Simpson Thacher

Memorandum

SEC Issues Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures

February 22, 2018

On February 21, 2018, the Securities and Exchange Commission announced it had unanimously approved a statement and interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents.[1] This guidance expands upon the Division of Corporation Finance's 2011 guidance regarding disclosure obligations related to cybersecurity risks and incidents.[2] The release also addresses two topics not developed in the Staff's 2011 guidance: the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the cybersecurity context.[3]

Disclosure Obligations

The SEC's interpretive guidance describes the "grave threat" cybersecurity risks pose to investors and capital markets. Consistent with prior guidance, it reiterates that publicly traded companies should consider the materiality of cybersecurity risks and incidents when preparing the disclosures that are required in registration statements under the Securities Act of 1933 ("Securities Act") and the Securities Exchange Act of 1934 ("Exchange Act") and periodic and current reports under the Exchange Act. In the Commission's view, although existing disclosure requirements do not specifically refer to cybersecurity risks and incidents, a number of the existing requirements impose an obligation to disclose such risks and incidents, depending on a company's particular circumstances, and to correct prior disclosures when necessary. Specifically, the interpretative guidance encourages public companies to consider cybersecurity risks as it relates to their risk

[1] *See* SEC Press Release 2018-22 (Feb. 21, 2018), available at: https://www.sec.gov/news/press-release/2018-22.

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

[3] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosure (Feb. 21, 2018), available at http://www.sec.gov/rules/interp/2018/33-10459.pdf.

factor, MD&A, business, legal proceedings and financial statement disclosures, along with their disclosures regarding the role of the company's board of directors in the risk oversight of the company.

The interpretive guidance provides that, in considering its disclosure obligations, an issuer should consider the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact of the incident on the company's operations. According to the Commission, the materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations. Furthermore, the materiality of cybersecurity risks and incidents also depends on the range of harm that such incidents could cause, including harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities.

Importantly, the guidance states 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 guidance does say, however, that the Commission expects companies to disclose a cybersecurity incident or risk that would be material to its investors in a timely fashion and sufficiently prior to the offer and sale of securities and to take steps to prevent corporate insiders from trading its securities until investors have been appropriately informed about the incident or risk.

Policies and Procedures

Disclosure Controls and Procedures. Separately, the interpretative guidance 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. In particular, the interpretative guidance suggests that companies should revisit their disclosure controls and procedures to confirm that they are designed to "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."

Insider Trading. The interpretative guidance further addresses the intersection of insider trading and cybersecurity risks and incidents. It provides that "information about a company's cybersecurity risks and incidents may be material nonpublic information, and directors, officers, and other corporate insiders would violate the antifraud provisions if they trade the company's securities in breach of their duty of trust or confidence while in possession of that material nonpublic information." In light of the foregoing, the guidance suggests that companies evaluate whether their codes of ethics and insider trading policies

sufficiently "take into account and prevent trading on the basis of material nonpublic information related to cybersecurity risks and incidents." Moreover, the guidance reminds public companies and persons acting on their behalf that they "should not selectively disclose material, nonpublic information regarding cybersecurity risks and incidents to Regulation FD enumerated persons before disclosing that same information to the public."

Significance of the Interpretative Guidance

While much of the commentary and perspective reflected in the interpretative guidance has been previously articulated by Commission staff in recent years, the guidance reflects the Commission's attempt to consolidate its views on a topic that is clearly of critical importance to the agency.

Of note, the Commission has not to date charged any public issuers with respect to disclosure violations relating to cyber incidents, which might reflect both the inherent difficulties in establishing the materiality of such events, as well as the absence of a comprehensive statement of regulatory expectations when such events occur. With the issuance of the interpretative guidance, we anticipate that the Commission will be more inclined to pursue cyber-related enforcement actions—on both disclosure and internal controls theories—to validate the principles articulated in the guidance. We also believe the Commission's pronounced focus on insider trading in connection with cyber events possibly reflects a perception among Commission staff that public issuers and insiders do not equate cyber incidents with the traditional types of corporate events and nonpublic information that might presumptively be viewed as material nonpublic information. In this light, SEC investigations relating to cyber events presumably will routinely encompass a thorough side-by-side investigation of any trading that occurred in proximity to the cyber incidents and related disclosures.

For further information about this development, please contact one of the following members of the Firm, or any other member of the Privacy and Cybersecurity or Public Company Advisory practices.

NEW YORK CITY

Nicholas S. Goldin
+1-212-455-3685
ngoldin@stblaw.com

Karen Hsu Kelley
+1-212-455-2408
kkelley@stblaw.com

Lori E. Lesser
+1-212-455-3393
llesser@stblaw.com

Michael J. Osnato, Jr.
+1-212-455-3252
michael.osnato@stblaw.com

Simpson Thacher Worldwide

UNITED STATES

New York
425 Lexington Avenue
New York, NY 10017
+1-212-455-2000

Houston
600 Travis Street, Suite 5400
Houston, TX 77002
+1-713-821-5650

Los Angeles
1999 Avenue of the Stars
Los Angeles, CA 90067
+1-310-407-7500

Palo Alto
2475 Hanover Street
Palo Alto, CA 94304
+1-650-251-5000

Washington, D.C.
900 G Street, NW
Washington, D.C. 20001
+1-202-636-5500

EUROPE

London
CityPoint
One Ropemaker Street
London EC2Y 9HU
England
+44-(0)20-7275-6500

ASIA

Beijing
3901 China World Tower
1 Jian Guo Men Wai Avenue
Beijing 100004
China
+86-10-5965-2999

Hong Kong
ICBC Tower
3 Garden Road, Central
Hong Kong
+852-2514-7600

Seoul
25th Floor, West Tower
Mirae Asset Center 1
26 Eulji-ro 5-Gil, Jung-Gu
Seoul 100-210
Korea
+82-2-6030-3800

Tokyo
Ark Hills Sengokuyama Mori Tower
9-10, Roppongi 1-Chome
Minato-Ku, Tokyo 106-0032
Japan
+81-3-5562-6200

SOUTH AMERICA

São Paulo
Av. Presidente Juscelino
Kubitschek, 1455
São Paulo, SP 04543-011
Brazil
+55-11-3546-1000