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

SEC Tightens Cybersecurity Requirements with Regulation S-P Amendments

Article By:

Joseph W. Swanson

Christopher D. Taylor

“The basic idea for covered firms is if you’ve got a breach, then you’ve got to notify. That’s good for investors.” Those were among the remarks that U.S. Securities and Exchange Commission (SEC) Chair Gary Gensler made in announcing the SEC’s amendments to Regulation S-P, governing the treatment of nonpublic personal information by certain financial institutions. For covered institutions (generally, broker-dealers, investment companies, registered investment advisers, and transfer agents), the amended regulation not only ushers in a mandatory data breach reporting requirement but also imposes additional cybersecurity requirements. We summarize the amended regulation and provide key takeaways below.

Incident Response Program

The amended regulation requires every covered institution to develop and implement an incident response program within their existing policies and procedures. This program must be “reasonably designed” to detect, respond to, and recover from incidents of unauthorized access to or use of customer information.

Although the amended regulation allows institutions the flexibility to tailor their policies and procedures to best fit their operational and risk profiles, certain foundational principles must be part of any incident response program:

1. **Assessment of Incidents:** The program must include policies and procedures for assessing the nature and scope of the incident. This involves identifying which customer information systems were compromised and the types of customer information that may have been accessed or used without authorization.
2. **Containment and Control:** Upon detecting an incident, institutions must take appropriate steps to contain and control the situation to prevent further unauthorized access or misuse of customer information. This step is crucial for mitigating the impact of the breach and

safeguarding against additional vulnerabilities.

3. **Notification of Affected Individuals:** The program must also outline procedures for notifying individuals whose sensitive customer information was, or is likely to have been, compromised. Notifications must be made unless the institution, following a reasonable investigation, determines that the sensitive customer information has not been and is not likely to be used in a manner that could result in substantial harm or inconvenience to the customer.

Notification Requirement

The amended regulation imposes a notification requirement where there has been unauthorized access or use of "sensitive customer information," defined as any element of customer data, alone or combined with other information, the compromise of which might substantially harm or inconvenience the individual associated with that information.

Under the amended regulation, covered institutions must conduct a reasonable investigation to determine the likelihood of harm resulting from a potential cybersecurity incident. If a covered institution concludes that the sensitive information has not been and is unlikely to be used in a manner that could result in substantial harm or inconvenience, the requirement to notify may be waived. The reasonableness of an investigation will be determined by the specifics of the situation. For instance, an intentional security breach by a cybercriminal might necessitate a more thorough investigation compared to an inadvertent data exposure by an employee.

If the covered institution concludes that there has been a compromise, that institution must notify affected individuals as soon as reasonably practicable and no later than 30 days, with limited exceptions. A notification must provide details about the breach, including the nature of the incident and the specific data involved. Moreover, the notices should guide affected individuals on appropriate steps to safeguard themselves from potential harm.

Oversight of Service Providers

The amended regulation requires that a covered institution's incident response program include written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers. A "service provider" is "any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution." This expansive definition could include a broad range of entities, including email providers, customer relationship management systems, cloud applications, and other technology vendors.

A covered institution's written policies and procedures must be reasonably designed to ensure the service providers take appropriate measures to protect against unauthorized access to or use of customer information and provide notification to the covered institution as soon as possible, but no later than 72 hours after becoming aware that a breach in security has occurred resulting in unauthorized access to a customer information system. Upon receipt of such notification, a covered institution must initiate its incident response program.

Other Aspects of the Amended Regulation

Among other things, the amended regulation imposes additional recordkeeping requirements on covered institutions, including documenting unauthorized access to or use of customer information

and any investigation made regarding such an incident. The amended regulation also requires policies and procedures related to the proper disposal of consumer information and customer information.

Key Takeaways

- The amended regulation is yet another data point demonstrating the federal government's focus generally, and the SEC's focus in particular, on cybersecurity compliance. Covered institutions can expect that focus to continue and the volume of cybersecurity enforcement actions to increase.
- The amended regulation will be effective later this summer. Larger entities will have 18 months to comply and smaller entities will have 24 months. Covered institutions should evaluate the regulation's application to them and plan their compliance efforts accordingly.
- Covered institutions should begin reviewing and updating their policies and procedures to ensure they reflect the new requirements. This proactive approach will help identify gaps and ensure compliance with the amended regulation within the prescribed timeline.
- Covered institutions should also review existing service provider agreements to ensure sufficient oversight and compliance of service providers consistent with the amendments. This includes implementing due diligence and monitoring measures to verify that service providers adhere to the new security and notification requirements.
- Although the amended regulation is noteworthy for imposing a mandatory notification requirement, as a practical matter, that obligation has existed in the form of state data breach laws and other regulations. As a result, covered institutions should leverage their existing incident response plans and notification playbooks and determine the extent to which existing processes and procedures can be leveraged.

National Law Review, Volume XIV, Number 165