NEWS ALERT

The SEC has announced changes to notifi cation requirements by certain financial institutions to people whose data was compromised "as soon as practicable but not later than 30 days" after learning of a breach.

NEW NOTIFICATION REQUIREMENTS FOR FINANCIAL INSTITUTIONS

The Security and Exchange Commission has adopted amendments to Regulation S-P, the regulation governing the treatment of non-public personal information about consumers by certain financial institutions.

The new amendments adopted on May 15, 2024, apply to broker-dealers (including funding portals), investment companies, transfer agents, as well as registered investment advisors.

› Regulation S-P

Adopted in 2000, Regulation S-P requires 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.

› New Requirement Highlights

The new amendments establish a Federal minimum standard for covered intuitions to provide data breach notifications to affected individuals. The requirements include:

- The response program must include procedures for covered institutions to provide notification 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 like to have occurred except under certain limited circumstances.
- Reporting must include details about the incident, the compromised information, and the steps that those affected can take 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.
- It broadens the scope of information covered under Regulation S-P's requirements beyond what the financial institution itself collects, expanding to covering personal information received from other financial institutions.
- It requires covered institutions, other than funding portals, to make and maintain written records documenting compliance with the requirements of the safeguards rule and disposal rule.
- It extends both the safeguards rule and the disposal rule to transfer agents registered with the Commission or another appropriate regulatory agency.

› Timing of Implementation

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.

› The Importance of Cyber Security

Continued developments coming in respect to these rules is expected and assessment of systemic risks and oversight will continue to increase. Advisors and funds should have an active cybersecurity framework including a risk assessment program to get ahead of these future requirements, especially in the area of written policies and record retention.

THE BOTTOM LINE

You can rely on us to be a trusted cyber and privacy expert and resource. Bringing us into the process as early as possible is important to help clients assess their exposure in this fast-changing arena and ensure coverage for critical risks, future potential claims management, and the latest developments in terms and conditions.