LEGALcurrents®

March 12, 2018

Harter Secrest & Emery LLP

ATTORNEYS AND COUNSELORS

SECURITIES AND CAPITAL MARKETS

PRIVACY AND DATA SECURITY

SEC PUBLISHES UPDATED INTERPRETIVE GUIDANCE ON CYBERSECURITY

On February 21, 2018, the Securities and Exchange Commission (the "SEC") issued interpretive guidance clarifying its views on the cybersecurity-related disclosures that public companies are required to make under federal securities laws. This interpretive guidance will affect all current SEC reporting companies as well as those companies filing their initial registration statement.

Background

The Division of Corporation Finance (the "Division") first issued cybersecurity guidance in October 2011 stating that public companies may be required to disclose cybersecurity risks and incidents despite no specific reference to cybersecurity in the existing disclosure rules. An overview of the Division's October 2011 guidance can be found here. The purposes of the SEC's most recent release were: (i) to reaffirm and expand upon the Division's earlier guidance; (ii) to emphasize the importance of cybersecurity in assessing the effectiveness of disclosure controls and procedures; and (iii) to encourage companies to consider cybersecurity risks and incidents in relation to insider trading prohibitions and the prohibition against selective disclosure of material nonpublic information under Regulation FD.

Disclosure Obligations

The SEC's interpretive guidance described the grave threats that cybersecurity risks pose to investors and the capital markets. The SEC stressed that companies must disclose material cybersecurity risks and incidents in a timely fashion, even though there are still no disclosure rules that explicitly reference cybersecurity. Regarding the timing of disclosures, while the SEC recognized that a company may require time to investigate an incident, an ongoing internal or external investigation is not, on its own, a basis to avoid disclosing a material incident. The SEC noted that there are many existing disclosure requirements that may obligate companies to include information relating to cybersecurity in their filings such as the following:

Risk Factors - Companies should include risk factors describing the risks associated with cybersecurity, including those arising from acquisitions, if such risks are significant. These risk factors should include specific examples of cybersecurity incidents, describing their severity and frequency, if applicable, and should address the likelihood and magnitude of future cybersecurity incidents and any limits the company perceives in its ability to prevent or contain them. The risk factors should describe the costs associated with preventing cybersecurity incidents, including, if applicable, insurance coverage and payments to third-party service providers. The risk factors should also describe existing or pending laws and regulations related to cybersecurity and the anticipated costs to comply with such laws and regulations along with a description of the costs associated with any litigation, regulatory investigations, and remediation costs associated with cybersecurity incidents.

MD&A - The Management Discussion and Analysis of Financial Condition and Results of Operations should include a discussion of expenses relating to ongoing cybersecurity efforts, if material, expenses, and other consequences of cybersecurity incidents, and the risk of potential cybersecurity incidents with respect to the company's financial condition, changes in financial condition, and results of operations. Companies should also consider disclosing potential costs related to the loss of intellectual property, preparing for and complying with proposed or current cybersecurity legislation, responding to litigation and regulatory investigations, and harm to the company's reputation and loss of competitive advantage associated with cybersecurity incidents.

Description of Business - Companies should discuss cybersecurity incidents or risks that materially affect their products, services, relationships with customers or suppliers, or competitive conditions.

Legal Proceedings - Companies must provide disclosure of material pending legal proceedings relating to cybersecurity if they or their subsidiaries are a party.

Financial Statements - Companies must incorporate expenses and financial impacts related to cybersecurity incidents into their financial statements in a timely manner. Such expenses and financial impacts include costs related to investigation, notification, remediation and litigation, loss of revenue, and diminished future cash flows.

Board Risk Oversight - When discussing the board of directors' role in the risk oversight of a company in its proxy statement, the company should also discuss the nature of the board's role in overseeing the management of cybersecurity risks, if material to the company.

Correction of Prior Disclosures - Companies have a duty to correct prior disclosures that become untrue or inaccurate after further investigation.

As with the Division's guidance, the SEC noted that it is not imposing a line-item requirement on public companies, but rather encouraging a principles-based approach in which companies should assess cybersecurity risks and incidents in the context of overall materiality.

Policies and Procedures

The SEC encouraged companies to adopt comprehensive policies and procedures related to cybersecurity risks and incidents and evaluate compliance on a regular basis. Disclosure controls and procedures should be designed to ensure that relevant information about cybersecurity incidents are reported in a timely manner to the appropriate company personnel. Specifically, companies will need to evaluate their processes to ensure that those responsible for responding to a cybersecurity incident, or identifying cybersecurity risks, are communicating with the appropriate disclosure and compliance professionals within the company so that management can assess the materiality of the information and reach timely disclosure decisions. While a specific reference to cybersecurity is not required in the discussion of disclosure controls and procedures in reports filed with the SEC, the SEC encouraged companies to assess their ability to detect and manage cybersecurity risks and incidents as part of their evaluation of disclosure controls and procedures generally. Further, the SEC advised companies that certifications by a company's principal executive officer and principal financial officer about the design and effectiveness of disclosure controls and procedures and

their conclusions about the effectiveness of such disclosure controls and procedures should consider the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact.

Insider Trading and Regulation FD

The SEC reminded companies and their corporate insiders, including directors and officers, that it is illegal to trade securities based on material nonpublic information, including material information relating to cybersecurity risks and incidents. The SEC suggested that companies assess whether their codes of ethics and insider trading policies prevent trading based on material nonpublic information regarding cybersecurity as well as prevent and address the appearance of improper trading. If a company is required by state or foreign cybersecurity laws or regulations to notify customers of cybersecurity incidents, or if contractual provisions require the company to notify counterparties of cybersecurity incidents, then companies should have policies and procedures in place to ensure compliance with Regulation FD by not selectively disclosing material nonpublic information relating to cybersecurity to customers or counterparties before publicly disclosing such information.

What to Do Now

Companies should expect increased scrutiny on their cybersecurity disclosures and policies and procedures and expect increased focus on cybersecurity related matters in SEC comment letters. We recommend that companies consider implementing the following changes:

- Review disclosures in Exchange Act reports or registration statements filed with the SEC in each of the areas identified above and other areas where disclosure of cybersecurity-related matters is relevant. Disclosures should be tailored to the company's specific circumstances and framed in the relevant context, by disclosing previous cybersecurity incidents.
- Ensure proxy disclosures regarding the board's oversight of risk specifically address cybersecurity risks, consider how oversight of cybersecurity risks is accomplished by the board, and update board procedures as necessary considering current circumstances.
- Review governance structures for cybersecurity and enterprise risk management, recognizing that cybersecurity risks are not the exclusive domain of the company's chief information officer or other IT professionals. A company's officers, and ultimately its board, should have a thorough understanding of the company's cybersecurity risks, how the company has responded to cybersecurity risks, and the costs incurred by the company in mitigating these risks. If not already in place, all public companies should seriously consider adopting robust, enterprise-level cybersecurity risk management programs and incident response and disaster recovery plans that are regularly tested.
- Evaluate whether disclosure controls and procedures are adequate to ensure cybersecurity matters are identified, processed, and reported to the appropriate personnel to ensure timely materiality and disclosure decisions by the company's management as reflected in the certifications management submits to the SEC.
- Review insider trading and Regulation FD policies to ensure that they address cybersecurity risks. Specifically, companies may want to consider including cybersecurity-related incidents to the

illustrative list of "material" events that insider trading and Regulation FD policies typically identify. It is also important for the individuals responsible for opening or closing the trading window or preclearing trades under the insider trading policy to receive notice of cybersecurity incidents under the company's cybersecurity incident response plan. Additionally, the company's cybersecurity incident response plan should reflect the need to inform the company's disclosure and compliance personnel and senior management of cybersecurity incidents in order for them to evaluate the materiality of the incident to ensure that disclosure of the cybersecurity incident is made in a Regulation FD compliant manner.

If you would like more information regarding compliance with SEC disclosure rules relating to cybersecurity or best practices for preparing for and avoiding a cybersecurity incident, please contact a member of Harter Secrest & Emery LLP's Securities and Capital Markets Group or Privacy and Data Security Group.