SEC Issues Updated Cybersecurity Guidance

February 23, 2018

On February 21, the Securities and Exchange Commission released updated **interpretive guidance** on cybersecurity disclosure, reaffirming **staff guidance** issued in 2011, providing more detailed guidance on disclosure of cybersecurity risks and incidents, advising companies to ensure that their disclosure controls and procedures take account of cybersecurity risks and noting the implications of cybersecurity incidents for insider trading prohibitions and Regulation FD compliance. The interpretive guidance lends the Commission's imprimatur to the previously issued staff guidance and underscores the importance for a company to be attuned to securities law obligations when responding to or managing for cyber risks and incidents.

Disclosure

The updated guidance does not create a new line-item disclosure requirement and, like the 2011 staff guidance, takes a principles-based approach that disclosure of cybersecurity risks and incidents should be assessed in light of overall materiality. At the same time, the new guidance sets forth the SEC's views on the application of these principles in a number of specific circumstances. It notes that while detailed disclosure of technical information about systems and vulnerabilities is not necessary, companies should consider disclosure of, among other things:

- prior occurrences of cybersecurity events (the guidance notes that it may be inappropriate to disclose the risk of such events without mentioning actual occurrences);
- the probability and potential magnitude of cybersecurity events; and
- limits on the company's ability to prevent or mitigate such events.

The SEC notes that initial disclosure of an incident may be required before all relevant facts are available, and cautions that the fact that an internal investigation is ongoing would not by itself be a permissible basis for delaying otherwise required disclosure of a material event. The guidance also addresses the need to revisit or refresh prior disclosure during investigation of a cybersecurity incident and reminds companies that they may have a duty to correct or update disclosure in light of subsequent developments.

When material, the SEC expects proxy statement disclosure about a board's involvement in risk oversight to include a discussion of cybersecurity threats and how the board engages with management on cybersecurity issues. This disclosure should address the nature of the board's role in overseeing the management of cybersecurity risk to the extent material and describe how the board discharges its responsibility.

Controls and Procedures

The guidance does not create any new control requirement relating to cybersecurity risk, but it does note that disclosure controls and procedures must be designed to identify cybersecurity risks and incidents, assess their impact on the business, and facilitate the flow of information concerning such risks and incidents to senior management responsible for disclosure decisions and certifications. Accordingly, when a company discloses its conclusions with respect to the effectiveness of disclosure controls and procedures, the conclusions should be informed by management's consideration of cybersecurity risks and incidents, although a specific reference to cybersecurity in the conclusions is not required. The SEC also notes that public company principal executive and financial officers responsible for certifying

effectiveness of disclosure controls and procedures should take into account the degree to which the effectiveness of such controls and procedures may be impacted by cybersecurity risks.

Insider Trading and Regulation FD

The guidance reminds companies that the antifraud provisions prohibiting insider trading on the basis of material nonpublic information encompass trading on information about cybersecurity risks and incidents. During investigation of a cyber incident, the SEC encourages companies to consider whether to implement blackout restrictions on trading prior to public disclosure. The SEC notes, however, that corporate insiders are not precluded from relying upon a 10b5-1 plan if all conditions of the rule are satisfied.

When a cybersecurity incident is material, Regulation FD prohibits its selective disclosure. The SEC encourages companies to disclose material information about cybersecurity matters on Form 8-K (or Form 6-K) to reduce the risk of selective disclosure as well as to maintain the accuracy and completeness of any existing shelf registration statement.

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.

John Banes	**+44 20 7418 1317**	**john.banes@davispolk.com**
Alan F. Denenberg	**650 752 2004**	**alan.denenberg@davispolk.com**
Joseph A. Hall	**212 450 4565**	**joseph.hall@davispolk.com**
Sophia Hudson	**212 450 4762**	**sophia.hudson@davispolk.com**
Michael Kaplan	**212 450 4111**	**michael.kaplan@davispolk.com**
Nicholas A. Kronfeld	**212 450 4950**	**nicholas.kronfeld@davispolk.com**
James C. Lin	**+852 2533 3368**	**james.lin@davispolk.com**
Byron B. Rooney	**212 450 4658**	**byron.rooney@davispolk.com**
Shane Tintle	**212 450 4526**	**shane.tintle@davispolk.com**
Richard D. Truesdell, Jr.	**212 450 4674**	**richard.truesdell@davispolk.com**