DORSEY
DORSEY+WHITNEY LLP

SEC Adopts Amendments to Expand the Requirements of Regulation S-P for Registered Investment Advisers and Broker-Dealers

by David Tang, Austin T. Chambers, and Michael Schmieder

On May 16, 2024, the SEC adopted amendments (the "Amendments") to Regulation S-P to require SEC-registered investment advisers and broker-dealers (collectively, "Covered Institutions") to develop, implement, and maintain written policies and procedures to protect customer information against any anticipated threats or hazards that could result in harm or inconvenience to customers. [1] The Amendments add requirements for an incident response program reasonably designed to detect, respond to, and recover from unauthorized access to or use of certain "customer information" and to notify customers whose information was, or is reasonably likely to have been, accessed or used without authorization.

Under the Amendments, "customer information" is expanded to include non-public personal information of a Covered Institution's customers, as well as such information received by a Covered Institution from other Covered Institutions. Examples of such customer information include typical non-public personal information such as Social Security number or driver's license number; biometric record; a unique electronic identification number, address, or routing code; and other customer information identifying an individual or the individual's account. The Amendments further define a subset of "sensitive customer information" that are subject to additional obligations. Sensitive customer information includes "any component of customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information."

Incident Response Program

The Amendments require Covered Institutions to adopt written policies and procedures to include a program reasonably designed to detect, respond to, and recover from unauthorized access or use of customer information, including customer notification procedures. The response program must include procedures for the Covered Institution

Related People

- David Tang
- Austin T. Chambers
- Michael Schmieder

Related Capabilities

- Investment Management
- Investment Funds
- Financial Services Regulatory
- Corporate Governance & Compliance

to:

(i) assess the nature and the scope of any incident involving unauthorized access to or use of customer information and identify the customer information systems and types of customer information that may have been accessed or used without authorization;

(ii) take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information; and

(iii) notify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization unless the Covered Institution determines, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, 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.

Notice to Affected Individuals

Covered Institutions are required to provide clear and conspicuous notice to each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. The notice to customers must include: a description and details of the incident, information to contact the Covered Institution about the incident, and actions to take to further protect themselves from the incident.

The notice must be transmitted by a means designed to ensure that each affected individual can reasonably be expected to receive actual notice in writing. If an incident of unauthorized access to or use of sensitive customer information has occurred or is reasonably likely to have occurred, but the Covered Institution is unable to identify which specific individuals' sensitive customer information has been accessed or used without authorization, the Covered Institution must provide notice to all individuals whose sensitive customer information resides in the customer information system that was, or was reasonably likely to have been, accessed or used without authorization. The notice must be provided to affected individuals as soon as practicable, but no later than 30 days, after the Covered Institution becomes aware of the unauthorized access to or use of customer information. A Covered Institution may enter into a written agreement with its service provider to notify affected individuals on the Covered Institution's behalf provided that the obligation to ensure that affected individuals are notified ultimately rests with the Covered Institution.

Oversight of Service Providers

The Amendments require Covered Institutions to establish, maintain, and enforce written policies and procedures reasonably designed to require oversight of service providers, including through due diligence and monitoring, and to ensure that affected individuals receive the notice required. These policies and procedures must be reasonably designed to ensure 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 maintained by the service provider.

Books and Records

The Amendments will add requirements for Covered Institutions to make and maintain written records documenting compliance with the new requirements, including 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 and written documentation of any investigation and determination made regarding whether notification is required.

Compliance Period

The SEC is providing an 18-month compliance period after the date of publication of the Amendments in the Federal Register for "larger entities" (defined to include registered investment advisers with $1.5 billion or more in assets under management and all broker-dealers that are not small entities under the Securities Exchange Act of 1934), and a 24-month compliance period after the date of publication of the Amendments in the Federal Register for all other "smaller entities."

Dorsey Observations

The Amendments expand the information security and incident response requirements of Regulation S-P providing additional avenues for possible SEC enforcement against Covered Institutions. Covered Institutions would be well-advised to review and revise their information security policies and procedures, as well as vendor management and incident response programs, to comply with the requirements of the Amendments prior to the compliance date. Dorsey's compliance services are available to assist Covered Institutions with their compliance with the Amendments.

[1] Regulation S-P; Privacy of Consumer Financial Information and Safeguarding Customer Information (May 17, 2024). The Amendments also apply to registered investment companies, funding portals, and transfer agents.