

Proposed Enhancements to Regulation S-P



The Securities and Exchange Commission proposed enhancements to Regulation S-P – the regulation protecting privacy of consumer financial information – to require broker-dealers, investment companies, registered investment advisers, and transfer agents (collectively, “covered institutions”) to notify individuals affected by certain types of data breaches that may put them at risk of harm. The proposed amendments would enhance protections of customer information by:

- Requiring covered institutions to adopt written policies and procedures for an incident response program to address unauthorized access to or use of customer information;
- Requiring covered institutions to have written policies and procedures 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” – Rule 248.30(a)); (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” – Rule 248.30(b)); and (3) implemented privacy policy notice and opt out provisions required by Congress.

Since Regulation S-P’s adoption, evolution in the technological landscape has made it easier for firms to obtain, share, and maintain individuals’ personal information, which has exacerbated the risk of unauthorized access to or use of customer information. The protections afforded to a customer of a covered institution in one state may differ substantially from the protections afforded to a customer of the same type of institution in another state.

How This Rule Would Apply

The proposal would establish a Federal minimum standard for covered institutions to provide data breach notifications to affected individuals.

Incident Response Program

To help protect against harms that may result from a security incident involving customer information, the proposed amendments would require covered institutions to adopt an incident response program as part of their written policies and procedures under the safeguards rule. The proposal would require an incident response program to be reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, include procedures to assess the nature and scope of any such incident, and contain and control such incidents. The proposal would also apply certain requirements related to incident response to covered institutions' relationships with third party service providers.

Customer Notification Requirement

The proposed amendments would 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 proposal would require a covered institution 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 would not need to provide the notification if the covered institution determines that the sensitive customer information was not actually and is not reasonably likely to be used in a manner that would result in substantial harm or inconvenience.

The proposed enhancements to Regulation S-P would also:

- Expand the safeguards and disposal rules to cover “customer information,” a new defined term referring to a record containing “nonpublic personal information,” a term already in use for other components of Regulation S-P, about a customer of a financial institution. The proposed amendments would therefore apply both rules to both nonpublic personal information that a covered institution collects about its own customers and nonpublic personal information it receives from a third party financial institution about customers of that financial institution;
- Require covered institutions 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 2015 Fixing America’s Surface Transportation Act, which would provide that covered institutions are not required to deliver an annual privacy notice if certain conditions are satisfied; and
- Extend the safeguards rule to transfer agents registered with the Commission or another appropriate regulatory agency. In addition, the proposed amendments would extend the disposal rule from covering only transfer agents registered with the Commission to also transfer agents registered with another appropriate regulatory agency.

Additional Information:

The public comment period will remain open until 60 days after the date of publication of the proposing release in the Federal Register.