COVINGTON

SEC Adopts New Guidance on Public Company Cybersecurity Disclosures and Insider Trading

March 1, 2018

Capital Markets and Securities

On February 21, 2018, the U.S. Securities and Exchange Commission (the "Commission") approved a statement and interpretive guidance that provides the Commission's views on a public company's disclosure obligations concerning cybersecurity risks and incidents (the "2018 Commission Guidance"). This guidance reinforces and expands upon previous cybersecurity disclosure guidance issued by the Division of Corporation Finance (the "Staff") in October 2011 (the "2011 Staff Guidance"). The 2018 Commission Guidance also focuses on two additional issues: (i) maintenance of comprehensive policies and procedures related to cybersecurity, including sufficient disclosure controls and procedures, and (ii) insider trading in the cybersecurity context.

The 2018 Commission Guidance repeats and expands upon the 2011 Staff Guidance, while also providing additional specific guidance around materiality and a public company's obligation to include discussion of cybersecurity risks and incidents in their periodic reports and registration statements. This includes, among others, providing: specific cybersecurity risk factor disclosure, including with respect to previous or ongoing material cybersecurity incidents; a discussion of the various costs of ongoing cybersecurity programs and responses to ongoing or previous incidents in the company's MD&A; and a discussion of the board of directors' oversight of cybersecurity risk in response to Item 407(h) of Regulation S-K and Item 7 of Schedule 14A. This last item was not addressed in the 2011 Staff Guidance, and underlines the importance of addressing the board's oversight of cybersecurity risks, if material to the company, in the annual proxy statement.

The new guidance puts a sharper emphasis on public companies' obligation to provide timely disclosure of material cybersecurity incidents or risks. The Commission says that it expects a company to make timely disclosure once it is aware of a cybersecurity incident or risk that would be material to investors, with such disclosure to be made at least before any offer and sale of company securities and before directors and officers (and other corporate insiders aware of the cybersecurity matters) trade in company securities. The guidance encourages companies to disclose a material cybersecurity incident even if such incident would not trigger a current report on Form 8-K. The 2018 Commission Guidance also notes that public companies may have a duty to correct prior disclosure that the company determines was untrue at the time it was made, or a duty to update disclosure that becomes materially inaccurate after it is made (although there is conflicting case law on whether such a duty to update exists).

The 2018 Commission Guidance notes that "[c]ompanies are required to establish and maintain appropriate and effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events, including those related to cybersecurity…" The Commission believes that companies must have effective cybersecurity policies, which include disclosure controls and procedures, that are able to discern the materiality of the cybersecurity risk and the likely impact on the company's financial condition and reputation. These policies and procedures should be designed to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, so that senior management can make disclosure decisions. Though under this expanded guidance companies still have the ability to take the time to investigate an incident or potential risk and weigh its materiality, an ongoing internal or external investigation of a cybersecurity incident or potential risk is not, on its own, a sufficient basis to delay disclosure of a material incident.

The 2018 Commission Guidance also emphasizes the heightened sensitivity around insider trading when a public company has an ongoing cybersecurity incident that has not been publicly disclosed. The guidance states that companies "should have policies and procedures in place to (1) guard against directors, officers and other corporate insiders taking advantage of the period between the company's discovery of a cybersecurity incident and public disclosure of the incident to trade on material nonpublic information about the incident, and (2) help ensure that the company makes timely disclosure of any related material nonpublic information." The 2018 Commission Guidance goes on to say that companies should consider what consequences insiders should face as a result of trading prior to the disclosure of a material cybersecurity event. This guidance raises fresh questions for companies in the midst of cybersecurity investigations. Due to the inherent nature of such investigations, it is often difficult to determine definitively when and whether information relating to the cyber incident becomes material.

Conclusion

The impact that the new guidance will have on cybersecurity disclosure practices is unclear. At a minimum, companies should revisit their cybersecurity disclosures to ensure that they are aligned with the new guidance. Although the new guidance has not added much to the mix in terms of how to approach cybersecurity disclosures, some of the new guidance, particularly the guidance regarding the disclosure of board oversight of cybersecurity, is likely to prompt companies to add to their existing disclosures. In addition, we expect companies to think twice on how they handle information regarding cybersecurity incidents in the context of their investor engagement and trading windows. In light of the emphasis that the SEC and its staff have placed on cybersecurity in this release and other statements, one thing is clear—this will not be the last thing that we hear regarding the SEC's expectations regarding cybersecurity.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Capital Markets and Securities practice:

David Engvall	+1 202 662 5307	dengvall@cov.com
Keir Gumbs	+1 202 662 5500	kgumbs@cov.com
Reid Hooper	+1 202 662 5984	rhooper@cov.com
Matthew Wood	+1 202 662 5943	mwood@cov.com