SEC Issues Further Guidance on Cybersecurity Disclosure

On February 21, 2018, the Securities and Exchange Commission (the "Commission") released interpretive guidance to assist public companies in complying with federal securities law disclosure requirements as they relate to cybersecurity risks and incidents (the "Release").[1] The Release reaffirms and expands on guidance issued by the Division of Corporation Finance in 2011 (the "2011 Guidance")[2], which called upon publicly traded companies to consider the materiality of cybersecurity risks and incidents when preparing the disclosures that are required in filings under the Securities Act of 1933 (the "Securities Act") or the Securities Exchange Act of 1934 (the "Exchange Act") (collectively, the "Securities Laws"). In addition to disclosure, the Release discusses the importance of implementing cybersecurity-related policies and procedures and the application of insider trading prohibitions in the cybersecurity context.

I. Disclosure

After an introduction that defines cybersecurity and contextualizes the related risks using currently available research, the Release reviews in detail the specific disclosure obligations that may require a discussion of cybersecurity risks and incidents, including risk factors, management's discussion and analysis of financial condition and results of operations ("MD&A"), description of business, legal proceedings, financial statement disclosures, and board risk oversight, as further described below.

1. Disclosure Obligations Generally; Materiality

In evaluating whether to disclose cybersecurity risks and incidents, the Release notes that companies should 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 the incident's effect on the company's operations. The Release stresses that the materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, specifically as they relate to compromised information or the business and scope of company operations.

The Release emphasizes that companies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors. The Commission expects companies to disclose cybersecurity risks and incidents that are material to investors, including their corresponding financial, legal, or reputational consequences. However, the Commission does not expect companies to publicly disclose specific, technical information regarding their cybersecurity systems in such detail that would result in such systems becoming more susceptible to a cybersecurity incident.

Recognizing that it may take time to determine the implications of a cybersecurity incident, the Commission cautions that the mere existence of an ongoing internal or external investigation would not provide a basis for avoiding disclosure. The Commission specifically states that it expects a company to make disclosure of any material cybersecurity incident "timely and sufficiently prior" to any offering of securities. Further, it expects

---

[1] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018), *available at* http://sec.gov/rules/interp/2018/33-10459.pdf.

[2] *See* CF Disclosure Guidance: Topic No. 2-Cybersecurity (Oct. 13, 2011), *available at* https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. *See also* SEC Provides Guidance on Cybersecurity Risks and Cyber Incidents (Oct. 21, 2011), *available at* https://www.cahill.com/publications/firm-memoranda/1012934.

directors and officers to be prevented from trading until investors are informed about the incident.[3] While noting relevant case law on the duty to update disclosure[4], the Commission urges companies to consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity event.

2. Risk Factors

In accordance with the Securities Laws, a company must disclose the most significant factors that make investments in the company's securities speculative or risky.[5] The Commission cautions that general disclosures of risk may be insufficient without the context provided by discussing past cybersecurity incidents. In evaluating cybersecurity risk factor disclosure, the Release expands on the 2011 Guidance by outlining the following factors to be considered:

- the occurrence of prior cybersecurity incidents, including their severity and frequency;
- the probability of occurrence and potential magnitude of cybersecurity incidents;
- the adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including, if appropriate, 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, the insurance coverage relating to cybersecurity incidents or payments to service providers;
- the potential for reputational harm;
- the existing or pending law and regulations that may affect the requirements to which companies are subject relating to cybersecurity and the associated costs; and
- litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents.

3. MD&A

In the preparation of MD&A, the Release encourages companies to consider the array of costs that may be associated with cybersecurity risks and incidents, including, but not limited to, any loss of intellectual property, the immediate costs of the incident, as well as the costs associated with implementing preventative measures, maintaining insurance, responding to litigation and regulatory investigations, preparing for and complying with proposed or current legislation, engaging in remediation efforts, addressing harm to reputation, and any loss of

[3] *See* Sections 7 and 10 of the Securities Act; Sections 10(b), 13(a) and 15(d) of the Exchange Act; and Rule 10b-5 under the Exchange Act [15 U.S.C. 78j(b); 15 U.S.C. 78m(a); 15 U.S.C. 78o(d); 17 CFR 240.10b-5].

[4] *See* Footnotes 36 and 37 in the Release.

[5] 17 CFR 229.503(c); 17 CFR 249.220f.

competitive advantage that may result.[6] The Commission expects companies to consider the impact of such incidents on each of their reportable segments.[7]

4. Financial Statements

The Commission expects a company's financial reporting and control systems to provide reasonable assurances that information about the range and magnitude of the financial impacts of a cybersecurity incident are incorporated into its financial statements on a timely basis. The Release identifies the following financial repercussions that may result from a cybersecurity incident:

- expenses related to investigation, breach notification, remediation, and litigation, including the costs of legal and other professional services;
- loss of revenue, cost of providing customers with incentives or loss of value of customer relationships;
- 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, tangible or other assets, recognition of liabilities, or increased financing costs.

5. Board Risk Oversight

Disclosures regarding the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing material risks facing the company. To the extent cybersecurity risks are material to a company's business, the Release reiterates the Commission's belief that this discussion should include the nature of the board's role in overseeing management of those risks.

6. Other Specific Disclosures

The Release reminds companies that disclosures regarding legal proceedings and the description of the company's business should also describe material cybersecurity matters. Any material cybersecurity-related litigation and proceedings should be described, including the name of the court in which such proceedings are pending, the date such proceedings were instituted, the principal parties thereto, the factual basis alleged to underlie such litigation or proceedings, and the relief sought. Further, any material impact of cybersecurity incidents or risks on the company's products, customers and suppliers should be disclosed.

---

[6] A number of past Commission releases provide general interpretive guidance on these disclosure requirements. *See, e.g.*, Commission Guidance Regarding Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 33-8350 (Dec. 19, 2003) [68 FR 75056 (Dec. 29, 2003)]; Commission Statement About Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 33-8056 (Jan. 22, 2002) [67 FR 3746 (Jan. 25, 2002)]; Management's Discussion and Analysis of Financial Condition and Results of Operations; Certain Investment Company Disclosures, Release No. 33-6835 (May 18, 1989) [54 FR 22427 (May 24, 1989)].

[7] 17 CFR 229.303(a).

II. Policies and Procedures

The Commission encourages 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. The Commission explains that officer certifications regarding disclosure controls should take into account the policies and procedures related to cybersecurity risks and incidents. In addition, management should correct any deficiencies in these policies and procedures that would impact the ability to make timely disclosures of material risks and incidents. In the Commission's view, effective controls and procedures should enable a company to identify a risk or incident, analyze its impacts on the business, evaluate its significance in open communications between technical experts and disclosure advisors, and make timely disclosure. The Commission also notes that policies and procedures must be designed to enable management to prevent directors, officers and insiders from trading prior to public disclosure of material information regarding cybersecurity risks and incidents.

III. Insider Trading and Regulation FD

The Commission reminds companies that information about a company's cybersecurity risks and incidents may be material nonpublic information. Therefore, directors, officers and other corporate insiders would violate antifraud provisions of the federal securities laws if they were to trade the company's securities in breach of their duty of trust or confidence while in possession of that material nonpublic information. The Release encourages companies to consider how their codes of ethics[8] and insider trading policies take into account and prevent trading on the basis of material information regarding nonpublic cybersecurity risks and incidents and avoid even the appearance of improper trading following an incident and prior to disclosure. The Release also emphasizes that companies and persons acting on their behalf should not selectively disclose material, nonpublic information regarding cybersecurity risks and incidents to Regulation FD-enumerated persons[9] before disclosing that same information to the public.[10]

IV. Conclusion

As highlighted in statements made by Commissioners Jackson and Stein following the Release, public companies, investors, and other market participants increasingly view confronting and mitigating cybersecurity risks as a major priority requiring more comprehensive action.[11] Globally, the average cost of cybercrime has

[8] Item 406 of Regulation S-K [17 CFR 229.406].

[9] Regulation FD applies generally to selective disclosure made to persons outside the issuer who are (1) brokers or dealers or persons associated with brokers or dealers; (2) investment advisors or persons associated with investment advisors; (3) investment companies or persons affiliated with investment companies; or (4) holders of the issuer's securities under circumstances which it is reasonably foreseeable that such persons will trade in the issuer's securities on the basis of the information. 17 CFR 243.100(b)(1).

[10] Final Rule: Selective Disclosure and Insider Trading, Release No. 34-43154 (Aug. 15, 2000) [65 FR 51716 (Aug. 24, 2000)].

[11] Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018), *available at* https://www.sec.gov/news/public-statement/statement-stein-2018-02-21 (supporting the release of additional guidance as it relates to cybersecurity issues, but urging the Commission to do even more). *See also* Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018), *available at* https://www.sec.gov/news/public-statement/statement-jackson-2018-02-21 (supporting the release of additional guidance but advocating for more comprehensive guidance).

increased 62% over the last five years[12], and it is estimated that cybercrime will cost businesses approximately $6 trillion per year on average through 2021.[13]

Given the growing incidence, severity, and impact of cyberattacks, the Commission is likely to take further action to assist companies in providing investors with detailed, company-specific disclosures and in formulating policies and procedures relating to cybersecurity risks and incidents. The likelihood of further Commission action will increase if the timeliness, breadth and depth of disclosure of cybersecurity risks and incidents does not improve after the Release, as Commissioner Stein points out was the case in response to the 2011 Guidance. Further Commission action may take the form of providing more comprehensive or rigorous guidance or seeking new legislation to mandate specific disclosure requirements or adoption of policies or practices. In order to reflect the urgency and the importance to the Commission of addressing cybersecurity issues, the Commission may be more apt to pursue cybersecurity-related enforcement actions. The Release presents public companies with an opportunity to reassess their disclosures and the adequacy of their policies and procedures to ensure compliance with the Securities Laws.

* * *

If you have any questions about the issues addressed in this memorandum, or if you would like a copy of any of the materials mentioned in it, please do not hesitate to call or email Helene Banks at 212.701.3439 or hbanks@cahill.com; Bradley J. Bondi at 202.862.8910 or bbondi@cahill.com; Charles A. Gilman at 212.701.3403 or cgilman@cahill.com; Geoffrey E. Liebmann at 212.701.3313 or gliebmann@cahill.com; or Enia Gyan at 212.701.3472 or egyan@cahill.com.

[12] *See* Cost of Cyber Crime Study: Insights on the Security Investments that Make a Difference, Accenture (2017), *available at* https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

[13] *See* Nick Eubanks, "The True Cost of Cybercrime For Businesses," *Forbes* (Jul. 13, 2017), *available at* https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#6c0453c44947.