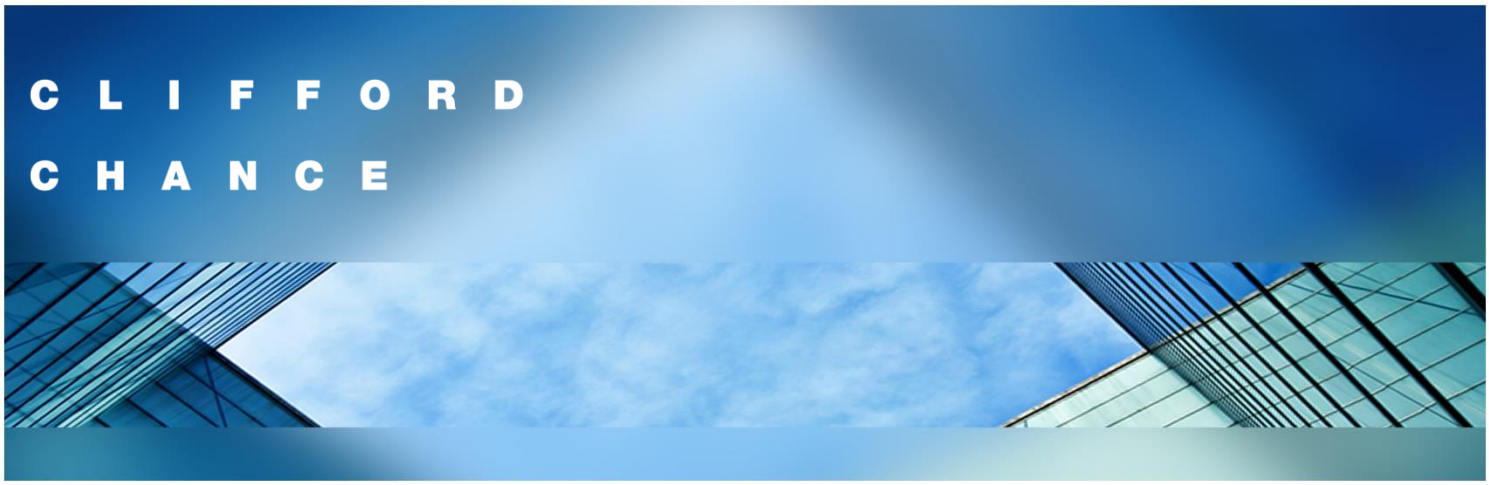

THE SECURITIES AND EXCHANGE COMMISSION ISSUES NEW CYBERSECURITY DISCLOSURE GUIDANCE

On February 21, 2018, the Securities and Exchange Commission ("SEC") issued a statement and interpretive guidance (the "Guidance") to assist issuers in preparing disclosures regarding cybersecurity risks and incidents.[1] Following the Guidance, issuers should expect enhanced scrutiny of their cybersecurity related disclosures and policies and procedures. As a result, issuers should take steps to enhance their current practices. The Guidance stresses the importance of sufficient cybersecurity policies and procedures and emphasizes the risk of insider trading based on the possession of material non-public information about cybersecurity incidents or risks. Although the Guidance was supported by the full Commission, the two Democrat appointees voiced concern that it did not go far enough.[2]

The Guidance supplements and reinforces October 2011 guidance by the Division of Corporation Finance ("2011 CF Guidance") regarding the same subject and continues a trend of increased regulatory focus on ensuring issuers are managing cybersecurity risks and adequately addressing cybersecurity incidents. The Guidance follows the New York State Department of Financial Services' recent adoption of cybersecurity rules last year, and recent cybersecurity enforcement activity by the Commodity Futures Trading Commission ("CFTC"). The SEC's release of the Guidance suggests that it will increase enforcement activity against

---

1 Securities and Exchange Commission, Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018) (*available at*: https://www.sec.gov/rules/interp/2018/33-10459.pdf)

2 Public Statement, Commissioner Kara M. Stein, Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018) (*available at*: https://www.sec.gov/news/public-statement/statement-stein-2018-02-21); Public Statement, Commissioner Robert J. Jackson Jr. Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018) (*available at*: https://www.sec.gov/news/public-statement/statement-jackson-2018-02-21)

issuers and SEC-regulated entities that fail to adequately minimize cybersecurity risk.

The Guidance may also increase litigation risk for issuers. In addition to ensuring issuers are focused on managing cybersecurity risk, the Guidance emphasizes the importance of cybersecurity risk and incident information as material to both current and prospective investors. Therefore, the Guidance provides a mechanism by which shareholders and the plaintiffs' bar will scrutinize the adequacy of issuers' disclosures related to cybersecurity risks and incidents.

Existing Rules Requiring Disclosure of Cybersecurity Issues

In the new Guidance, the SEC highlights seven relevant disclosure obligations that may be implicated by a cyber incident: (i) general disclosure obligations and materiality, (ii) risk factors, (iii) MD&A of financial condition and results of operations, (iv) description of business, (v) legal proceedings, (vi) financial statement disclosures, and (vii) board risk oversight.

General Disclosure Obligations and Materiality

The Guidance explains that when preparing registration statements, disclosures required under the Securities Act of 1933 (the "Securities Act") and the Exchange Act of 1934 (the "Exchange Act"), and periodic and current reports under the Exchange Act, issuers should consider the materiality of cybersecurity risks and incidents. The Guidance specifically references the requirements of Regulation S-K and Regulation S-X which impose an obligation to disclose cybersecurity risks and incidents in the following manner:

- *Periodic Reports*: Issuers are expected to provide timely and ongoing information in their reports regarding material cybersecurity risks and incidents that trigger disclosure obligations.
- *Securities Act and Exchange Act Obligations*: Issuers should ensure they are providing adequate cybersecurity-related disclosure in connection with Sections 11, 12, and 17 of the Securities Act and Section 10(b) and Rule 10b-5 of the Exchange Act.
- *Current Reports*: Issuers are encouraged to utilize current reports in Form 8-K or Form 6-K to ensure their shelf registration statements remain current with regard to the costs and other consequences of material cybersecurity incidents.

Issuers are also expected to disclose "such further material information, if any, as may be necessary to make the required statements in light of the circumstances under which they are made, not misleading." Omitted information about cybersecurity risks or incidents may be material depending on their nature, extent, and potential impact. The materiality of a breach will also be impacted by the harm, including the nature of any compromised information, the impact on the business, company operations, and the range of harm, the incident could cause (*e.g.* reputational, financial, private litigation or regulatory action).

The Guidance explains that the SEC does not expect issuers to disclose information that could compromise their cybersecurity efforts, including specific

technical information about their cybersecurity systems, related networks and devices, or potential system vulnerabilities.

Risk Factors

When making risk factor disclosures, issuers must consider cybersecurity risk under Item 503(c) of Regulation S-K and Item 3.D of Form 20-F. This Item requires disclosure of the most significant factors that make investments in the issuer's securities speculative or risky, including, but not limited to prior cybersecurity incidents, risk of future cybersecurity incidents, the adequacy and cost of undertaking preventative measures, costs associated with compliance and remediation and potential for reputational harm.

In disclosing risk, issuers must include ongoing or previous cybersecurity incidents and related events to provide the appropriate context.

MD&A of Financial Condition and Results of Operation

Issuers are expected to include cybersecurity information in analyzing their financial condition, changes in financial condition, and results of operations as required by Item 303 of Regulation S-K and Item 5 of Form 20-F. Specifically, issuers must incorporate the costs and other consequences of cybersecurity incidents and the risks of potential cybersecurity incidents, including loss of intellectual property, as well as the potential costs of an incident, including the costs of insurance, litigation and regulatory investigations costs, compliance costs, and reputational or competitive harm.

Description of Business

Issuers must include a description of cybersecurity incidents or risks that materially affects their products, services, relationships with customers or suppliers, or competitive condition in Item 101 of Regulation S-K and Item 4.B of Form 20-F.

Legal Proceedings

Issuers are expected to disclose any material pending criminal or civil legal proceedings to which they or their subsidiaries are a party that relate to cybersecurity issues under Item 103 of Regulation S-K.

Financial Statement Disclosures

Information about the range and magnitude of the financial impact of cybersecurity incidents and risks must be incorporated into an issuer's financial statements as it becomes available.

Board Risk Oversight

Disclosures pursuant to Item 407(h) of Regulation S-K and Item 7 of Schedule 14A, which require an issuer to disclose the extent of its board of directors' role in risk oversight of the issuer, must incorporate the nature of the board's role in overseeing the management of cybersecurity risks. These disclosures should also include information regarding the board's collaboration with management on cybersecurity issues.

Policies and Procedures

The SEC also emphasizes in the Guidance that issuers must consider: (i) disclosure controls and procedures, (ii) insider trading, and (iii) Regulation FD and selective disclosure.

Disclosure Controls and Procedures

Issuers are encouraged to adopt comprehensive cybersecurity policies and procedures and to regularly assess compliance and controls.

Certifications and disclosures pursuant to Exchange Act Rules 12b-20, 13a-15, 15d-15, 13a-14, and 15d-14 and Item 307 of Regulation S-K and Item 15(a) of Exchange Act Form 20-F should address and take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact. Furthermore, management should assess the impact cybersecurity risks and incidents pose to an issuer's ability to record, process, summarize, and report information that is required to be disclosed in filings.

Insider Trading

Issuers, their directors, officers, and other corporate insiders should ensure they strictly comply with insider trading laws when in possession of cybersecurity related material non-public information. Directors, officers, and other corporate insiders are prohibited from trading in the issuer's securities while in possession of such information. Issuers should also assess how their own internal codes of ethics and insider trading policies can take into account the risks posed by trading on the basis of material non-public cybersecurity related information.

Regulation FD and Selective Disclosure

Regulation FD requires that material non-public information made available to certain enumerated individuals is disclosed to the public. Issuers should not selectively disclose material non-public information regarding cybersecurity risks and incidents to enumerated persons prior to disclosure to the public. Issuers are expected to adopt policies to ensure compliance with Regulation FD for cybersecurity information.

Conclusion

The new Guidance is the latest sign of an increased focus on cybersecurity by the SEC and heralds an increased risk of enforcement activity and follow-on private litigation in this area. Issuers should be prepared for increased scrutiny of their disclosures and policies and procedures as they relate to cybersecurity risks and incidents by the SEC, other regulators, and the plaintiffs' bar.

CLIFFORD CHANCE

CONTACTS

Steven Gatti
Partner

T +1 202 912 5095
E steven.gatti@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver@cliffordchance.com

Alice Kane
Counsel

T +1 212 878 8110
E alice.kane@cliffordchance.com

Benjamin Berringer
Associate

T +1 212 878 3372
E benjamin.berringer@cliffordchance.com

David Rabinowitz
Associate

T +1 202 912 5436
E david.rabinowitz@cliffordchance.com

Daniel Podair
Associate

T +1 212 878 4989
E dan.podair@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 2001 K Street NW
Washington, D.C. 20006-1001, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Bangkok • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.