SEC Issues Guidance on Public Company Cybersecurity Disclosures

The guidance outlines the SEC's views regarding cybersecurity disclosure obligations and highlights the importance of cybersecurity policies and procedures.

On February 21, 2018, the U.S. Securities and Exchange Commission (SEC) published updated interpretive guidance to assist public companies in preparing disclosures regarding cybersecurity risks and incidents. The guidance reinforces and expands upon the SEC staff's guidance issued in October 2011, CF Disclosure Guidance: Topic No. 2 – Cybersecurity. The guidance outlines the SEC's views on disclosure obligations regarding cybersecurity risk and incidents under existing U.S. federal securities laws. In addition, the guidance addresses the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the cybersecurity context.

To read the SEC's full guidance, click here.

Disclosure Obligations Generally and Materiality

The guidance states that companies should consider the materiality of cybersecurity risks and incidents when making disclosures required in registration statements under the Securities Act of 1933 (Securities Act) and registration statements and periodic and current reports under the Securities Exchange Act of 1934 (Exchange Act), as well as any disclosure obligations imposed by the listing requirements of any applicable national securities exchange. The guidance notes that although line-item disclosure requirements set forth in Regulation S-K and Regulation S-X do not specifically refer to cybersecurity risks and incidents, U.S. federal securities laws impose an obligation to disclose cybersecurity risks and incidents depending on the particular circumstances, including as may be required by Exchange Act periodic reports, Securities Act and Exchange Act registration statements and Exchange Act current reports. In addition to the information, a public company is required to disclose "such further material information, if any, as may be necessary to make the required statements, in light of the circumstances under which they are made, not misleading." In evaluating disclosure obligations regarding cybersecurity risks and incidents, public companies generally weigh, among other things, the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact of the incident on the company's operations. The materiality of cybersecurity 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. The materiality of cybersecurity risks and incidents also depends on the range of harm that such incidents could cause, including harm to reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions. The guidance does not suggest that a public company should make detailed disclosures that could compromise its cybersecurity efforts (e.g., by providing a "roadmap" for cybersecurity attackers). The guidance recognizes that it may take time for a public company to discern the implications of a cybersecurity incident. The guidance also recognizes that while an ongoing internal or external investigation can be lengthy, such an investigation on its own would not provide a basis for avoiding disclosures of a material cybersecurity incident. The SEC staff expects companies to

provide disclosure that is tailored to their particular cybersecurity risks and incidents and to provide specific information that is useful to investors rather than generic cybersecurity-related disclosure.

Risk Factors

The guidance notes that Item 503(c) of Regulation S-K and Item 3.D of Form 20-F require public companies to disclose the most significant factors that make investments in their securities speculative or risky. Companies should disclose the risks associated with cybersecurity and cybersecurity incidents if these risks are among these factors. The guidance provides the following non-exhaustive list of issues for companies to consider when evaluating cybersecurity risk factor disclosure:

- the occurrence of prior cybersecurity incidents, including their severity and frequency;
- the probability of the occurrence and potential magnitude of cybersecurity incidents;
- the adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including, if appropriate, discussing the limits of the company's ability to prevent or mitigate certain cybersecurity risks;
- the aspects of the company'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 cybersecurity incidents or payments to service providers;
- the potential for reputational harm;
- existing or pending laws and regulations that may affect requirements to which public companies are subject relating to cybersecurity and the associated costs to companies; and
- litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents.

MD&A, Description of Business, and Legal Proceedings

The guidance notes that Item 303 of Regulation S-K and Item 5 of Form 20-F require a public company to provide a management's discussion and analysis of financial condition and results of operations (MD&A), including events, trends, or uncertainties that are reasonably likely to have a material effect on its results of operations, liquidity, or financial condition, or that would cause reported financial information not to be necessarily indicative of future operating results or financial condition and such other information that the company believes to be necessary to an understanding of its financial condition, changes in financial condition, and results of operations. Companies should consider the costs of actions taken both to prevent cybersecurity incidents and

to respond to incidents that have already occurred (e.g., maintaining insurance, litigation and regulatory investigations, mitigating harm to reputation or competitive advantage, preparing for and complying with current or proposed regulations, and enhancing existing cybersecurity efforts).

The guidance notes that Item 101 of Regulation S-K and Item 4.B of Form 20-F require public companies to discuss their products, services, relationships with customers and suppliers, and competitive conditions. Any cybersecurity risks or incidents that may materially affect a company's business or relationships with its customers, suppliers, and competitors must be appropriately disclosed pursuant to these items.

The guidance further notes that Item 103 of Regulation S-K requires companies to disclose information relating to material pending legal proceedings to which they or their subsidiaries are a party. This requirement includes any such proceedings that relate to cybersecurity issues.

Financial Statement Disclosures

The guidance notes that cybersecurity incidents and the risks that result therefrom may affect a public company's financial statements. For example, cybersecurity incidents may result in:

- expenses related to investigation, breach notification, remediation and litigation, including the costs of legal and other professional services;
- loss of revenue, providing customers with incentives or a loss of customer relationship assets value;
- claims related to warranties, breach of contract, product recall/replacement, indemnification of counterparties, and insurance premium increases; and
- diminished future cash flows, impairment of intellectual, intangible or other assets, recognition of liabilities, or increased financing costs.

The SEC expects that a company'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 cybersecurity incident would be reflected in its financial statements on a timely basis as the information becomes available.

Board Risk Oversight

The guidance notes that Item 407(h) of Regulation S-K and Item 7 of Schedule 14A require disclosure of the board's role in risk oversight of the company. To the extent cybersecurity risks are material to the company's business, the SEC staff believes this discussion should include the nature of the board's role in overseeing the management of such risks. The SEC staff also believes disclosures regarding the company's cybersecurity risk management program and how the board engages with management on cybersecurity issues would allow investors to assess how the board is discharging its risk oversight responsibility.

Disclosure Controls and Procedures

The guidance encourages public companies to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure. The guidance reminds public companies that they are required to maintain disclosure controls and procedures pursuant to Exchange Act rules 13a-15 and 15d-15 and that their management must evaluate their effectiveness. These disclosure controls and procedures should not be limited to disclosure specifically required, but should also ensure timely collection and evaluation of information potentially subject to required disclosure, or relevant to an assessment of the need to disclose developments and risks that pertain to the company's businesses. When designing and evaluating disclosure controls and procedures, companies should consider whether such 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. In addition, certifications and disclosures required under Exchange Act rules 13a-14 and 15d-14, Item 307 of Regulation S-K and Item 15(a) of Form 20-F should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact. To the extent cybersecurity risks or incidents pose a risk to a company's ability to record, process, summarize, and report information that is required to be disclosed in filings, management should consider whether there are deficiencies in disclosure controls and procedures that would render them ineffective.

Insider Trading and Regulation FD

The guidance reminds public companies and their directors, officers and other corporate insiders of the need to comply with insider trading laws when information about cybersecurity risks and incidents (including vulnerabilities and breaches) becomes available. The guidance notes that information about cybersecurity risks and incidents may be material nonpublic information.

The guidance also reminds public companies and their directors, officers and other corporate insiders of the need to comply with applicable insider trading-related rules, including consideration of how their codes of ethics and insider trading policies take into account and prevent trading on the basis of material nonpublic information related to cybersecurity risks and incidents. In addition, if a company is investigating and assessing a significant cybersecurity incident, the company should consider whether and when it may be appropriate to implement restrictions on insider trading in the company's securities.

Public companies are also reminded that they may have disclosure obligations under Regulation FD in connection with cybersecurity matters. The SEC staff expects companies to have policies and procedures to ensure that any disclosures of material nonpublic information related to cybersecurity risks and incidents are not made selectively under Regulation FD.

* * * * *

About Curtis

Curtis, Mallet-Prevost, Colt & Mosle LLP is a leading international law firm. Headquartered in New York, Curtis has 17 offices in the United States, Latin America, Europe, the Middle East and Asia. Curtis represents a wide range of clients, including multinational corporations and financial institutions, governments and state-owned companies, money managers, sovereign wealth funds, family-owned businesses, individuals and entrepreneurs.

For more information about Curtis, please visit www.curtis.com.

Attorney advertising. The material contained in this client alert is only a general review of the subjects covered and does not constitute legal advice. No legal or business decision should be based on its contents.

For further information, contact:

Jeffrey N. Ostrager
Partner
jostrager@curtis.com
212.696.6918

Valarie A. Hing
Partner
vhing@curtis.com
212.696.6943

Raymond T. Hum
Partner
rhum@curtis.com
202.452.7358

Brendan A. Klaassen
Associate
bklaassen@curtis.com
212.696.6110