CHAPMAN
Focused on Finance

Client Alert

SEC Proposes Enhanced Cybersecurity Regulations for Financial Industry Participants

March 22, 2023

On March 15, 2023, the U.S. Securities and Exchange Commission ("SEC") issued a series of proposals designed to improve firms' preparedness and responses to cyber incidents. The proposals, which would impact many of the financial services industry participants regulated by the SEC, generally require that firms establish policies and procedures to better prevent and detect cyber incidents and disclose certain cyber incidents to clients and the SEC within specified time periods. The proposals take the form of amendments to Regulation S-P and Regulation SCI and new rules under the Investment Advisers Act of 1940 ("Advisers Act"), the Investment Company Act of 1940 ("Investment Company Act") and the Securities Exchange Act of 1934 ("Exchange Act"), as well as related form changes. Two of the commissioners made statements that were critical of the proposals, pointing out that the proposals would create overlapping and divergent obligations on industry participants and that the proposed rules did not address comments to a similar proposal made in 2022. If the proposals are adopted, their impact would be twofold: the proposals would (1) expand the SEC's oversight of firms' handling of cybersecurity and cyber incidents, including with respect to examinations and enforcements, and (2) create new obligations on behalf of industry participants to generate client disclosures and/or regulatory filings in the event of a cyber incident. A summary of each of the proposed rules is below. The comment period on each rule will run for 60 days following publication in the Federal Register.

Cybersecurity Risk Management Programs and Disclosures for Advisers and Funds

The SEC has re-opened the comment period for proposed new rules under the Advisers Act and the Investment Company Act and related form amendments that would, among other things, require advisers and registered investment companies to adopt and implement policies and procedures reasonably designed to address cybersecurity risks. A fund would be required to include additional cybersecurity-related disclosure, including any significant cyber incidents, in its registration statement. Advisers would be required to provide comparable cyber disclosures in Part 2A of its Form ADV. In addition, advisers would be required to report cybersecurity incidents, including on behalf of a registered or private fund client, to the SEC via new Form ADV-C within 48 hours of having a reasonable basis to conclude that a significant cybersecurity incident had occurred or is occurring. This proposal was originally put forward by the SEC's Division of Investment Management in February 2022. The complete SEC proposal is available here.

Cybersecurity Risk Programs for Market Entities

Proposed Rule 10 under the Exchange Act would require broker-dealers, clearing agencies, major security-based swap participants, the Municipal Securities Rulemaking Board, national securities associations, national securities exchanges, security-based swap data repositories, security-based swap dealers and transfer agents (collectively, "Market Entities") to establish and review, at least annually, written policies and procedures reasonably designed to address their cybersecurity risks. All Market Entities also would need to give the SEC immediate written electronic notice of a significant cyber incident upon having a reasonable basis to conclude that the significant cyber incident had occurred or is occurring.

In addition, Market Entities, other than certain small broker-dealers, would be required to adopt specified policies and procedures to address cybersecurity risks and file new Form SCIR. A covered Market Entities would be required to file Part I of Form SCIR in the event it experiences a significant cyber incident. Part I would disclose information about the incident and the entity's efforts to respond to and recover from the cyber incident and would be required to be filed after the "immediate written electronic notice" to the SEC, but within 48 hours of when the entity had a

reasonable basis to conclude that the significant cyber incident had occurred or is occurring. Covered Market Entities would be required to amend a filed Part I if the information materially changes or becomes inaccurate and when the entity resolves the issue and closes any internal investigation of the incident. Part II of Form SCIR would be filed annually and disclose summary descriptions of cybersecurity risks and significant cyber incidents experienced during the current or previous calendar year. A covered Market Entity would also be required to make its Part II available on its website. The complete SEC proposal is available here.

Proposed Changes to Regulation S-P

Regulation S-P, in its current form, requires that broker-dealers, funds and advisers safeguard and properly dispose of customer information as well as implement a privacy policy notice with opt-out provisions. Amended Regulation S-P would expand the current requirements to transfer agents registered with the SEC or another regulatory authority. Amended Regulation S-P would also require that all covered institutions create an incident response program to respond to and recover from data breaches and provide data breach notifications to affected customers. Data breach notifications would be required within 30 days of the covered institution becoming aware that unauthorized access to sensitive customer information has occurred or was reasonably likely to have occurred, unless the covered institution determines that the sensitive customer information was not, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience. The proposal would also require that covered institutions to amend contracts with certain third-party service providers to include specified provisions related to protection of customer data and notification of data breaches. The proposal would also expand the scope of information covered by the current provisions of Regulation S-P to include nonpublic personal information for customers of the covered institution as well as the information of customers of other financial institutions, meaning that a firm's safeguarding and disposal obligations would apply to all nonpublic personal information to which the firm has access even if the information pertains to a person that is not a customer of the firm so long as the person is a customer of another covered financial institution. The complete SEC proposal is available here.

Proposed Changes to Regulation SCI

Regulation SCI currently requires self-regulatory organizations, such as national securities exchanges, certain clearing agencies, registered securities associations, certain alternative trading systems, certain market data consolidators and disseminators and the Municipal Securities Rulemaking Board, to have policies and procedures designed to ensure their system's capacity, integrity, resiliency, availability and security. The current form of Regulation SCI also requires that, if a cyber event occurs, the covered entity take appropriate corrective action and provide certain notitices and reports to the SEC. Current Regulation SCI also provides a safe harbor for SCI Entities, who will be deemed to have policies and procedures that comply with the Regulation if the policies are consistent with "current SCI industry standards."

As proposed, the amended Regulation SCI would expand the list of covered entities to include registered securities-based swap data repositories, clearing agencies exempt from registration with the SEC and registered broker-dealers that exceed either a total assets threshold or one or more transaction activity thresholds. In addition, the proposal would strengthen Regulation SCI by specifying additional required policies and procedures, including, among other things, an inventory, classifications and lifecycle management program for direct and indirect SCI systems; a program to manage and oversee third-party service providers; business continuity/disaster recovery programs and testing that account for the use of third-party service providers; and a program to prevent unauthorized access to SCI systems and information. The SEC also proposes that, in order to take advantage of the safe harbor provided in the current Regulation, SCI policies and procedures will need to identify the industry standards with which such policy is consistent. The proposed amendments would also expand the definition of "systems instrusion" covered by Regulation SCI and provide additional requirements for review and assessment of risks to covered systems. The complete SEC proposal is available here.

For More Information

If you would like further information concerning the matters discussed in this article, please contact a member of Chapman's Corporate and Securities Department or the Investment Management Group or visit us online at chapman.com.