Blogs
December 19, 2023
Corp Fin Director Erik Gerding Speaks on Cyber Incident Disclosure

Yesterday, we **blogged** about four CDIs that Corp Fin issued last week on the "limited disclosure exception" to the obligation of reporting material cybersecurity incidents under Item 1.05 of Form 8-K. Last week, Corp Fin Director Erik Gerding also provided this **informative statement** on the cybersecurity disclosure rules, with insight on how the rules evolved from the proposed to final formulations and what is – and is not – required. Erik's statement is worth noting because of its comprehensive nature and the importance of the topic given that the compliance date for new Item 1.05 of Form 8-K was yesterday.

Here's an excerpt from Erik's statement: "*When must it be disclosed?* Public companies must provide the required cybersecurity incident disclosure within four business days after the company determines the incident to be material. The deadline is *not* four business days after the incident occurred or is discovered. This timing recognizes that, in many cases, a company will be unable to determine materiality the same day the incident is discovered.

A public company may alert similarly situated companies as well as government actors at any point in its incident response, including immediately after discovering an incident and before determining materiality, so long as it does not unreasonably delay its internal processes for determining materiality. The Commission had proposed a "as soon as reasonably practicable" standard but changed this to requiring a materiality determination for a cybersecurity incident "without unreasonable delay." The "without unreasonable delay" standard in the final rule was intended to address commenter concerns regarding the timing of the materiality determination. As the Commission recognized in the adopting release, "a materiality determination necessitates an informed and deliberative process."

Some have asked why the Commission chose four business days as the deadline for disclosure. This timing is consistent with the reporting of other events the Commission requires be reported on a Form 8-K, such as entry into or termination of a definitive material agreement or a bankruptcy. In adopting the four business-day deadline, the Commission explained that cybersecurity incident disclosure was not sufficiently different from

other Form 8-K reporting events to warrant a different approach.

The Commission also recognized that a company may not have complete information about the incident even if it knows enough to determine the incident was material. If the company does not know all the information required to be disclosed four business days after a materiality determination, the final rule contains a mechanism for the company to disclose that information in a subsequent filing.

Why use a materiality standard? I also have heard some people, perhaps less familiar with the Federal securities laws, asking why the standard for disclosure here is limited to "material" cybersecurity incidents. Some seem to prefer a more bright line rule. Materiality is a touchstone of securities laws. It connects disclosures back to the needs of investors. I don't mean to suggest that all disclosures required under the Federal securities laws have or must have a materiality qualifier. Some required disclosures do not. In this case, the Commission determined that a materiality qualifier was appropriate. In my view, this makes sense when you consider that some companies may experience cyber attacks on a daily basis if not more frequently.

In both the adopting release and the proposing release, the Commission affirmed that the materiality standard companies should apply for the cybersecurity incident disclosure is the same standard articulated by the Supreme Court in cases such as *TSC Industries, Inc. v. Northway*, *Basic, Inc. v. Levinson*, and *Matrixx Initiatives, Inc. v. Siracusano*, as well as in Commission rules. The Commission declined to adopt a new standard for materiality unique to cybersecurity. Using this time-tested and familiar materiality standard, rather than a new bespoke standard, is consistent with the overarching rationale for the rule: to give investors disclosure to help assess risks to their investments, in the same way that they receive consistent and comparable disclosure about other risks that public companies face."

Explore more in

Corporate Law

Topics

Quick Alerts