Cooley

SEC Remains Focused on Disclosure of Cybersecurity Incidents

June 6, 2024

Recent Securities and Exchange Commission (SEC) enforcement action and statements by SEC officials show that the Commission remains focused on disclosures regarding cybersecurity incidents. On May 21, 2024, Erik Gerding, director of the SEC's Division of Corporate Finance, **issued a statement to clarify** that public companies are only required to disclose a cybersecurity incident under Item 1.05 of Form 8-K if the incident is "determined by the registrant to be material." The next day, on May 22, 2024, the SEC announced that it has **settled charges** with The Intercontinental Exchange (ICE) relating to ICE's alleged failure to timely inform the SEC of a cyber intrusion under Regulation Systems Compliance and Integrity (SCI). While Regulation SCI only applies to a small number of key market participants, the SEC's enforcement order and recent statements signal that the SEC will not hesitate to enforce regulations that require disclosures of cybersecurity incidents.

Gerding's statement

In July 2023, the SEC adopted cybersecurity rules that require public companies to disclose material cybersecurity incidents under Item 1.05 of Form 8-K. In his statement, Gerding clarified that Item 1.05 should only be used after a company has determined that the cybersecurity incident is material (for more background on the SEC's cybersecurity rules, **see our August 2023 post**). If a company chooses to voluntarily disclose a cybersecurity incident but has not yet made a materiality determination, or has determined that the incident is immaterial, the company is free to do so under a different item of Form 8-K, such as Item 8.01. However, if the company subsequently determines that the incident is material, then it is required to file an Item 1.05 Form 8-K within four business days of such materiality determination. Gerding stated that the clarification is intended to encourage the voluntary disclosures of cybersecurity incidents in a manner that does not result in investor confusion or dilution of Item 1.05 disclosures.

Gerding acknowledged the difficulty of determining whether a cybersecurity incident is material and encouraged companies to consider a wide range of factors, including the impact of the cybersecurity incident on the company's financials, reputation, customer relationships, and potential regulatory actions. Indeed, as Gerding noted, a significant cybersecurity incident would be material even if the company has not yet assessed its impact on the company's financials.

SEC's settlement with ICE

In light of the speed and interconnected nature of the securities markets, the SEC promulgated Regulation SCI in 2015 to improve the SEC's oversight of the core technology of key market participants. It requires covered entities – which include national securities exchanges – to implement policies and procedures to ensure the integrity and resiliency of their computer and network systems, to report the occurrence of any systems disruptions (called "SCI events") to the SEC and take corrective actions, and to conduct periodic testing and review of their systems. Notably, Rule 1002(b)(1) requires covered entities to "immediately" notify the SEC of an SCI event when they have "a reasonable basis to conclude" that the SCI event occurred. Rule 1002(b)(2) further requires covered entities to submit a written notification containing additional information on the SCI event "within 24 hours." Timely notification of an SCI event is required unless the covered entity immediately concludes that the SCI event had de minimis impact on the entity's operations or on market participants.

In a May 2024 order, the SEC alleged that on April 15, 2021, a third party notified ICE that it was one of several entities potentially impacted by a "zero-day" (i.e., previously unknown) vulnerability in its virtual private network (VPN) concentrators. The next day, ICE identified malicious code associated with the threat actor on one of its VPN devices. According to the SEC, this meant that ICE had "a reasonable basis to conclude" that it was subject to the cyber intrusion, thus triggering the obligation to immediately report the SCI event to the SEC.

According to the SEC enforcement order, ICE did not immediately notify the SEC of the cyber intrusion. Over the next four days, ICE analyzed the vulnerability and ultimately concluded that there was no evidence of an established unauthorized VPN session or penetration of the ICE network environment. ICE's legal and compliance personnel then determined the intrusion to be a de minimis SCI event that did not require immediate notification to the SEC.

Two days later, on April 22, 2021, the SEC independently contacted ICE about the zero-day vulnerability. ICE thereafter provided information to the SEC about the intrusion, including that ICE has declared it to be a de minimis SCI event.

The SEC found that ICE's failure to immediately report the cyber intrusion violated Regulation SCI. According to the SEC, ICE had an obligation to immediately notify the SEC of the cyber intrusion because they could not reasonably estimate that the intrusion was a de minimis event right away. The SEC explained that the reasoning behind this strict reporting requirement is "simple:" "If the SEC receives multiple reports across a number of these types of entities, then it can take swift steps to protect markets and investors."

The SEC's settlement with ICE is the latest installment in a series of recent SEC enforcement actions relating to companies' disclosures about cybersecurity incidents. In October 2023, the SEC **filed a complaint against SolarWinds Corp. and its chief information security officer** relating to SolarWinds' failure to disclose and address ongoing cybersecurity issues. In March 2023, the SEC **settled charges against Blackbaud** relating to Blackbaud's public disclosures about a ransomware attack. The SEC staff has signaled the importance of timely and consistent disclosures of cybersecurity incidents (despite the fact that key market participants are required to report cyber incidents "immediately," whereas other public companies have four business days). In a **statement from December 2023**, Gerding expressed his view that the cybersecurity disclosure rules were not meant to "prescribe particular cybersecurity defenses, practices, technologies, risk management, governance, or strategy." Rather, those rules are meant to ensure "consistent and comparable disclosures" in order to assist investors in making informed investment and voting decisions.

Key takeaways

Gerding's remarks and the SEC enforcement actions highlight the SEC's focus on cybersecurity and varied requirements regarding disclosure obligations.

For public companies, it may be preferable to voluntarily disclose cybersecurity incidents under Item 8.01 of Form 8-K even if the materiality of the incidents has not been (or could not be) determined. Once a cybersecurity incident is determined to be material, public companies have an obligation to timely disclose the event under Item 1.05 of Form 8-K.

For key market participants that are covered under Regulation SCI, the fact that a cybersecurity incident is not material (or could not be immediately determined to be material) does not mean that disclosure is not required. Rather, as soon as a covered entity has a "reasonable basis" to believe that an SCI event occurred, the covered entity must notify the SEC, unless the covered entity also immediately determines that the SCI event is de minimis. Time is of the essence. In the words of Gurbir S. Grewal, director of the SEC's Division of Enforcement: "When it comes to cybersecurity, especially events at critical market intermediaries, every second counts and four days can be an eternity."

Contributors

Elizabeth Skey
Bio

Bingxin Wu
Bio
