Hogan Lovells

SEC Update

March 5, 2018

This is a commercial communication from Hogan Lovells. See note below.

SEC issues new interpretive guidance on cybersecurity disclosures

On February 21, the Securities and Exchange Commission published interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents. The Commission's release follows shorter cybersecurity "disclosure guidance" issued in 2011 by the staff of the SEC's Division of Corporation Finance. The new guidance was prompted by the agency's concern over the increase in the risks and frequency of data breach incidents and other cyber-attacks affecting public companies. The Commission's release addresses many of the matters raised in the staff's guidance, while expanding the discussion to cover additional disclosure and compliance considerations.

The Commission's release does not propose new rules or rule amendments that would impose new requirements, but rather expresses the Commission's views within the existing disclosure framework. The new guidance nevertheless deserves careful study, because it represents a comprehensive statement of the Commission's perspective on the obligation of companies to inform investors about material cybersecurity risks and incidents in a timely fashion. Based on experience with the 2011 guidance, the SEC staff can be expected to refer to the new release in evaluating cybersecurity disclosures – or the absence of such disclosures – by companies whose filings it selects for review.

The Commission's release does not address the specific implications of cybersecurity for entities regulated under the federal securities laws, such as registered investment companies, investment advisers, brokers, dealers, exchanges, and self-regulatory organizations. The SEC staff previously has issued guidance on cybersecurity measures for some of these entities.

The Commission's release is available ***here***.

Overview

As discussed in the ***SEC Update*** we issued in October 2011, the SEC staff's ***guidance*** outlined the staff's views on how companies should describe cybersecurity matters and their potential effects under existing disclosure rules, and in particular in response to specified items of Regulation S-K. The staff also highlighted the manner in which cybersecurity matters may affect financial statement disclosure.

In identifying contexts in which companies may need to disclose cybersecurity risks and incidents, the staff indicated that it had designed its guidance "to be consistent with the relevant disclosure considerations that arise in connection with any business risk." The Commission's guidance broadens that discussion to address assessments of materiality, a company's possible duty to correct or update cybersecurity disclosures, and disclosure concerning board oversight of cybersecurity risks. The new guidance also directs attention to related areas of regulatory concern, including:

- The adequacy of disclosure controls and procedures for identifying and assessing the impact of cybersecurity risks and incidents
- The application of trading prohibitions to corporate insiders when a cybersecurity risk or incident that may be material has not been publicly disclosed
- Compliance with Regulation FD to avoid selective disclosure of a material cybersecurity risk or incident

Disclosure considerations

The new guidance in part recapitulates the staff's 2011 discussion of the application of existing rules to disclosure of cybersecurity risks and incidents. The Commission's discussion also considers how basic principles of securities disclosure can shape decisions about the content and timing of cybersecurity disclosures.

Line-item disclosures. Although no existing SEC disclosure requirement expressly refers to cybersecurity risks and incidents, the staff reminded companies in 2011 that a number of items of Regulation S-K may impose an obligation on public companies to disclose such risks and incidents. Consistent with the staff's discussion, the Commission urges companies to consider cybersecurity matters when preparing disclosures for their financial statements and for sections of their filings covering risk factors, management's discussion and analysis, descriptions of the business and legal proceedings.

The Commission echoes the staff's recognition that companies can face challenges in crafting appropriate disclosure on this subject without jeopardizing their information security. The Commission notes that it is mindful of concerns that "detailed disclosures… could compromise cybersecurity efforts – for example, by providing a 'roadmap' for those who seek to penetrate a company's security protections." It affirms that it does "not expect companies to publicly disclose specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident."

Companies might derive less comfort from the Commission's statement about the importance of timely public disclosure of a material cybersecurity incident. Although the Commission acknowledges that a company may need some time to develop an accurate picture of the nature and effects of such an incident, which could require a lengthy internal investigation or cooperation with law enforcement in an external investigation, the Commission does not believe that the need to complete the assessment alone would justify "avoiding" disclosure of the incident. At most, in the Commission's view, such a need may affect the "scope" of any initial disclosure.

Materiality assessments. The Commission indicates in its release that a public company should assess cybersecurity risks and incidents in light of their materiality to the company and in the context of prior disclosures in the company's SEC filings and other public statements. Citing the standard of materiality articulated long ago by the U.S. Supreme Court, the Commission says that it considers information to be material if (1) there is a substantial likelihood that a reasonable investor would consider the information important when making an investment decision or (2) disclosure of the information would be viewed by a reasonable investor as having significantly altered the "total mix" of information available. The Commission emphasizes that the materiality of cybersecurity risks or incidents, in particular, "depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations….[and] on the range of harm that such incidents could cause."

Deciding that a specific item of Regulation S-K does not require a cybersecurity disclosure does not end the assessment of whether disclosure is required. As the Commission notes, the company also must consider the parallel directives of Rule 408(a) under the Securities Act and Rule 12b-20 under the Exchange Act to disclose, in addition to any specifically required information, "such further material information, if any, as may be necessary to make the required statements, in the light of the circumstances under which they were made, not misleading." The same principle underlies the antifraud provisions of the federal securities laws, which apply to statements both in SEC filings and in other communications.

Duty to correct and duty to update. Companies considering a cybersecurity disclosure should be aware of its implications for future public statements about the matter. The Commission reminds companies that, once they disclose a cybersecurity risk or incident, they "may" have a legal duty to correct or update the disclosure.

The federal securities laws do not impose on a public company an affirmative duty to disclose information simply because it is or might be material. Instead, the duty to disclose arises when an SEC rule requires the disclosure, such as in a periodic or current report, or in other circumstances that have been recognized by the courts.

One such circumstance is when the issuer discovers that a disclosure was inaccurate or misleading when it was made. In this situation, many courts have held that the issuer has a "duty to correct" the disclosure. Such a duty might arise, for example, if a company issues a public

statement incorrectly denying that it has experienced any cyber-attacks.

The Commission also notes that a company may have a "duty to update" a statement that was accurate when made if circumstances change and the statement subsequently becomes inaccurate or misleading. The duty might arise because investors may continue to rely on the original statement in making investment decisions with respect to the company's securities. For example, if a company discloses a cyber-attack and states that, based on its initial evaluation, it does not expect the attack to have material financial impacts, the company may have a duty to update the statement if the company later determines that the financial consequences to the company will be material.

As the cases cited by the Commission indicate, not all federal courts have recognized a duty to update. Moreover, federal courts recognizing the duty to update may differ on its scope. In its guidance, the Commission only refers to federal court decisions addressing the duties to correct and update and does not express its own view on the existence or scope of such duties. Nevertheless, the Commission's focus on this topic underlines the importance of carefully weighing whether a cybersecurity disclosure is required and, if so, how to frame the disclosure in a fashion that is accurate and balanced. An ill-considered disclosure could require difficult future judgments about the need to modify the disclosure or issue additional statements on the subject.

Board risk oversight

Item 407(h) of Regulation S-K and Item 7 of Schedule 14A under the Exchange Act's proxy rules require a company to disclose the extent of the board's role in the risk oversight of the company. The new guidance emphasizes that, to the extent cybersecurity risks are material to a company's business, the discussion of board oversight should inform investors about the nature of the board's role in overseeing the management of those risks. This mandate may serve to sharpen the attention of public company boards to their cybersecurity risk management programs.

Disclosure controls and procedures

The staff urged companies in 2011 to consider whether there are any deficiencies in their disclosure controls and procedures related to the risks posed by cybersecurity incidents, such as an incident affecting information systems, that would render the controls and procedures ineffective.

The Commission shifts the focus on this topic from the potential effect of cybersecurity incidents on the company's controls and procedures to whether the controls and procedures are adequate to ensure accurate and timely disclosure of cybersecurity risks and incidents. The Commission underscores that "[c]rucial to a public company's ability to make any required disclosure of cybersecurity risks and incidents in the appropriate timeframe are disclosure controls and procedures that provide an appropriate method of discerning the impact that such matters may have on the company and its business, financial condition, and results of operations, as well as a protocol to determine the potential materiality of such risks and incidents." The new guidance reflects the Commission's belief that cybersecurity policies and procedures are key elements of enterprise-wide risk management, including as they relate to compliance with the federal securities laws, and therefore that companies should adopt comprehensive policies and procedures related to cybersecurity and regularly assess the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosures.

In keeping with its perspective on materiality assessments, the Commission observes that a company's disclosure controls and procedures should not be limited to promoting compliance with line-item disclosure requirements, but also should ensure timely collection and evaluation of other information for which disclosure might be required, such as under Exchange Act Rule 12b-20. Adequate disclosure controls and procedures would enable companies to identify cybersecurity risks and incidents, assess their impact on the company's business, escalate findings to senior management and disclosure advisors when appropriate, and make timely disclosures with respect to material risks and incidents.

The Commission concludes by pointing out that required quarterly certifications made by the company's principal executive officer and principal financial officer in Exchange Act reports should take into account the adequacy of disclosure controls and procedures for identifying and assessing the impact of cybersecurity risks and incidents.

Insider trading prohibitions

Antifraud provisions of the federal securities laws prohibit directors, officers and other corporate insiders from trading in a company's securities while in the possession of material nonpublic information. The Commission observes that material nonpublic

information could include a significant cybersecurity risk or incident experienced by the company. The guidance encourages companies to consider how their codes of ethics and insider trading policies take into account material nonpublic information pertaining to cybersecurity matters. The Commission recommends that, during any period in which a company is investigating a cybersecurity incident that has not yet been publicly disclosed, it consider whether and when it might be appropriate to implement restrictions on trading by its insiders.

Regulation FD and selective disclosure

In accordance with Regulation FD, whenever a public company, or person acting on its behalf, discloses material nonpublic information to certain enumerated classes of persons, it must make contemporaneous public disclosure of the information. The Commission employs the new guidance to remind companies and their directors, officers and other insiders of their obligations under Regulation FD to refrain from making selective disclosures about cybersecurity risks or incidents. The guidance sets forth the Commission's expectation that companies will maintain policies and procedures that ensure that any disclosures of material nonpublic information related to cybersecurity incidents comply with the requirements of Regulation FD.

Compliance considerations

There are no major surprises in the Commission's guidance. The guidance does not add to or otherwise modify any of the SEC's existing disclosure requirements. Further, most of the considerations concerning cybersecurity disclosures discussed in the guidance apply to disclosures about other types of business risk. The Commission, however, does highlight the complexities involved in assessing the materiality of cybersecurity risks and incidents, preparing the required disclosures, and effectively integrating cybersecurity matters into a company's policies and practices.

The impact of the new guidance on public companies will vary with the extent to which companies previously have addressed the compliance considerations discussed by the Commission. Some companies may benefit by taking a fresh look at their existing cybersecurity disclosures and the factors they would consider in determining whether disclosures concerning a particular event are warranted. Companies preparing their annual proxy statements should consider whether their presentation on board risk oversight should include a discussion of the board's oversight of cybersecurity risks.

Companies should review their disclosure controls and procedures in light of the new guidance and consider whether enhancements are advisable to ensure proper identification and evaluation of cybersecurity risks and incidents and issuance of accurate and timely disclosure in appropriate circumstances. For example, companies might weigh implementing "severity ratings" that specify when and how quickly their information technology personnel must escalate the occurrence of a cybersecurity incident to senior management and to the legal and disclosure teams to allow for timely decisions about disclosure. In addition, companies may wish to consider adding cybersecurity matters to disclosure certifications provided to senior officers and disclosure committees.

Companies also may wish to consider whether the new guidance holds any lessons for the operation of their insider trading and Regulation FD compliance policies. Although amendment of the policies to refer specifically to cybersecurity matters might reinforce awareness of the potential materiality of those matters, the more important step will be to build consideration of cybersecurity risks and incidents into administration of the policies.

This SEC Update is a summary for guidance only and should not be relied on as legal advice in relation to a particular transaction or situation. If you have any questions or would like any additional information regarding this matter, please contact your relationship partner at Hogan Lovells or any of the lawyers listed on the following page of this update.

Contacts

Peter J. Romeo (Co-editor)
Washington, D.C.
peter.romeo@hoganlovells.com
T +1 202 637 5805

Richard J. Parrino (Co-editor)
Washington, D.C.
richard.parrino@hoganlovells.com
T +1 202 637 5530

C. Alex Bahn
Washington, D.C.; Philadelphia
alex.bahn@hoganlovells.com
T +1 202 637 6832 (Washington, D.C.)
T +1 267 675 4619 (Philadelphia)

John B. Beckman
Washington, D.C.
john.beckman@hoganlovells.com
T +1 202 637 5464

Alan L. Dye
Washington, D.C.
alan.dye@hoganlovells.com
T +1 202 637 5737

Amy Bowerman Freed
Baltimore; New York, NY
amy.freed@hoganlovells.com
T +1 410 659 2774 (Baltimore)
T +1 212 918 8270 (New York, NY)

Kevin K. Greenslade
Northern Virginia
kevin.greenslade@hoganlovells.com
T +1 703 610 6189

Paul Hilton
Denver
paul.hilton@hoganlovells.com
T +1 303 454 2414

Harriet Pearson
Washington, D.C.; New York, NY
harriet.pearson@hoganlovells.com
T +1 202 637 5477 (Washington, D.C.)
T +1 212 918 5548 (New York, NY)

Timothy P. Tobin
Washington, D.C.
tim.tobin@hoganlovells.com
T +1 202 637 6833

Lillian Tsu
New York
lillian.tsu@hoganlovells.com
T +1 212 918 3599

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

www.hoganlovells.com