

SEC Adopts Cybersecurity-Related Amendments to Regulation S-P for Market Participants

May 23, 2024

Fourteen months after it proposed cybersecurity-related requirements for certain market intermediaries, the SEC has now adopted them, formally requiring such covered entities to adopt written policies and procedures to prepare for and address cybersecurity incidents. The mandate, adopted on May 15, 2024 principally comes from amendments to Regulation S-P.

Who is affected?

Broker-dealers, investment companies, SEC-registered investment advisers and transfer agents, as well as transfer agents registered with other agencies and funding portals under Regulation Crowdfunding.

What will be required?

- Covered entities will be required to have written incident response programs reasonably designed to detect, respond to, and recover from situations in which customer information is improperly accessed or used.
- Entities must develop, maintain, and implement policies and procedures establishing such programs. "Reasonably designed" procedures should specifically include requirements to assess the nature and scope of any cyber breach and to take appropriate steps to contain and control it.
- The programs must provide for timely notification to customers if sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization (as further explained below). Sensitive information is that for which there is a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information.
- The programs must include policies and procedures to address oversight of service providers (including affiliates) through due diligence and monitoring. Policies and procedures must be reasonably designed to ensure that service providers notify the covered institution as soon as possible (no later than 72 hours) after becoming aware that a breach has occurred (consistent with the Cyber Incident Reporting for Critical Infrastructure Act of 2022). Then the covered institution must initiate its own procedures.

What customer notification is necessary?

- After becoming aware that an incident is likely to have occurred, as soon as practicable (and, in any event, within 30 days), the covered market participant must notify customers likely to have been affected with details to assist them in responding appropriately.
 - The notice must describe, in general terms, the incident and the type of sensitive customer information that was or is reasonably believed to have been accessed or used without authorization.
-

- The notice must include information such as the date or estimated date of the incident, contact information sufficient to permit an affected individual to contact the Covered Institution to inquire about the incident, and information about how customers can protect themselves.
- No notice is required if it can be determined 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. For example, if encryption makes the accessed information unusable to the party exfiltrating the data, no notification would be required.
- A covered entity may “delay” customer notification for up to 30 days when the SEC receives a request from the U.S. Attorney General that notice poses a substantial risk to national security or public safety (under an interagency communication process). The delay is renewable.
- Unlike the original proposal, a customer notice does not have to “[d]escribe what has been done to protect the sensitive customer information from further unauthorized access or use” to avoid providing an updated roadmap to threat actors.
- The notification obligation may be satisfied by ensuring that notice is provided, such as by another institution.

What significant other requirements and changes will go into effect?

- Covered institutions must make and maintain written records documenting compliance with the requirements of the amended rules, including the “safeguards rule” and “disposal rule” that address administrative, technical, and physical safeguards for the protection of nonpublic customer records and information and proper disposal of such records.

When does it bite?

Investment company complexes with net assets of \$1 billion or more; registered investment advisers with assets under management over \$1.5 billion; and broker-dealers and transfer agents (that are not “small entities” under the 1934 Act) will have 18 months after the date of publication in the Federal Register to comply; other covered participants will have 24 months.

This is a more relaxed timetable than the one-year implementation originally proposed, but we encourage covered entities to have their compliance groups prepare or update their policies, and to engage in interpretative discussions with internal and external legal counsel and cybersecurity consultants. Covered institutions should ensure that incident response plans include all requirements and that newly updated policies reflect what will actually happen when response plans get triggered.

Carter Ledyard & Milburn LLP uses Client Advisories to inform clients and other interested parties of noteworthy issues, decisions and legislation which may affect them or their businesses. A Client Advisory does not constitute legal advice or an opinion. This document was not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein. © 2024 Carter Ledyard & Milburn LLP.

related professionals

Ronald M. Feiman / Partner
D 212-238-8880
feiman@clm.com

Matthew D. Dunn / Partner

D 212-238-8706

mdunn@clm.com