WILLKIE FARR & GALLAGHER LLP

CLIENT ALERT

Beyond Disclosure: SEC Reinforces Public Company Cybersecurity Obligations

February 27, 2018

AUTHORS

Elizabeth P. Gray | Athena Eastwood | Neal E. Kumar | Philip F. DiSanto
Marc J. Lederer

On February 21, 2018, the Securities and Exchange Commission ("**SEC**") published long-anticipated interpretive guidance concerning the disclosures that public companies must make about cybersecurity risks and incidents (the "**Guidance**").[1] The Guidance clarifies for the first time that the SEC expects public reporting companies to develop and maintain comprehensive policies and procedures related to cybersecurity, as well as appropriate and effective disclosure controls to satisfy their obligations under federal securities laws.[2] At least one Commissioner stated in connection with the release that the SEC should do more to encourage companies to adopt comprehensive cybersecurity programs. The Guidance reinforces SEC Chairman Clayton's view that cybersecurity is a corporate governance as well as information technology issue in which senior officers and public company boards must be actively involved.[3]

With respect to disclosure obligations, the Guidance largely reaffirms the Division of Corporation Finance's October 2011 guidance concerning the disclosure of material cybersecurity risks and incidents (the "**2011 Guidance**").[4] The Guidance also reminds companies that insiders must not trade on nonpublic information regarding cybersecurity risks and incidents.

1 Willkie Farr & Gallagher published a summary of the Guidance on February 23, 2018.

2 SEC-regulated financial institutions, such as SEC registered investment companies, SEC-registered investment advisers and SEC-registered broker-dealers are already subject to the information safeguarding requirements of Regulation S-P, 17 C.F.R. Part 248.

3 For more information, please see our previous client alert, "Companies Face a Maze of Cybersecurity Regulations and Heightened Risk Management" (July 27, 2017), available here.

4 CF Disclosure Guidance: Topic No. 2 – Cybersecurity, SEC Division of Corporation Finance (Oct. 13, 2011), available here.

SEC Expects Comprehensive Cybersecurity Policies and Procedures

The Guidance specifically 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 disclosure." The Guidance points out that Exchange Act Rules 13a-15 and 15d-15 require companies obligated to make public filings to maintain disclosure controls and procedures, and management must evaluate their effectiveness.[5] The Guidance goes on to state that "companies 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."

The Guidance addresses the need for disclosure controls and procedures to assess cyber risk and breaches. In addressing the disclosure controls and procedures, the Guidance notes that they should be designed to "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." Such controls and procedures should also appropriately record, process, summarize, and report the information related to cybersecurity risks and incidents that is required to be disclosed in filings. For cyber breaches, the Guidance states that such controls and procedures should "enable companies to identify cybersecurity risks and incidents, assess and analyze their impact on a company'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."[6]

In addition, the Guidance notes that certifications and disclosures required under the Exchange Act rules and forms,[7] and under Regulation S-K,[8] should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact. Furthermore, "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

---

5 Exchange Act Rules 13a-15 and 15d-15 define "disclosure controls and procedures" as those controls and other procedures designed to ensure that information required to be disclosed by the company in the reports that it files or submits under the Exchange Act is (1) "recorded, processed, summarized and reported, within the time periods specified in the Commission's rules and forms," and (2) "accumulated and communicated to the company's management . . . as appropriate to allow timely decisions regarding required disclosure."

6 Guidance at 20.

7 Exchange Act Rules 13a-14 and 15d-14 (17 CFR 240.12b-20); Item 15(a) of Exchange Act Form 20-F.

8 Item 307 of Regulation S-K.

disclosed in filings, management should consider whether there are deficiencies in disclosure controls and procedures that would render them ineffective."[9]

New Details on Cybersecurity Disclosure Obligations

The Guidance "reaffirms" and "expands upon" the SEC's 2011 Guidance concerning disclosure obligations related to cybersecurity risks and incidents. In general, the Guidance reaffirms that companies should weigh the nature, extent, and potential magnitude of any cybersecurity risk or incident in weighing the materiality of those risks or incidents. The Guidance also notes that companies should weigh reputational harm, competitive harm, and litigation or regulatory risks related to cybersecurity in determining materiality.[10] Disclosures should be "*tailored*" to the company's specific risk profile, and companies should "avoid *generic* cyber-related disclosure."[11] Nevertheless, the SEC acknowledges that disclosure need not include *technical* details that could "compromise [the company's] cybersecurity efforts" or provide a "roadmap" for those who seek to penetrate a company's security protections.[12]

Notable new details concerning specific disclosure obligations include the following:[13]

- **Risk Factors:** A company is expected to disclose information about (1) the "adequacy" of cybersecurity protections and "limits" on a company's ability to prevent or mitigate cybersecurity risks, (2) costs associated with maintaining cybersecurity protections, (3) laws or regulations that may affect cybersecurity costs, (4) the potential for "reputational harm" to the company, and (5) litigation, investigations, or remediation costs associated with cybersecurity incidents.

- **MD&A of Financial Conditions and Results of Operations:** A company should consider in preparing its MD&A actual or potential costs associated with preventative measures, insurance coverage, litigation and regulations, remediation efforts, and reputational or competitive harms arising from cybersecurity risks or incidents.

- **Board Risk Oversight:** A company is expected to disclose information concerning its board of directors' role in cybersecurity risk management and engagement with management on cybersecurity issues, if cybersecurity risks are material to the company's business.

---

9 Guidance at 20.

10 *Id.* at 11-12.

11 *Id.* at 11-13 (emphasis added).

12 *Id.* (emphasis added).

13 This is a non-exhaustive list of changes from the SEC's 2011 Guidance concerning disclosure obligations.

The Guidance also recognizes that some time may be necessary to "discern the implications of a cybersecurity incident," including to cooperate with law enforcement when necessary, but that companies should not delay the disclosure of material risks and incidents based solely on the existence of an ongoing internal or external investigation.

Reminder of Insider Trading Prohibition and Regulation FD Compliance

The Guidance includes a reminder that the prohibition of insider trading applies to information regarding cybersecurity risks and breaches.[14] That is, a company's cybersecurity vulnerabilities or breaches may represent material nonpublic information, in which case, insiders would violate securities laws if they traded the company's securities based upon the information in breach of their duty of trust and confidence.

The SEC also notes that exchanges may require companies to adopt codes of conduct that address, among other topics, insider trading. Therefore, the SEC expects companies' insider trading policies and procedures to address "*information relating to cybersecurity risks and incidents*."[15] These policies and procedures should include "prophylactic measures" to prevent company insiders from trading on the basis of material nonpublic information before disclosure of a cybersecurity incident.

In addition, the Guidance reminds companies of their need to make public disclosures under Regulation FD if a company selectively discloses material nonpublic information related to cybersecurity issues to "enumerated persons." The scope of enumerated persons includes: (1) a broker or dealer; (2) an investment adviser; (3) an investment company; or (4) a holder of the issuer's securities when it is reasonably foreseeable that the person will trade the issuer's securities on the basis of the information.[16] The SEC notes that it expects companies to have policies and procedures in place to ensure compliance with Regulation FD in the context of information concerning cybersecurity risks and incidents.

Conclusion

The Guidance indicates that public companies need to take several steps with respect to their cybersecurity programs. First, the SEC expects companies to have a cybersecurity program in place, and for the program to be adequately sophisticated to address risks and disclose breaches. Second, companies should have robust procedures and controls to ensure compliance with their disclosure obligations. Third, disclosure of cyber risk should include the adequacy of the controls used to prevent breaches, costs to maintain the protections, and costs in the event of a breach. Importantly, if cyber risks are material to a company's business, the disclosure should include the role of the board of directors in

[14] The SEC's 2011 Guidance did not address insider trading related to cybersecurity.

[15] Guidance at 22 (emphasis added).

[16] Persons associated with a broker, dealer, investment advisor, or investment company would also be enumerated persons.

cybersecurity risk management. Finally, companies should have policies and procedures in place that address insider trading and Regulation FD as they relate to cyber issues.

If you have any questions regarding this client alert, please contact the following attorneys or the attorney with whom you regularly work.

Elizabeth P. Gray
202 303 1207
egray@willkie.com

Athena Eastwood
202 303 1212
aeastwood@willkie.com

Neal E. Kumar
202 303 1143
nkumar@willkie.com

Philip F. DiSanto
212 728 8534
pdisanto@willkie.com

Marc J. Lederer
212 728 8624
mlederer@willkie.com