Katten

FINANCIAL MARKETS AND FUNDS ADVISORY

New Rules for Investment Advisers and Brokers Relating to Cybersecurity Breaches

June 27, 2024

On May 16, the Securities and Exchange Commission (SEC) unanimously approved amendments to Regulation S-P, which imposes new rules relating to cybersecurity breaches involving investment advisers and brokers. Larger entities must comply with the new rules by January 3, 2026, and smaller entities must comply with the new rule by June 3, 2026.

Regulation S-P previously had three main components: an information safeguards rule, privacy rules and an information disposal rule. The information safeguard rules generally require financial institutions — including broker-dealers, funding portals, investment advisers, registered investment companies and employee securities companies — to adopt written policies and procedures to protect customer nonpublic personal information (Customer Information) against unauthorized access and use, including anticipated threats or hazards to the security or integrity of Customer Information. The privacy rules require these covered institutions to provide initial and annual privacy notices to customers describing information-sharing policies and informing customers of their rights. The information disposal rule generally requires financial institutions to properly dispose of Customer Information and consumer information.

The amendments to Regulation S-P will add a fourth requirement, compelling covered institutions to adopt written policies and procedures that are reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer nonpublic personal information. This recovery or response program includes procedures to (1) assess the nature and scope of any incident; (2) take appropriate steps to contain and control the incident; and (3) notify affected individuals whose Sensitive Customer Information (as defined below) was, or is reasonable likely to have been, accessed or used without authorization unless, after a reasonable investigation, the covered institution 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.

“Sensitive Customer Information” is a subset of Customer Information, the compromise of which would present a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information. The amendments to Regulation S-P provide a non-exhaustive list of Sensitive Customer Information in two categories. The first category is information that can be uniquely identified with an individual (like a Social Security Number or biometric identifiers). Second, Sensitive Customer Information includes information that could be used to gain access to an account (e.g., username in conjunction with password or mother’s maiden name).

Importantly, the amended rule expands the definition of Customer Information to include not only information about individuals with whom the financial institution has a customer relationship but also information about “the customers of other financial institutions where such information has been provided to the covered institution.” This expanded definition of Customer Information does not apply to Regulation S-P’s privacy rules but does apply to the information safeguards rule, the information disposal rule and the new rules regarding detecting and responding to unauthorized access to Customer Information (all of the foregoing collectively the Information Protection Rules).

Accordingly, financial institutions are expected to adopt policies and procedures to comply with the Information Protection Rules with respect to nonpublic personal information they possess about persons with whom they do not have a customer relationship.

The notice required by amended Regulation S-P must be provided as soon as practicable but generally not later than 30 days after the financial institution becomes aware of an unauthorized breach of Sensitive Customer Information. The notice must include details about the incident, the breached data and how affected individuals can respond to the breach to protect themselves. Notification is necessary even if the financial institution is unable to identify which specific individuals' Sensitive Customer Information has been accessed or used without authorization. In such circumstances, the financial 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 without authorization.

Under the amendments to Regulation S-P, financial institutions' incident response programs must include policies and procedures "reasonably designed to require oversight, including through due diligence on and monitoring, of service providers" to ensure the financial institution meets its customer notification requirements. Such policies and procedures must be reasonably designed to monitor that 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 of a breach in security has occurred resulting in unauthorized access to a Customer Information system maintained by the service provider.

The amendments also (1) require covered institutions, other than funding portals, to make and maintain written records documenting compliance with the requirements of the information safeguards rule and information disposal rule; (2) conform Regulation S-P's annual privacy notice delivery provisions to the terms of an exception added by the FAST Act, which provides that covered institutions are not required to deliver an annual privacy notice if certain conditions are met; and (3) extend both the information safeguards rule and the information disposal rule to transfer agents.

Action Steps

Review and Update Policies and Procedures. Covered institutions must revise their policies and procedures by the compliance dates. This should include updating existing information safeguards and disposal policies to account for the expanded definition of Customer Information, updating incident response programs and updating vendor risk management policies and procedures.

Assess Competing Incident Notification Requirements. The amendments to Regulation S-P provide another requirement in the myriad notification requirements that financial institutions face from other federal and state regulations.

Identify and Update Service Provider Arrangements. Identify the service providers in scope under the amendments to Regulation S-P and review existing contracts or other agreements to ensure there is sufficient oversight in place for compliance. To the extent updates are necessary, determine whether changes need to be made to existing contracts or whether there are other means of oversight that satisfy new requirements. Consider updating standard contract provisions to ensure appropriate oversight provisions for new service providers going forward.

Update Record-Keeping. Ensure that books and records required by the amendments to Regulation S-P are appropriately maintained and that any retention schedules are updated accordingly.

Consider New Monitoring Tools. The broad definition of affected individuals will expand potential notification obligations.

Considerations for Private Fund Advisers. The adopting release for the new rules reaffirms the SEC's longstanding guidance that Regulation S-P does not apply to private investment funds (Private Funds). However, since Customer Information has been expanded to include information about "customers of other financial institutions," it is likely that investment advisers to Private Funds will need to comply with Information Protection Rules with respect to nonpublic personal information of natural person investors in Private Funds that they manage. That is because Private Funds would normally be deemed financial institutions for the purposes of Regulation S-P, and, therefore, if an investment adviser to a Private Fund receives nonpublic personal information regarding the Private Fund's investors, such information will be deemed Customer Information of the investment adviser. Private Funds were already subject to the Federal Trade Commission information safeguards rule (FTC Rule). Although the FTC Rule and the Information Protection Rules have certain similarities, they also have certain differences. For example, the FTC Rule does not have a customer notification requirement for breaches but does require that certain breaches be reported to the Federal Trade Commission. Private Fund investment advisers will need to be cognizant of the requirements of the FTC Rule and the Information Protection Rules when implementing their information security programs.

CONTACTS

For more information, please contact your Katten attorney or either of the following Financial Markets and Funds attorneys.

David Y. Dickstein
+1.212.940.8506
david.dickstein@katten.com

Richard D. Marshall
+1.212.940.8765
richard.marshall@katten.com