Akin Gump
STRAUSS HAUER & FELD LLP

Cybersecurity, Privacy & Data Protection Alert

February 28, 2018

Key Points

- Disclosures must inform investors about material cybersecurity risks and incidents, including addressing material cybersecurity risks for cyber-attacks that have not yet occurred.
- Comprehensive policies and procedures related to cybersecurity risks and incidents, including systems to help gauge the impact of these issues on their business and a protocol to determine materiality, are now mandatory for public companies.
- Insider trading policies of public companies should address and actively protect against misuse of material nonpublic information related to cybersecurity risks and incidents. They should also consider adopting prophylactic measures to cease trading during certain sensitive periods related to cybersecurity incidents to avoid the appearance of impropriety.

Revised SEC Guidance Concerning Disclosure of Cybersecurity Risks and Cyber Incidents

I. Introduction

On February 21, 2018, the Securities and Exchange Commission (SEC) issued long-awaited interpretive guidance on public companies' cybersecurity disclosures through its Statement and Guidance on Public Company Cybersecurity Disclosures (the "Guidance").[1] The SEC issued the Guidance without the open public meeting that it had previously scheduled for the same day and that it had abruptly canceled the day before without explanation. The new Guidance was adopted unanimously, although some Commissioners have since issued public comments suggesting that the Guidance does not go far enough.

The new Guidance addresses public companies' disclosure obligations under existing securities laws and regulations; the new expectation that companies have effective cybersecurity policies and procedures in place; the need for companies to have efficient disclosure controls and policies, including an internal protocol for determining materiality; insider trading prohibitions in the cybersecurity-incident context, as well as the new expectation that companies update their insider trading policies to cover cybersecurity incidents; and prohibitions against selective disclosure in the cybersecurity context.

The latest Guidance builds off of, and closely resembles, guidance on the same issues released by the staff of the SEC Division of Corporation Finance in 2011 (the "2011 Staff Guidance").[2] The SEC states that its new Guidance is intended to reinforce and expand upon the 2011 Staff Guidance. The elevation of

these issues to the level of SEC Guidance may be a signal of the SEC's increased focus on cybersecurity risks and compliance.

In a statement issued the same day, SEC Chairman Jay Clayton said that he hoped that the new Guidance would "promote clearer and more robust disclosure by companies about cybersecurity risks and incidents, resulting in more complete information being available to investors." He "urge[d] 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." Clayton also announced that he has "asked the Division of Corporation Finance to continue to carefully monitor cybersecurity disclosures as part of their selective filing reviews." In a signal of potential future action in the area, he explained that the SEC "will continue to evaluate developments in this area and consider feedback about whether any further guidance or rules are needed."[3]

The key takeaway from the Guidance, similar to the 2011 Staff Guidance, is that the SEC believes that public companies have an obligation to inform investors about material cybersecurity risks and incidents in a fulsome and timely fashion.[4] This includes public companies that are subject to material cybersecurity risks, but have not yet been the target of a cyber-attack. The disclosures should be specific enough to provide useful information, but they do not need to be so specific that they provide information that could harm a company.

The SEC added two key focus areas to the new Guidance not present in the 2011 Staff Guidance. First, the SEC stressed the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents. The Guidance repeatedly emphasizes that a company's ability to make appropriate disclosures is dependent upon the company having proper disclosure controls and procedures to provide information on the impact that risks or incidents will have on a business, as well as having an internal protocol for determining materiality. The company's board should oversee implementation of these controls and procedures. This emphasis mirrors cybersecurity-related focus areas listed in the SEC's 2018 Examination Priorities, including the continued focus on governance and risk assessment.[5]

Second, the SEC reiterated that insider trading prohibitions apply in the cybersecurity context and that companies are expected to have policies in place to stop the misuse and selective disclosure of material nonpublic information about cybersecurity risks or incidents especially during the ongoing investigation. Companies are also encouraged to consider preventative measures to halt any trading in the context of a cybersecurity incident as a means of avoiding the perception of impropriety. This issue recently came to public attention after Equifax executives were found to have traded stock in the period between discovery and disclosure of the company's data breach.

II. Select Commissioners Voice Disappointment; Say SEC Did Not Go Far Enough

Two Commissioners, Kara M. Stein and Robert J. Jackson, Jr., issued independent statements after the SEC's release of its Guidance providing reluctant support and decrying the SEC's failure to take stronger action in the face of increasing cybersecurity risks and incidents. Both Stein and Jackson suggested that

the new Guidance does little beyond reiterate the older 2011 Staff Guidance. In his statement, Jackson noted that the "guidance essentially reiterates years-old staff-level views on this issue" and that "economists of all stripes agree that much more needs to be done." Jackson highlighted, through citation to a statement by the current White House Council of Economic Advisers, the questionable effectiveness of the 2011 Staff Guidance to date and the existence of externalities that, without sufficiently robust regulation, lead firms to rationally underinvest in cybersecurity.[6]

Stein noted that "meaningful disclosure has remained elusive" under the prior 2011 Guidance and suggested that there is little hope that disclosures will improve now that the SEC has reiterated the same guidance. She wrote that "guidance, alone, is plainly not enough" and that the SEC should take stronger action. Stein noted other actions that the SEC could have taken, apart from simply reiterating old guidance, including seeking notice and comment on proposed rules to address improvements to the company's board's risk management framework related to cyber risks and threats, whether the SEC should establish minimum standards to protect personally identifiable information of investors, proposed rules that would require a public company to provide useful notice and disclosure to investors within a certain time following a cyber incident, or whether the SEC should issue rules that are more programmatic and that would require a public company to develop and implement cybersecurity-related policies and procedures beyond just disclosure. She called on the SEC to ensure that the new Guidance is just the first step that it takes on these issues.[7]

III. Discussion of the Guidance

The SEC broke its Guidance into two main buckets – overview of rules requiring disclosure of cybersecurity risks and incidents, and related policies and procedures generally – with multiple topics covered in each section. Many of the topics in the new Guidance were covered in the 2011 Staff Guidance. The expanded descriptions in the latest Guidance, however, warrant close review to ensure all aspects of the SEC's recommendations are implemented in company compliance policies and programs. Details on the key aspects of the SEC's new Guidance are provided below.

A. Disclosure of Cybersecurity Issues

Determining the Materiality of and Disclosing Risks and Incidents – When considering their reporting obligations, companies should consider the materiality of cybersecurity risks and incidents. Factors to weigh include the potential materiality of any identified risk or, in the case of a cybersecurity incident, the importance of any compromised information and the impact of the incident on the company's operations. The materiality of any particular risk or incident is fact-dependent. Companies should consider the nature and extent of a particular risk or incident. The range of harm that might result should also be considered (e.g., resulting regulatory actions, remediation costs).

Once a company has determined that a cybersecurity risk or incident is material, it should disclose the information in a timely and sufficiently robust manner, avoiding boilerplate language. Companies should also disclose any concomitant financial, legal or reputational consequences related to a particular risk or incident. Disclosure should take place well before any offer and sale of securities. Companies may have an obligation to amend prior disclosures where those disclosures were incorrect at the time that they were

made or where additional information comes to light after the disclosure. The SEC encourages the disclosure of cybersecurity in current reports on Form 8-K or 6-K.

An ongoing investigation alone (even an external investigation), without leave of law enforcement, is insufficient to excuse a delay in disclosure. Indeed, the SEC disclosed its own recent breach while its investigation into the same was ongoing.

Guidance on When to Disclose Risks and What Risks to Disclose – Companies should disclose cybersecurity risks if those risks make investments in the companies' securities speculative or risky, including any such risks that arise in the context of an acquisition (e.g., purchase of a subsidiary with a significant history of prior cyber incidents). It may be necessary for a company to provide details of past or ongoing incidents in order to place discussions of current risks in context. Past incidents involving third parties (vendors, customers, competitor, etc.) also may be relevant. The SEC suggests that companies consider the following factors with regard to determining what risks to disclose:

- occurrence of prior cybersecurity incidents and their severity and frequency
- probability of the occurrence and potential magnitude of cybersecurity incidents
- adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including the limits on a company's ability to prevent or mitigate such risks
- 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 vendor and service provider risks
- costs associated with maintaining cybersecurity protections, including any applicable insurance coverage or payments to service providers
- potential for reputational harm to the company from a cybersecurity incident
- existing or pending laws and regulations that may affect the requirements to which companies are subject relating to cybersecurity and the associated costs to companies
- litigation, regulatory investigation and remediation costs associated with cybersecurity incidents.

Disclosure Obligations in the Context of Specific Rules – After providing general guidance on materiality and the disclosure of risks, the SEC provided insight into the disclosures required in the context of particular rules, specifically Management's Discussion and Analysis Financial Condition and Results of Operations (MD&A), description of business, legal proceedings, financial statement disclosures and oversight by the board.

MD&A – The cost of ongoing cybersecurity efforts, the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents could inform a company's analysis and should be included in MD&A materials. The SEC expects companies to consider the impact of cybersecurity incidents on each of their reportable segments.

Description of Business – A company must provide an appropriate disclosure if cybersecurity incidents or risks materially affect its products, services, relationships with customers or suppliers, or competitive conditions, such as the loss of intellectual property or cost of remediation.

Legal Proceedings – Any material legal proceedings to which companies are a party related to cybersecurity incidents should be disclosed. The disclosure should include a description of the litigation, the name of the court in which proceedings are pending, the date that the case was initiated, the principal parties, the underlying facts and the relief sought.

Financial Statement Disclosures – A company's financial reporting and control systems should be designed to provide reasonable assurance that information about the potential financial impacts of a cybersecurity incident are incorporated into its financial statements. Cybersecurity incidents may affect a company's financial statements as a result of:

- 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 or
- diminished future cash flows; impairment of intellectual, intangible or other assets; recognition of liabilities; or increased financing costs.

Special Need to Disclose Oversight of Risks by Board – To the extent that cybersecurity risks are material, a company must disclose the nature of its board's role in overseeing the management of that risk in order to meet the general requirements regarding disclosure of its board's role in managing material risks overall. The SEC also suggests that this information be disclosed to provide investors with the ability to gauge how well the board is discharging its duties with regard to cybersecurity risk oversight.

B. Cybersecurity-Related Policies and Procedures

Need for Robust and Effective Disclosure Controls and Procedures – The SEC indicates that cybersecurity risk management policies and procedures are key elements of any company's enterprise wide risk management. Companies should assess compliance with these policies and procedures regularly, particularly their disclosure controls. Those controls should ensure that risks and concerns are properly escalated up the corporate ladder. Disclosure controls should not be limited to information strictly required by the statutes, but should allow for a more nuanced approach to determining the proper level of detail to disclose. Proper 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.

The SEC indicates that CFO and CEO certifications should address the effectiveness of disclosure controls and should take into account the adequacy of the controls and procedures used to identify cybersecurity risks and incidents and for assessing and analyzing their impact. In addition, controls and procedures may be considered ineffective if cybersecurity risks or incidents would pose a risk to a company's ability to record and report information required to be disclosed in public filings. Management should take this last point into account when adopting or revising controls and procedures.

Incorporating the Cybersecurity Context into Insider Trading Policies – As noted above, insider trading laws apply in the context of cybersecurity incidents, and the SEC expects companies to incorporate rules and policies related specifically to cybersecurity into their insider trading policies and protections. This should come as no surprise to companies, given the public outcry that arose in the wake of the Equifax breach when it came to light that Equifax executives had traded in the company's stock in the period between discovery and disclosure. The SEC also encourages companies to consider updating their codes of ethics required under exchange listing rules to take into account the potential for insider trading in the cybersecurity context. Companies may be well served by considering prohibiting all trading or taking other measures to try and protect against the appearance of improper trading during the period following a cybersecurity incident and before that incident is publicly disclosed.

Upholding Regulation FD in the Cybersecurity Context – Regulation FD requires that, when an issuer or someone acting on its behalf discloses nonpublic information to certain persons, it must make that information public. The SEC indicates that Regulation FD applies in the cybersecurity context and that it expects companies to have policies and procedures in place to address the Regulation FD.

IV. Implications Moving Forward

The 2018 Guidance demonstrates a continued focus by the SEC on cybersecurity risks and compliance. Public companies should take steps now as part of their annual corporate governance review of board committee charters and corporate policies to address the recommendations in the Guidance. The addition of specific guidance with regard to the need to adopt robust cybersecurity policies and procedures, as well as the insider trading guidance, in particular, are areas that should receive special attention by companies to address operational risks and ensure compliance. Furthermore, companies should review risk factors contained in their periodic reports and their forward-looking statements boilerplates to identify whether any additional disclosures should be made.

Some Commissioners and commentators have called on the SEC to move beyond guidance and implement rules to incentivize fulsome cybersecurity disclosures. Although there is no indication that more stringent measures will be adopted, significant future cybersecurity events may spur further regulatory action. For now, companies should continue to carefully consider cybersecurity risk and adopt disclosures and policies to comply with the latest SEC guidance.

Contact Information

If you have any questions regarding this alert, please contact:

Alice Hsu
ahsu@akingump.com
212.872.1053
New York

Jason M. Daniel
jdaniel@akingump.com
214.969.4209
Dallas

Natasha G. Kohne
nkohne@akingump.com
415.765.9505
San Francisco

Michelle A. Reed
mreed@akingump.com
214.969.2713
Dallas

Diana E. Schaffner
dschaffner@akingump.com
415.765.9507
San Francisco

---

[1] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, SEC Release Nos. 33-10459; 34-82746 (Feb. 26, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[2] *See* Division of Corp. Finance SEC, CF Disclosure Guidance: Topic No. 2 – Cybersecurity (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[3] Jay Clayton, Statement on Cybersecurity Interpretive Guidance (Feb. 21, 2018), https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21.

[4] The latest Guidance concerns public companies only; it does not address the implications of cybersecurity risks and incidents with regard to other entities regulated by the SEC.

[5] *See* 2018 National Exam Program Examination Priorities, Office of Compliance Inspections and Examinations, SEC, https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2018.pdf.

[6] Commissioner Robert J. Jackson, Jr., Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018), https://www.sec.gov/news/public-statement/statement-jackson-2018-02-21.

[7] Commissioner Kara M. Stein, Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018), https://www.sec.gov/news/public-statement/statement-stein-2018-02-21.