CARLTON FIELDS

SEC Stirs Its Pot of Cybersecurity Preparedness and Response Proposals

May 25, 2023

The SEC remains laser-focused on cybersecurity, with the agency recently reopening the comment period on a sweeping rule for investment advisers and investment companies. In addition, the SEC issued proposed enhancements to Regulation S-P, the agency's existing regulation designed to protect the privacy of consumer financial information.

Last year, we reported on the SEC's proposed cybersecurity rule intended to increase regulation of advisers' and investment companies' cybersecurity preparedness. See "SEC Plants New Cybersecurity Regulations; Time Will Tell What Will Bloom." That proposed rule would have required, among other things, more detailed and well-documented cybersecurity programs, as well as cybersecurity disclosures to current and prospective clients and security holders and reports to the SEC within 48 hours of "significant cybersecurity incidents." Although the comment period for that rule closed in April 2022, the SEC announced on March 15, 2023, that it was reopening that period, such that it will receive additional comments until May 22, 2023.

Also on March 15, the SEC proposed amendments to Regulation S-P, with comments due June 5, 2023.

Adopted in 2000, Regulation S-P generally requires broker-dealers, investment companies, and registered investment advisers to adopt policies and procedures to safeguard customer records and information. The existing regulation, however, does not include a breach notification requirement.

The proposed amendments to Regulation S-P would change this and place greater emphasis on incident response by requiring the following from covered institutions:

- Written policies and procedures for an incident response program to address unauthorized access to, or use of, customer information.
  - That program must be reasonably designed to detect, respond to, and recover from unauthorized access to, or use of, customer information.
- Notice to individuals whose sensitive customer information was or is reasonably likely to have been accessed or used without authorization.
  - That notice would be required as soon as practicable but no later than 30 days after the institution becomes aware of the potential compromise of customer information.
- Procedures to address security risks involving service providers, through contractual provisions requiring the protection of customer information and prompt notification to the covered institution in the event of a breach.

In announcing the release of the proposed amendments, the SEC appeared focused on addressing the ever-increasing risk of customer information being compromised, given the many expansions in technology. The SEC also noted how, under the current patchwork approach to breach notification provided by varying standards under state law, the SEC's proposal would establish a federal minimum standard for breach notifications by covered institutions. Given the SEC's continued interest in cybersecurity, covered institutions should consider the following action items:

- Evaluate the extent to which existing cybersecurity programs can help satisfy the proposed new standards. Because many covered institutions may already have robust programs to comply with other regulatory regimes, such as the New York State Department of Financial Services' cybersecurity regulation, those institutions would be wise to leverage their existing programs and efficiently comply with any new standards formally adopted by the SEC.
- Emphasize incident preparation and response, particularly in light of potential new breach notification requirements under one or both of the SEC proposals. To meet those requirements, institutions will need to quickly detect, investigate, and respond to suspected incidents.

The proposals described above also come against the backdrop of the SEC also proposing on March 15 a new rule, form, and related amendments to require "market entities," including many broker-dealers, to address cybersecurity risks through the implementation of policies and procedures, regular reviews of those policies and procedures, and immediate notice to the SEC of any significant cybersecurity incident. Comments on this proposal are due by June 5, 2023.

Meanwhile, for its part, the National Association of Insurance Commissioners' Cybersecurity (H) Working Group is seeking input this spring on a plan to aid state insurance regulators in responding to cybersecurity events, which would include collecting information from companies regarding those

events. This would be another regulatory development focused on cyber incident response. Covered institutions would be wise to plan accordingly.

Related Practices

Securities Transactions and Compliance
Financial Services Regulatory
Cybersecurity and Privacy
Life, Annuity, and Retirement Solutions

Related Industries

Life, Annuity, and Retirement Solutions
Securities & Investment Companies
Life, Annuity, and Retirement Solutions