Skadden

SEC Reporting & Compliance Alert

Contacts

Brian V. Breheny
Partner / Washington, D.C.
202.371.7180
brian.breheny@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Caroline S. Kim
Associate / Washington, D.C.
202.371.7555
caroline.kim@skadden.com

Four Times Square
New York, NY 10036
212.735.3000

SEC Issues Interpretive Guidance on Cybersecurity Disclosures

On February 21, 2018, the U.S. Securities and Exchange Commission (SEC) issued an interpretive release providing guidance for public companies relating to disclosures of cybersecurity risks and incidents. Although the guidance is unlikely to impact annual reports being filed in the near term, companies may wish to consider the new guidance in connection with preparing their proxy statements for upcoming annual meetings and other SEC filings. In addition, the guidance addresses cybersecurity considerations in connection with company disclosure controls and procedures and insider trading policies. Below is a brief summary of the key takeaways from the new guidance.

Disclosure Matters and Materiality. With respect to disclosure matters, the guidance largely echoes and reaffirms the disclosure guidance issued by the staff of the SEC's Division of Corporation Finance in 2011 (available here). Specifically, companies should consider whether there are material cybersecurity risks and incidents that should be disclosed in registration statements, periodic reports and other filings with the SEC as part of the disclosure of risk factors, management's discussion and analysis of financial condition and results of operations, descriptions of the company's business and legal proceedings, and financial statements and accompanying notes. The SEC emphasized that a company should avoid boilerplate language and tailor its disclosures to its own business and industry, including a discussion of the potential financial, legal or reputational impact of cybersecurity risks or incidents. At the same time, however, the SEC stated that the disclosures should not be so detailed as to compromise a company's cybersecurity efforts.

Notably, the SEC indicated that the test for materiality in the cybersecurity context is the same facts-and-circumstances analysis applicable in other contexts. That is, information is material if there is a substantial likelihood that a reasonable investor would consider such information important in making an investment decision or a reasonable investor would view the information as significantly altering the total mix of information available. Elaborating on these general notions, the SEC stated that materiality of cybersecurity risks and incidents will depend on their nature, extent, potential magnitude and range of harm that an incident could cause.

Also, the SEC noted that while companies may need time to assess the implications of a cybersecurity event, and that the scope of disclosure may be affected by ongoing investigations and cooperation with law enforcement, these considerations do not provide a basis to avoid disclosure of a material cybersecurity incident. In addition, the

SEC encouraged the use of current reports on Form 8-K to make prompt disclosures of material cybersecurity incidents. Finally, the SEC used the guidance to remind companies that, during the process of investigating a cybersecurity incident, companies should consider whether they have a duty to correct prior disclosures that have turned out to have been untrue or to update disclosures that were true at the time of their release but have become materially inaccurate.

Board Risk Oversight. The guidance notes the requirement to disclose in proxy statements the board's role in risk oversight. The SEC stated that disclosure of how the board engages in cybersecurity risk oversight will allow investors to better assess a board's performance in this important area. In light of the guidance, as well as investor calls for such information, companies may wish to take a fresh look at their proxy statement disclosure regarding board oversight of risk and consider addressing or enhancing disclosures regarding board oversight of cybersecurity risks.

Policies and Procedures. The SEC guidance expands on the 2011 staff guidance with respect to company policies and procedures. Specifically, the SEC guidance focuses on disclosure controls and procedures and on company insider trading policies.

Disclosure controls and procedures are designed to ensure that information required to be disclosed is processed and reported to management in a manner that allows for timely decisions regarding disclosure. The guidance states that these controls and procedures should encompass the collection and evaluation of information subject to potential disclosure and that companies should evaluate whether their disclosure controls and procedures are sufficient to ensure that relevant information pertaining to cybersecurity risks and incidents is collected, processed and reported up the chain on a timely basis to allow for management to assess and analyze whether cybersecurity risks and incidents should be disclosed. Further, the SEC states that the adequacy of controls and procedures for identifying cybersecurity incidents and risks, as well as assessing and analyzing their impact, should be taken into account when preparing CEO/CFO certifications of periodic reports and making disclosures regarding the effectiveness of disclosure controls and procedures. In practice, although companies likely have protocols for reporting cybersecurity incidents to increasingly senior levels of management, the SEC guidance indicates that companies should review these protocols to ensure that persons having familiarity with, and responsibility for, a company's SEC disclosure decisions are included in the information flow regarding cybersecurity matters that have the potential to be material to investors.

The SEC guidance describes the fact that it is illegal for insiders to trade securities on the basis of material nonpublic information and that information about a company's cybersecurity incidents and risks has the potential to be material nonpublic information. Accordingly, the SEC is encouraging companies to evaluate whether their insider trading policies are designed to prevent insider trading on the basis of material nonpublic information relating to cybersecurity incidents and risks, and to consider whether restrictions on trading need to be imposed during periods when companies are investigating and assessing the significance of a cybersecurity incident. Again, this guidance appears geared toward ensuring that members of a company's legal team with responsibility for securities law compliance matters are included as part of the information flow regarding cybersecurity matters.

Lastly, the SEC reminds companies of their obligations under Regulation FD, which prohibits selective disclosure of material nonpublic information, which would include the selective disclosure of material cybersecurity risks and incidents.

* * *

The SEC's interpretive release is available here. For additional information regarding the SEC staff's 2011 guidance, see our previous alert available here.