the "Program") to their written policies and procedures if they have not already done so. The Program must be designed to detect, respond to, and recover customer information from unauthorized third parties. The nature and scope of the incident must be documented with further steps taken to prevent additional unauthorized use. Covered institutions will also be responsible for adopting procedures regarding the oversight of third-party service providers that are receiving, maintaining, processing, or accessing their client's data. The safeguard rule and disposal rule require that nonpublic personal information received from a third-party about their customers should be treated the same as if it were your own client.

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. 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. To the extent a covered institution will have a notification obligation under both the final amendments and a similar state law, a covered institution may be able to provide one notice to satisfy notification obligations under both the final amendments and the state law, provided that the notice includes all information required under both the final amendments and the state law, which may reduce the number of notices an individual receives.

Recordkeeping

Covered institutions will have to make and maintain the following in their books and records:

- Written policies and procedures required to be adopted and implemented pursuant to the Safeguards Rule, including the incident response program;
- 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 the incident response program;
- Written documentation of any investigation and determination made regarding whether notification to customers is required, including the basis for any determination made and any written documentation from the United States 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 as part of service provider oversight;
- Written documentation of any contract entered into pursuant to the service provider oversight requirements; and
- Written policies and procedures required to be adopted and implemented for the Disposal Rule.

Registered investment advisers will be required to preserve these records for five years, the first two in an easily accessible place.

National Law Review, Volume XIV, Number 163