Blogs
December 07, 2023
Corp Fin Director Erik Gerding Talks Risk Disclosure

Here's the entirety of this "White Collar Briefly" blog penned by Gina Buschatzke and Kathryn Campbell:

"At the recent 2023 Garrett Securities Law Institute Conference SEC panelists, including Erik Gerding, Director of the Division of Corporation Finance, reinforced how important it is for companies to assess emerging risks for materiality—particularly those risks stemming from Environmental, Social and Governance (ESG) issues and cybersecurity issues—and to ensure that those risks are appropriately disclosed to investors.

The SEC panelists further cautioned that disclosures related to emerging risks should not be generic disclosures based on industry-wide trends or risks, but instead should focus on the particular ESG or cybersecurity risk faced by the disclosing company. The SEC reiterated that disclosures regarding emerging risks must be specific enough for investors to appreciate the risks that the company is actually facing.

ESG issues and cybersecurity were front and center in the discussions about potentially disclosable emerging risks.

Disclosing ESG Risks

Panelists cautioned that although certain emerging ESG risks may not be immediately identifiable as a disclosable risk, the SEC is still expecting companies to disclose them as soon as possible. The Commission has issued guidance regarding ESG risks, including through "Dear Issuer" letters, which provide a set of sample comments that companies may expect to receive during the public filing review process. The letters can be valuable to identify emerging risks and potential applicability of those risks to a company. For example, in July 2023, the Commission published a "Dear Issuer" letter related to risks associated with investing in companies based in China.

Panelists also advised companies to develop a targeted ESG disclosure plan that is both communicated effectively across the business and actually executable. Moreover, any ESG disclosure program has to be consistent with other corporate public filings like a company's proxy statement and Form 10-K, even including disclaimers for forward looking statements.

Disclosing Cybersecurity Risks

The SEC explained that the final cybersecurity rules adopted in July 2023 merely add to the existing disclosure framework and do not upend historical materiality assessment practices which are based on what a reasonable investor would determine to be material. Additional disclosures required under the final cybersecurity rules include material aspects of the nature, scope, and timing of the cybersecurity incident. Moreover, the SEC advised that the Commission's 2018 cybersecurity guidance was still applicable and encouraged companies to consider it when assessing materiality.

Although the final cybersecurity rules require a Form 8-K to be filed within four business days after the company determines a material cybersecurity event has occurred, questions surrounding timing still remain and were a focus of the panel. For example, if a company contacts the Department of Justice to seek a disclosure delay, does that contact mean that a materiality assessment has already been made and the four-day clock for disclosure has started to run? The answer, according to SEC panelists, is that companies still have to assess the total mix of information available and make a materiality determination without unreasonable delay, but the four-day clock doesn't run until the materiality determination is concluded. Since materiality determinations are often times tied to an analysis of legal issues, it remains to be seen what it will take to convince the SEC that the four-day deadline was met without intruding into a company's legal privileges.

Accordingly, understanding the contours of cybersecurity disclosures will likely remain a significant topic for the SEC and registered entities alike as companies seek to comply with the recently adopted final rules. More detail regarding the final cybersecurity rules including practical considerations regarding implementation can be found here.

Key Takeaways

1. Companies should consider emerging risks, including those related to ESG and cybersecurity, and how those risks are being communicated to investors when they are deemed material.
2. Risks are not static and may change over time, therefore companies and their counsel should continually reassess risks facing their business and whether those risks are material.
3. In-house counsel and private practitioners were encouraged to "manage, measure, and assess" risks which are anchored in statutory language requiring full and fair disclosure.

The renewed emphasis on requiring the disclosure of risks in the ESG and cybersecurity arenas, especially in conjunction with new guidance that expands what needs to be analyzed, provides additional grounds for the SEC to investigate a company's compliance program and internal controls. Accordingly, companies would be well advised to stay abreast of SEC-issued guidance discussing emerging risks and the disclosures those risks may require."

Explore more in

Corporate Law