KING & SPALDING

Client Alert

Data, Privacy & Security and Securities Regulation Practice Groups

March 1, 2018

SEC Reinforces and Elevates Cybersecurity Guidance; Board Oversight of Cybersecurity at the Forefront

On February 21, 2018, the Securities and Exchange Commission ("SEC") published interpretive guidance on public company cybersecurity disclosures. While the new guidance confirms the SEC's intensified focus on cybersecurity disclosures, by the SEC's own characterization, it primarily reinforces and somewhat expands upon guidance previously issued by the SEC staff in October 2011. In fact, much of the language included in this new guidance tracks word for word with the staff's 2011 guidance. The SEC's five commissioners voted unanimously to issue the guidance, but the support of two commissioners was given with reservation based on their view that these "reminders" do not raise the bar on disclosure to the necessary level and leave much more to be done by the SEC on the topic.

Notable differences to the 2011 guidance include:

- Elevated significance from staff guidance to Commission-level guidance;
- Inclusion of a discussion on disclosure regarding the board of directors' role in risk oversight of cybersecurity;
- Enhanced focus on disclosure controls and procedures as they relate to cybersecurity; and
- Considerations with respect to insider trading laws and selective disclosure under Regulation FD raised by cybersecurity incidents.

While the consensus appears to be that this "new" guidance does not represent a significant change to SEC rules and guidance already in effect, we believe that it still warrants vital attention due not only to the importance of the subject matter, but also to the emphasis on board oversight, a growing focus in this area.

The full text of the SEC's statement and guidance can be found here.

Reinforcing 2011 Guidance

The new interpretive guidance provides important reminders regarding SEC rules that may require disclosure of cybersecurity matters, including an outline of (1) disclosure obligations in annual and quarterly reports and under the Securities Act of 1933, (2) the use of current reports on Form 8-K as tools to update registration statements and report cybersecurity incidents (without imposing a specific current

For more information, contact:

Carrie A. Ratliff
+1 404 572 2801
cratliff@kslaw.com

Matthew H. Baughman
+1 404 572 4751
mbaughman@kslaw.com

Alana Griffin
+1 404 572 2450
agriffin@kslaw.com

Alec Koch
+1 202 626 8982
akoch@kslaw.com

Michael Smith
+1 404 572 4824
mrsmith@kslaw.com

Phyllis Sumner
+1 404 572 4799
psumner@kslaw.com

Richard H. Walker
+1 212 556 2290
rwalker@kslaw.com

King & Spalding
www.kslaw.com

reporting obligation), (3) materiality considerations as they relate to cybersecurity matters, and (4) the sections of public filings that may prompt disclosure: Risk Factors, MD&A, Description of Business, Legal Proceedings and Financial Statement Disclosures.

As in the 2011 guidance, the new guidance emphasizes that a company's disclosure should be "tailored to their particular cybersecurity risks and incidents" but is explicit that it is not intended to "suggest that a company 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 new guidance also provides additional insight on factors the SEC believes should be weighed when assessing the materiality of a particular incident, including the importance of any compromised information, the impact on the company's operations, reputation, financial performance and third party relationships and the possibility of litigation or regulatory action.

Board Oversight of Cybersecurity Risk

A disclosure area that was not previously highlighted in the 2011 guidance but that is notably explored in the new guidance is board risk oversight. Under Item 407(h) of Regulation S-K and Item 7 of Schedule 14A, companies are required to disclose the extent of the board of directors' role in risk oversight. The new guidance is clear that, to the extent cybersecurity risks are material to a company's business, the SEC believes the risk oversight discussion in a company's proxy statement should include disclosure regarding the board's role in overseeing management of cybersecurity risks.

The Importance of Disclosure Controls and Procedures

The new guidance emphasizes the need to maintain disclosure controls and procedures designed to ensure timely and accurate disclosure of cybersecurity matters and focuses on whether those controls sufficiently escalate the information regarding cybersecurity incidents and risks up the corporate ladder to top management, including the CEO and CFO providing required certifications. The SEC advises that certifications and disclosures should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents.

Implications Under Insider Trading Laws and Regulation FD

The new guidance reminds companies that information about cybersecurity incidents and risks may constitute material nonpublic information and encourages a reevaluation of insider trading policies and procedures to confirm they adequately address material nonpublic information related to cybersecurity matters to avoid both violations of antifraud provisions and reputational damage. On that same note, the SEC also reminds companies to remain mindful of selective disclosure concerns under Regulation FD that may be raised due to cybersecurity matters.

Key Takeaways

1. *The SEC is serious about meaningful cybersecurity disclosure*. There is no doubt that if a company experiences a breach, its cybersecurity disclosures will come under scrutiny. Even in the absence of a breach, at the direction of Chairman Jay Clayton, the SEC will be carefully monitoring cybersecurity disclosures as part of the regular review process. Companies should review their existing disclosures utilizing the disclosure framework contained in the new guidance and refresh as appropriate.

2. *Expect increasing emphasis on board oversight not only from the SEC but from shareholders, customers and other stakeholders.* The board should have a firm understanding of its role and oversight responsibilities with respect to cybersecurity. Boards should take affirmative steps to confirm directors understand the risks and are

comfortable with how the board oversees those risks. This year's proxy statement should also include disclosure describing the board's oversight. In addition, companies should consider whether it would be valuable to their investors to highlight any experience or expertise in cybersecurity matters held by their directors, as suggested by Commissioner Kara Stein in her statement on the new guidance.

3. *Revisit disclosure controls and insider trading and selective disclosure policies and procedures to confirm cybersecurity incidents and risks are adequately prepared for*. Companies should ensure senior decision-makers are receiving adequate information about cybersecurity matters to enable them to make informed disclosure and insider trading decisions and "whiteboard" how a significant incident would play out under applicable policies and procedures. This includes information potentially subject to disclosure, as well as consideration of prophylactic measures in the context of trading by corporate insiders.

4. *Management's judgment will continue to be required when faced with cybersecurity incidents and risks*. While the SEC's guidance establishes a framework to assist in determinations of materiality and preparation of disclosure, it does not provide "check the box" line item requirements that can be used to determine if an incident is disclosable and, if disclosable, when it should be disclosed. Every cybersecurity incident unfolds differently, with the level of information about the breadth and severity of the intrusion and potential data compromised often developing over the course of days, weeks or even months. While the SEC underscores "timeliness" in its guidance, there is no one size fits all for the timing and content of disclosure, and management will continue to be called upon to use judgment in these disclosure matters.