CARTER LEDYARD

our resources

SEC Addresses Cybersecurity Market Risks, Controls and Disclosures for Market Participants Through Proposed New Rules and Amendments

April 06, 2023

On March 15, 2023, the U.S. Securities and Exchange Commission (the "SEC") proposed rigorous regime changes for a wide range of market participants that maintain data about investors. This flurry of rulemaking activity by the SEC that began last year is intended to address cybersecurity and technology risks and their implications for the markets and supports the SEC's view that "technology is not just fundamental to the operation of the markets—it is the markets, and managing it is vital for investor protection and fair, orderly, and efficient market operations."[1]

- The SEC proposed to apply cybersecurity risk management rules to market entities such as broker-dealers, including those that operate alternative trading systems; clearing agencies, national securities exchanges and FINRA and the Municipal Securities Rulemaking Board; security-based swap dealers, participants and repositories; and transfer agents (some of which, based on regulatory capital, total assets or other criteria, would have additional requirements as "covered entities"). These rules would require written policies and procedures, notification of certain breaches to the SEC (immediately and within 48 hours on a new EDGAR form, and upon development of further significant information), and enhanced public disclosures. Covered entities would have to produce annual assessment reports.[2]

- The SEC reopened the comment period on proposed rules related to cybersecurity risk management and cybersecurity-related disclosures for registered investment advisers, registered investment companies, and business development companies that were initially proposed in early 2022 (with the initial comment period ending on April 11, 2022).[3] We detailed aspects of these rules in a previous client advisory.

- The SEC proposed amendments to Regulation S-P—which requires parties such as investment companies, broker-dealers, and investment advisers to have written policies and procedures to safeguard records consisting of customer information and to properly dispose of them. The amendments would require that these entities maintain an incident response program for occurrences of unauthorized access to or use of customer information. Such a program would provide for investigation, assessment and reporting, including notice to affected individuals within 30 days of awareness of an incident—sooner if "practicable"—that is reasonably likely to cause risk of substantial harm or inconvenience or to be accessed or used by an unauthorized third party. Perhaps, even more significantly, written contracts with service providers (and policies and procedures for their engagement) would need to obligate the provider to act to "protect against" unauthorized access or use of customer information and notify individuals within 48 hours of becoming aware of a breach. Transfer agents would be added to those entities subject to Regulation S-P.[4]

- In addition, the SEC proposed to amend Regulation SCI (Systems Compliance and Integrity), which applies to entities with automated and similar systems that support any of six securities market functions: trading, clearance and settlement, order routing, market data, market regulation, and market surveillance—as well as systems that would be reasonably likely to pose a security threat to the forenamed systems, if breached. Entities that use third-party providers, including cloud services, would be required to have

programs to manage and oversee such providers and to take account of them in business continuity plans. The proposals would also add types of cyber events and incidents (*e.g.*, DDoS attacks) that would require immediate reporting to the SEC. The amendments would also impose new requirements such as the development of internal controls for SCI systems, assessment of their design and effectiveness, management of third-party risks, and annual penetration testing.[5]

In all of the foregoing proposals, additional recordkeeping requirements would be incorporated. Comments are due on each proposal within 60 days of its publication in the Federal Register. Covered Entities should become familiar with the proposed amendments now, begin to assess the steps that would be necessary to achieve compliance, and anticipate the costs and mechanisms they would need to implement fully compliant administrative, physical, and technical safeguards. Covered entities are encouraged to consult legal counsel to assist in interpreting the proposed rules and amendments, evaluating prospective compliance obligations, and submitting comments on these proposed rules and amendments.

* * *

---

[1] https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523.

[2] https://www.sec.gov/news/press-release/2023-52; https://www.sec.gov/rules/proposed/2023/34-97142.pdf.

[3] https://www.sec.gov/news/press-release/2023-54; https://www.sec.gov/rules/proposed/2023/33-11167.pdf.

[4] https://www.sec.gov/news/press-release/2023-51; https://www.sec.gov/rules/proposed/2023/34-97141.pdf.

[5] https://www.sec.gov/news/press-release/2023-53; https://www.sec.gov/rules/proposed/2023/34-97143.pdf.

---

related professionals

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

Matthew D. Dunn / Partner
D 212-238-8706
mdunn@clm.com