Blogs
March 20, 2023
Highlighting Enforcement Focus on Cybersecurity, SEC Proposes New Disclosure & Incident Response Rules

The U.S. Securities and Exchange Commission's focus on cybersecurity continues in its most recent effort to modernize financial privacy rules and emphasize transparency between SEC-regulated entities who suffer from a cyber breach and the individuals impacted by the breach.

The SEC's latest proposals focus on registrants including broker-dealers, investment advisors, and investment companies, and seek to impose cyberbreach disclosure requirements similar to those the SEC previously proposed for public companies.

On March 15, 2023, the SEC proposed amendments to current data privacy rules that would require covered firms to adopt written policies and procedures for incident response programs. Under the proposed amendments, such policies and procedures must address unauthorized access to or use of customer information, including procedures for providing timely notification to individuals affected by an incident involving sensitive customer information with details about the incident and information designed to help affected individuals respond appropriately. The proposed changes would come through amendments to rules under Regulation S-P.

Regulation S-P currently requires covered registrants to notify customers about how they use their financial information, but it does not require them to notify customers about breaches. The proposed amendments would also ensure that breaches are properly identified, and that sensitive customer data is monitored to determine whether it was accessed.

In announcing the proposed amendments, Chairman Gensler explained that investors would benefit from a financial privacy rule "more modern than the AOL era."

In addition, on March 15, 2023, the SEC proposed a rule impacting broker-dealers and other market entities that would require the establishment, maintenance, and enforcement of written policies and procedures that are reasonably designed to address their cybersecurity risks. Notably, under the proposed rule, broker-dealers would

need to give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident had occurred or is occurring.

These are not the SEC's first set of proposed rules modernizing cybersecurity reporting. In fact, the SEC has similarly proposed rules and amendments related to cybersecurity risk management, strategy, governance, and incident reporting for public companies subject to the Securities Exchange Act of 1934, which are set to become effective in June 2023.

Given the SEC's focus on cybersecurity and reporting obligations, broker-dealers, investment companies, and investment advisers registered with the SEC would be wise to look to recent SEC enforcement actions when drafting policies and procedures related to incident response and customer notification. Enforcement actions like *First American* and most recently, *Blackbaud*, for example, demonstrate the importance of the internal reporting structure for issues related to cybersecurity to ensure that the right people have the necessary information to make fulsome and accurate customer notifications. As the SEC continues to emphasize transparency between companies who suffer a cyber breach and those impacted by that breach, covered entities should preemptively focus on shoring up and modernizing their cybersecurity reporting policies and procedures.

Authors

Explore more in

White Collar & Investigations