February 27, 2018

SEC Issues Updated Guidance on Cybersecurity Disclosure

On February 21, 2018, the Securities and Exchange Commission (the "SEC") issued an interpretive release providing Commission-level guidance to assist public companies in preparing disclosures concerning cybersecurity risks and incidents. The release supplements guidance provided by the Staff of the SEC's Division of Corporation Finance (the "Staff") in October 2011, and emphasizes the need for comprehensive policies and procedures related to cybersecurity risks and incidents, in order to ensure compliance with disclosure obligations as well as to prevent violations of insider trading laws.

In connection with the interpretive release, SEC Chairman Jay Clayton stated: "[P]roviding the Commission's views on these matters will promote clearer and more robust disclosure by companies about cybersecurity risks and incidents, resulting in more complete information being available to investors. In particular, I urge public companies to examine their controls and procedures, with not only their securities law disclosure obligations in mind, but also reputational considerations around sales of securities by executives."

Background

In October 2011, the Staff issued written guidance (CF Disclosure Guidance: Topic No. 2) setting forth its views regarding disclosure obligations concerning cybersecurity risks and cyber incidents. The 2011 guidance addressed potential disclosure issues in the context of applicable disclosure requirements, including risk factors, MD&A, business description, legal proceedings, financial statement disclosure, and disclosure controls and procedures. In recent years, the SEC has in some cases directed registrants to consider disclosure of information concerning cybersecurity issues as part of comment letters issued in respect of registration statements and periodic reports.

As noted in the newly released guidance, cybersecurity threats can result from unintentional events or deliberate attacks by insiders or third parties, including cybercriminals, competitors, nation-states and "hacktivists." Cyberattacks vary significantly and may include the theft or destruction of financial assets, intellectual property or other sensitive information belonging to companies, their customers or their business partners, or disrupting the operations of public companies or their business partners. The increase in frequency and scope of cyberattacks may raise the costs and potential negative consequences for companies, including remediation costs, increased cybersecurity protection costs, lost revenues, litigation and legal risks, increased insurance premiums, reputational damage that adversely affects customer or investor confidence and damage to the company's competitiveness, stock price and long-term shareholder value.

Interpretive Guidance

Rules Requiring Disclosure of Cybersecurity Issues. In the release, the SEC provides guidance with respect to a number of cybersecurity disclosure issues, in large part building upon the Staff's 2011 guidance.

- Disclosure Obligations Generally; Materiality. The SEC states that registrants should consider the materiality of cyber risks and incidents when preparing the disclosure that is required in registration statements and periodic and current reports. As described in the release, the materiality of cyber risks or incidents depends upon their nature, extent and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations. Materiality also depends on the range of harm that cyber incidents could cause, which can include harm to a company's reputation, financial performance and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions.

  In the release, the SEC notes that an ongoing internal or external investigation would not on its own provide a basis for avoiding disclosure of a material cyber incident. It also clarifies that the guidance is not intended to suggest that a registrant should make detailed disclosures that could compromise its cybersecurity efforts—for example, by providing a "roadmap" for those who seek to penetrate a company's security protections. The release also notes that registrants should avoid generic cybersecurity-related disclosure while providing specific information that is useful to investors.

  The guidance reminds registrants that, as they develop additional facts about a cyber incident, they may have a duty to correct or update prior disclosure. This could well be the case if a registrant determines that prior disclosure was untrue (or omitted a material fact necessary to make the disclosure not misleading) at the time it was made (for example, if the registrant subsequently discovers contradictory information that existed at the time of the initial disclosure), or has a duty to update disclosure that becomes materially inaccurate after it is made (for example, when the original statement is still being relied upon by reasonable investors). The SEC reminds registrants that they should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident.

- Risk Factors. Registrants should disclose significant risks associated with cybersecurity and cyber incidents, including risks that arise in connection with acquisitions. Registrants should consider the following issues, among others, in evaluating cybersecurity risk factor disclosure:

  - the occurrence of prior cyber incidents, including their severity and frequency;

  - the probability of the occurrence and potential magnitude of cyber incidents;

- the adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including, if appropriate, discussing the limits of the registrant's ability to prevent or mitigate certain cybersecurity risks;

- the aspects of the registrant's business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks, including industry-specific risks and third-party supplier and service provider risks;

- the costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cyber incidents or payments to service providers;

- the potential for reputational harm;

- existing or proposed laws and regulations that may affect the requirements to which the registrant is subject relating to cybersecurity and the associated costs of compliance; and

- litigation, regulatory investigation and remediation costs associated with cyber incidents.

The SEC notes that in meeting their disclosure obligations, registrants may need to disclose previous or ongoing cyber incidents or other past events in order to place discussions of these risks in the appropriate context.

Registrants are also reminded that prior incidents involving suppliers, customers, competitors and others may be relevant when drafting risk factors.

- MD&A. The guidance notes that the costs of ongoing cybersecurity efforts (including enhancements to existing efforts), the costs and other consequences of cyber incidents, and the risks of potential cyber incidents, among other matters, could inform a company's MD&A. In addition, registrants may consider the array of costs associated with cybersecurity issues, including, but not limited to, loss of intellectual property, the immediate costs of the incident, the costs associated with implementing preventative measures, maintaining insurance, responding to litigation and regulatory investigations, preparing for and complying with current or proposed legislation, engaging in remediation efforts, and addressing harm to reputation and the loss of competitive advantage that may result. Notably, the SEC expects registrants to consider the impact of such incidents on each of their reportable segments.

- Description of Business. If cyber incidents or risks materially affect a registrant's products, services, relationships with customers or suppliers or competitive conditions, it must provide appropriate disclosure.

- Legal Proceedings. Item 103 of Regulation S-K requires registrants to disclose information relating to material pending legal proceedings in which they or their subsidiaries are parties. This requirement includes any such proceedings that relate to cybersecurity issues. For example, if a registrant experiences a cyber incident involving the theft of customer information and the incident results in material litigation by customers against the company, the registrant should describe the litigation, including the name of the court in which the proceedings are pending, the date the proceedings are instituted, the principal parties thereto, a description of the factual basis alleged and the relief sought.

- Financial Statement Disclosures. Cyber incidents may affect a registrant's financial statements. The SEC expects that a registrant's financial reporting and control systems would be designed to provide reasonable assurance that information about the range and magnitude of the financial impacts of a cyber incident would be reflected in its financial statements on a timely basis as the information becomes available. Financial statements could be impacted by costs related to investigations, remediation, notice of breaches and litigation; loss of revenue; warranty claims; increases in insurance premiums; and impairment of assets and diminished cash flow.

- Board Risk Oversight. To the extent cybersecurity risks are material to a registrant's business, the SEC believes this discussion should include the nature of the board's role in overseeing the management of that risk.

Disclosure Controls and Procedures. In the release, the SEC notes that cybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including as they relate to compliance with the federal securities laws. Registrants should assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and certifications and to facilitate policies and procedures designed to prohibit directors, officers and other corporate insiders from trading on the basis of material nonpublic information about cybersecurity risks and incidents.

Registrants should consider whether their disclosure controls and procedures will appropriately record, process, summarize and report the information related to cybersecurity risks and incidents that is required to be disclosed in filings. Controls and procedures should enable registrants to identify cybersecurity risks and incidents, assess and analyze their impact on a registrant's business, evaluate the significance associated with such risks and incidents, provide for open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents. The focus on disclosure controls and procedures is consistent with the view of the Staff that cyber issues need to be elevated from the IT department to those tasked with assessing the need for public disclosure.

Exchange Act Rules 13a-14 and 15d-14 require a registrant's principal executive officer and principal financial officer to make certifications regarding the design and effectiveness of disclosure controls and

procedures, and Item 307 of Regulation S-K and Item 15(a) of Exchange Act Form 20-F require registrants to disclose conclusions on the effectiveness of disclosure controls and procedures. These certifications and disclosures should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact.

Insider Trading. The SEC's guidance cautions that information about a registrant's cybersecurity risks and incidents can constitute material nonpublic information and that, therefore, directors, officers and other corporate insiders could violate the antifraud provisions of the securities laws by trading securities while in possession of such information. In the release, the SEC notes that registrants should maintain well designed policies and procedures to prevent trading on the basis of all types of material nonpublic information, including information relating to cybersecurity risks and incidents. In the case of cyber incidents, the relevant period during which material information would be considered nonpublic would be between the time the registrant discovers the incident and the public disclosure of the incident.

The SEC suggests that while registrants are investigating significant cybersecurity incidents, determining the underlying facts and assessing the ramifications and materiality of these incidents, registrants should consider whether and when it may be appropriate to implement restrictions on insiders trading in their securities. The SEC notes that such a restriction on trading not only serves to prevent insider trading, but also to avoid even the appearance of improper trading.

Regulation FD and Selective Disclosure. Under Regulation FD, when a domestic reporting company, or person acting on its behalf, discloses material nonpublic information to certain enumerated persons, it must make public disclosure of that information. The SEC reminds registrants of their obligations to refrain from making selective disclosures of material nonpublic information about cybersecurity risks and incidents. The SEC also notes that it expects registrants to have policies and procedures in place to ensure that any disclosures of material nonpublic information regarding cybersecurity risks and incidents are not made selectively.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Mark S. Bergman
+44-20-7367-1601
mbergman@paulweiss.com

Andrew J. Foley
+1-212-373-3078
afoley@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

David S. Huntington
+1-212-373-3124
dhuntington@paulweiss.com

Jeh Charles Johnson
+1-212-373-3093
jjohnson@paulweiss.com

Lorin L. Reisner
+1-212-373-3250
lreisner@paulweiss.com

Raphael M. Russo
+1-212-373-3309
rrusso@paulweiss.com

Richard C. Tarlowe
+1-212-373-3035
rtarlowe@paulweiss.com

Hank Michael
+1-212-373-3892
hmichael@paulweiss.com

Associates Chand Edwards-Balfour and Agbeko C. Petty contributed to this Client Memorandum.