SULLIVAN & CROMWELL LLP

February 27, 2018

SEC Issues Expanded Interpretive Guidance on Cybersecurity Matters

Disclosure Controls and Procedures Should Ensure Appropriate Escalation and Disclosure of Cybersecurity Risks and Incidents and Issuers Should Craft Policies and Procedures Against Insider Trading and Selective Disclosure of Non-Public Information Related to Cybersecurity Risks and Incidents

SUMMARY

On February 20, 2018, the SEC issued further interpretive guidance to assist public companies in disclosing, and crafting policies and procedures for reporting, risk management and preventing insider trading in relation to, cybersecurity risks and incidents.

The SEC highlighted the need for public companies to have in place disclosure controls and procedures designed to escalate cybersecurity risks and incidents to appropriate decision-makers and make appropriate disclosure to investors. The SEC also highlighted how insider trading and selective disclosure compliance should be considered in connection with information regarding cybersecurity vulnerabilities and incidents, and emphasized the need for public companies to implement policies and procedures that prevent directors, officers and other corporate insiders from trading on material non-public cybersecurity information.

BACKGROUND

In October 2011, the Division of Corporation Finance of the Securities and Exchange Commission provided guidance on disclosure obligations relating to cybersecurity risks and incidents (the "2011 Release"). In that release, the SEC observed that the securities laws, although technically silent on cybersecurity matters, implicate important disclosure requirements for material computer system

intrusions and information technology risks.[1] Following the 2011 Release, many public companies included additional cybersecurity-related disclosures in their annual and quarterly reports, often in the form of risk factors, as well as in forward-looking statement disclosure. Our recent review of risk factor disclosure indicates that many public companies in industries that are particularly vulnerable to cybersecurity risks, such as financial services, technology and healthcare, have been disclosing cybersecurity risks with specific attention to the risks facing their particular businesses.

Since 2011, companies have become even more dependent on computing and Internet resources, and cyber incidents have increased in complexity, frequency and impact. SEC Chairman Jay Clayton has observed that the current threat of cybersecurity incidents is now a concern for all public companies, regardless of industry.[2] The costs of monitoring and preventing cybersecurity incidents have become an increasingly important part of all companies' financial results, and the financial costs of responding to and remediating intrusions into a company's computer systems, products or services may be less significant than the significant damage that can be done to a company's reputation and business prospects. In light of these developments, to "promote clearer and more robust disclosure by companies,"[3] the SEC has issued guidance (the "2018 Guidance") that reinforces and expands the Corporation Finance Division's 2011 Release in three main areas:[4]

- the SEC has highlighted and refined its guidance on disclosure requirements that public companies must consider when evaluating cybersecurity risks and incidents;
- the SEC has emphasized the need for disclosure controls and procedures to ensure proper disclosure of cybersecurity issues; and
- the SEC has elaborated upon public companies' responsibilities in implementing policies and procedures that prevent insider trading on, and selective disclosure of, material non-public information related to cybersecurity risks and incidents.

CYBERSECURITY DISCLOSURE REQUIREMENTS

Although the rules governing disclosures made in registration statements under the Securities Act of 1933 (the "Securities Act") and in periodic filings pursuant to the Securities Exchange Act of 1934 (the "Exchange Act") do not specifically mention disclosure of cybersecurity risks or incidents, the 2018 Guidance discusses a number of ways in which these requirements may obligate disclosure of cybersecurity risks and incidents. Public company disclosure around cybersecurity should be crafted with a view towards disclosing all material information in a timely fashion.

---

1 *See* SEC, *CF Disclosure Guidance: Topic No. 2 – Cybersecurity* (Oct. 13, 2011).

2 *See* Jay Clayton, SEC Chairman, *Statement on Cybersecurity Interpretive Guidance* (Feb. 21, 2018) ("Chairman's Statement on Cybersecurity").

3 *See Chairman's Statement on Cybersecurity*.

4 *See* SEC, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* (Feb. 20, 2018).

Assessing Materiality and Adequacy of Disclosures. Evaluations of the materiality of information about cyber risks and incidents should consider whether a reasonable investor would consider that information important to an investment decision and whether its disclosure would alter a reasonable investor's view of the total mix of information available about a company. The 2018 Guidance observes that the materiality of a cybersecurity risk or incident is context-dependent: Companies must weigh the "nature, extent, and potential magnitude" of these risks and the harms that such incidents could cause. In weighing the materiality of these harms, the SEC has encouraged companies to take a comprehensive view of the potential harm of a cybersecurity risk or incident, including analyzing the impact to a company's reputation, the costs and associated impact on the company's financial performance, and the harm to customer and vendor relationships, as well as the impact of possible litigation and regulatory investigations.

A "company-by-company" approach should also guide the content of cybersecurity disclosures. The 2018 Guidance stresses that companies should avoid "generic" or "boilerplate" disclosures when disseminating information to investors, who should be provided with disclosures that are "tailored to [a company's] particular cybersecurity risks and incidents." When making cybersecurity disclosures, the 2018 Guidance does not require companies to provide specific technical detail that would give potential assailants the ability to infiltrate or commandeer a company's network or devices, but the SEC does expect that companies will provide sufficient detail for investors to understand material cybersecurity risks and incidents and their "concomitant financial, legal or reputational consequences."

Board Oversight of Risk Management Under Item 407(h) of Regulation S-K and Item 7 of Schedule 14A. The 2018 Guidance adds emphasis on the disclosure of a board of directors' role in overseeing management of cybersecurity risks and incidents. Under Item 407(h) of Regulation S-K, a company is required to include in its proxy statement a description of how its board of directors administers its risk oversight function. The 2018 Guidance states that, to the extent cybersecurity risks are material, companies should specifically describe the nature of the board's role in overseeing management of cybersecurity risks. The SEC views disclosures concerning a company's cybersecurity risk management program, and how the board of directors engages with management on cybersecurity matters, as important to enabling investors to assess how effectively a board is discharging its oversight responsibilities in an "increasingly important area."

Description of Risk Factors Under Item 503(c) of Regulation S-K and Item 3.D of Form 20-F. If cybersecurity risks and incidents (including those in connection with acquisitions) are among the significant factors that add risk to an investment in a company's securities, they should be disclosed to investors. The 2018 Guidance offers several issues for companies to consider when evaluating what to disclose in a cybersecurity risk factor, including:

- the severity and frequency of past cybersecurity events and the likelihood and potential gravity of future events;

- the adequacy, likely future effectiveness, limits and cost of preventative and mitigation measures, including the costs of cybersecurity insurance and payments to service providers;
- the company's characteristics that give rise to material cybersecurity risks, including industry-specific and third-party risks, and the potential costs and consequences of those risks;
- any laws and regulations relating to cybersecurity that impose compliance and other costs, and the costs of litigation, regulatory investigation and remediation associated with cybersecurity incidents; and
- the potential for reputational harm.

Consistent with a "company-by-company" approach to disclosure, the 2018 Guidance observes that cybersecurity risk factors should include discussion of the circumstances and consequences of past or ongoing cyber incidents in a company's history to allow investors to appreciate the full extent of a risk. For instance, according to the SEC, a purely forward-looking risk factor noting that a company could have a denial of service through network intrusions would likely be inadequate if a company had suffered such breaches in the past. Details of incidents involving third parties, such as suppliers, customers and even competitors, may also be necessary to provide sufficient context for investors to understand a risk.

Management's Discussion and Analysis (MD&A) of Financial Condition and Results of Operations Under Item 303 of Regulation S-K and Item 5 of Form 20-F. The costs and competitive harms from past, present and potential cybersecurity incidents and efforts should inform MD&A disclosures when they are reasonably likely to have a material impact on a company's results of operations, liquidity, financial condition or future performance. Present and anticipated costs of preventative and mitigation efforts, legal compliance, reputational harm or loss of proprietary information or competitive advantage may be relevant to the MD&A discussion, and the SEC anticipates that companies will consider how cybersecurity incidents impact each reportable business segment.

Timing and Propriety of Disclosures. When a company has learned of a cybersecurity incident or risk that is material to its investors, the 2018 Guidance emphasizes that companies are expected to make appropriate disclosures, including filings on Form 8-K or Form 6-K as appropriate.[5] In the case of companies offering securities, the SEC expects such disclosures to be made sufficiently prior to any offer and sale of securities so that potential investors are appropriately informed. The SEC recognizes that disclosures may be required before an investigation has been completed; that such investigations may prove lengthy; and that cooperation with law enforcement may limit the disclosure that can be made in a cybersecurity incident. However, the 2018 Guidance explicitly notes that an investigation, whether internal or external, does not alone justify withholding disclosure about a material cybersecurity event.

Financial Statement Disclosures. Cybersecurity risks and incidents entail a number of potential costs that may impact a company's financial statements, such as the costs of investigation, breach notification

[5] The 2018 Guidance also reminds companies to consider obligations under stock listing requirements, such as Section 202.05 of the NYSE Listed Company Manual and NASDAQ Listing Rule 5250(b)(1).

and remediation; litigation-related expenses; loss of current revenue or diminished future cash flows; warranty product liability or breach of contract claims; insurance premium increases; increased financing costs; recognition of losses and impairment of assets. The SEC expects that a company's financial reporting and control systems will be "designed to provide reasonable assurance that information about the range and magnitude of the financial impacts of a cybersecurity incident would be incorporated into its financial statements on a timely basis as the information becomes available."

DISCLOSURE CONTROLS AND PROCEDURES

Noting the critical nature of cybersecurity risk management policies and procedures to a company's enterprise-wide risk management, the 2018 Guidance also emphasizes the need for comprehensive disclosure policies and procedures to appropriately address cybersecurity risks and incidents and the importance of regularly assessing the effectiveness of these policies and procedures.

The 2018 Guidance notes that effective disclosure controls and procedures are not limited to collecting information required to be disclosed; rather controls and procedures should ensure that all potentially relevant information is collected, considered and monitored, as developments and additional information may require disclosure in the future, including to provide materially important context to other disclosed statements. In particular, the SEC indicates that disclosure controls and procedures should enable a company to identify cybersecurity risks and incidents, access and analyze their input on an ongoing basis, evaluate the significance associated with the risks and incidents and provide for open communication between technical experts and decision-makers.

Required certifications by a company's principal executive officer and principal financial officer as to the design and effectiveness of disclosure controls and procedures should take into consideration whether a company's disclosure controls and procedures for cybersecurity are, in particular, capable of fully assessing and escalating such cyber risks and incidents. In preparing these certifications, public companies should consider whether cybersecurity risks and incidents may themselves threaten a company's ability to process and report information that is required to be disclosed in filings (such as by compromising audit trails or data backups).

INSIDER TRADING AND SELECTIVE DISCLOSURE ISSUES

Companies should consider whether they and their insiders possess material non-public information concerning cybersecurity risks and incidents, and the 2018 Guidance emphasizes that companies must be vigilant in ensuring that such material non-public information does not create a risk of illegal trading by directors, officers and other corporate insiders. The 2018 Guidance also cautions companies not to selectively disclose such information in violation of Regulation FD.

Insider Trading. The 2018 Guidance indicates that insider trading policies should address information relating to cybersecurity. Issuers should consider not only the federal securities anti-fraud laws that

prohibit insider trading, but also their own internal corporate codes of ethics, their prompt disclosure obligations under relevant exchange rules and appearances that may be created by trading by insiders. In particular, the 2018 Guidance suggests that companies consider the potential consequences of trading by directors, officers and other insiders after a cybersecurity incident and prior to disclosure, and suggests the adoption of protective policies to prevent such trading.

Regulation FD Compliance. The 2018 Guidance emphasizes that companies subject to Regulation FD should have policies and procedures to promote compliance with Regulation FD regarding cybersecurity risks and incidents. In particular, these policies and procedures should work to ensure that the company, or a person acting on its behalf, does not make any selective disclosures about cybersecurity risks and incidents to Regulation FD-enumerated persons without the required broadly disseminated public disclosure.

OBSERVATIONS AND IMPLICATIONS

The SEC's 2018 Guidance highlights and refines the disclosure principles described in the 2011 Release. Commissioners Kara M. Stein and Robert J. Jackson noted that the first part of the 2018 Guidance, concerning disclosures, substantially tracks the 2011 Release.[6] However, in addition to elaborating upon and refining that disclosure guidance to take into account issues currently presented by cybersecurity risks and incidents, the 2018 Guidance supplements it with new guidance for public companies' disclosure controls and procedures and insider trading and Regulation FD policies and procedures. Chairman Clayton has urged public companies to "in particular … 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."[7] Although much of the guidance provided by the SEC in the 2018 Guidance aligns with its prior interpretations and the current public company disclosure practices, all issuers should evaluate the adequacy of their disclosure controls and procedures and insider trading and Regulation FD policies in light of the 2018 Guidance.

* * *

[6] *See* Kara M. Stein, SEC Commissioner, *Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures* (Feb. 21, 2018); *see also* Robert J. Jackson, Jr., SEC Commissioner, *Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures* (Feb. 21, 2018).

[7] *See Chairman's Statement on Cybersecurity*.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.

CONTACTS

New York

Mehdi Ansari	1-212-558-4314	ansarim@sullcrom.com
Robert E. Buckholz	1-212-558-3876	buckholzr@sullcrom.com
Catherine M. Clarkin	1-212-558-4175	clarkinc@sullcrom.com
H. Rodgin Cohen	1-212-558-3534	cohenhr@sullcrom.com
Donald R. Crawshaw	1-212-558-4016	crawshawd@sullcrom.com
Robert W. Downes	1-212-558-4312	downesr@sullcrom.com
Mitchell S. Eitel	1-212-558-4960	eitelm@sullcrom.com
John Evangelakos	1-212-558-4260	evangelakosj@sullcrom.com
William G. Farrar	1-212-558-4940	farrarw@sullcrom.com
Jared M. Fishman	1-212-558-1689	fishmanj@sullcrom.com
Nicole Friedlander	1-212-558-4332	friedlandern@sullcrom.com
John P. Mead	1-212-558-3764	meadj@sullcrom.com
Mark J. Menting	1-212-558-4859	mentingm@sullcrom.com
Scott D. Miller	1-212-558-3109	millersc@sullcrom.com
Nader A. Mousavi	1-212-558-1624	mousavin@sullcrom.com
Robert W. Reeder III	1-212-558-3755	reederr@sullcrom.com
Melissa Sawyer	1-212-558-4243	sawyerm@sullcrom.com
James M. Shea Jr.	1-212-558-4924	sheaj@sullcrom.com
William D. Torchiana	1-212-558-4056	torchianaw@sullcrom.com
Marc Trevino	1-212-558-4239	trevinom@sullcrom.com
Benjamin H. Weiner	1-212-558-7861	weinerb@sullcrom.com

Washington, D.C.		
Eric J. Kadel, Jr.	1-202-956-7640	kadelej@sullcrom.com
Robert S. Risoleo	1-202-956-7510	risoleor@sullcrom.com
Los Angeles		
Patrick S. Brown	1-310-712-6603	brownp@sullcrom.com
Alison S. Ressler	1-310-712-6630	resslera@sullcrom.com
Palo Alto		
Sarah P. Payne	1-650-461-5669	paynesa@sullcrom.com
John L. Savva	1-650-461-5610	savvaj@sullcrom.com
London		
Kathryn A. Campbell	44-20-7959-8580	campbellk@sullcrom.com
Oderisio de Vito Piscicelli	44-20-7959-8589	devitopiscicellio@sullcrom.com
John Horsfield-Bradbury	44-20-7959-8491	horsfieldbradburyj@sullcrom.com
Richard A. Pollack	44-20-7959-8404	pollackr@sullcrom.com
David Rockwell	44-20-7959-8575	rockwelld@sullcrom.com
Paris		
Krystian Czerniecki	49-69-4272-5525	czernieckik@sullcrom.com
Frankfurt		
Krystian Czerniecki	49-69-4272-5525	czernieckik@sullcrom.com
Melbourne		
Robert Chu	61-3-9635-1506	chur@sullcrom.com
Sydney		
Waldo D. Jones Jr.	61-2-8227-6702	jonesw@sullcrom.com
Tokyo		
Izumi Akai	81-3-3213-6145	akaii@sullcrom.com
Keiji Hatano	81-3-3213-6171	hatanok@sullcrom.com
Beijing		
Garth W. Bray	852-2826-8691	brayg@sullcrom.com
Hong Kong		
Garth W. Bray	852-2826-8691	brayg@sullcrom.com
Chun Wei	852-2826-8666	weic@sullcrom.com