ALERT MEMORANDUM

SEC Issues Interpretive Release on Cybersecurity Disclosure

February 28, 2018

On February 21, 2018, the Securities and Exchange Commission (the "Commission") published interpretive guidance to assist public companies when considering, drafting and issuing disclosure about cybersecurity risks and incidents (the "interpretive guidance"). The interpretive guidance became effective immediately upon issuance.

The Commission's interpretive guidance reaffirms and expands upon guidance issued by the Division of Corporation Finance in 2011 (the "Division guidance") relating to the disclosure of cyber-related matters. The interpretive guidance also addresses two additional topics not covered in the Division guidance, specifically that a company's disclosure controls and procedures need to cover cyber-related matters and that compliance with insider trading prohibitions must take into account cybersecurity incidents. The Commission's issuance of interpretive guidance underscores the Commission's increased focus on cybersecurity and follows on the establishment of the Commission's Cyber Unit in 2017 to target cyber-related misconduct and repeated statements by Chairman Jay Clayton and other Commission officials that cybersecurity is a priority area for the agency.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or any of our partners and counsel listed under Cybersecurity and Privacy and Capital Markets in the "Our Practice" section of our website.

NEW YORK
One Liberty Plaza
New York, NY 10006-1470
T: +1 212 225 2000
F: +1 212 225 3999

Commission Interpretive Guidance

I. Disclosure Obligations

Although disclosure requirements under the Securities Act of 1933 (the "Securities Act") and the Securities Exchange Act of 1934 (the "Exchange Act") do not specifically address cybersecurity, the interpretive guidance reiterates the view from the Division guidance that a number of the existing disclosure requirements of the Securities Act and the Exchange Act may impose an obligation for companies to disclose cyber-related matters. The determination of whether a company must make such disclosures is based on generally applicable standards of materiality.[1] The interpretive guidance suggests that, in determining their obligations to disclose cyber-related matters, companies weigh "the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and the impact of the incident on the company's operations. 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

[1] The U.S. Supreme Court has held that information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision or if it "would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available" to the shareholder. *TSC Industries v. Northway*, 426 U.S. 438, 449 (1976); *Basic Inc. v. Levinson*, 485 U.S. 224, 231-32 (1988) (internal citation omitted). Additionally, a company is required 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." 17 CFR § 408; 17 CFR § 240.12b-20; 17 CFR § 240.14a-9.

of company operations." The interpretive guidance highlights a number of factors that may inform the materiality determination, including the range of harm that cybersecurity incidents could have on a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions.

When disclosure is required, the Commission expects companies to provide disclosure that is tailored to their particular cybersecurity risks and incidents, including as they relate to "the concomitant financial, legal and reputational consequences," and placed in the appropriate context. In this regard, the interpretive guidance reiterates the need for non-generic cyber-related disclosure, though specific technical information is not required if it would compromise a company's cybersecurity protections and any remedial efforts.

In addition, while an ongoing internal or external investigation of a material cybersecurity incident does not on its own provide a basis for avoiding disclosure, the Commission is mindful that some material facts may not be available at the time of the initial disclosure. Therefore, the interpretive guidance reminds companies that they may have a duty to correct prior disclosure that the company determines was untrue (or omitted a material fact necessary to make the disclosure not misleading) at the time it was made or a duty to update disclosure that becomes materially inaccurate after it is made.[2]

The interpretive guidance then addresses the areas of disclosure that had been the focus of the Division guidance and expands upon the considerations that companies should review when determining whether disclosure is required and, if so, the scope of such disclosure. In addition to reminding companies to consider cybersecurity disclosure in the context of risk factors, management's discussion and analysis of financial condition and results of operations, business description, legal proceedings and financial statement disclosure, which were covered in the Division guidance, the interpretive guidance also highlights a new area, namely, disclosure of the board's risk oversight. The Commission reminds companies that, to the extent cybersecurity risks are material to a company's business, companies should disclose how the board oversees the management of such risk in their proxy statement as required by Item 407(h) of Regulation S-K.

II. Disclosure Controls and Procedures

The interpretive 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. Companies should assess whether their controls and procedures are adequate to ensure that relevant information about cybersecurity risks and incidents is recorded, processed and reported in a timely manner to senior management responsible for disclosure decisions.[3] The interpretive guidance reminds companies that the controls should not be focused solely on information that relates to disclosure that *is* required, but should also "ensure timely collection and evaluation of information *potentially* subject to required disclosure, or relevant to an assessment of the need to disclose developments and risks that pertain to the company's business." Such disclosure controls and procedures should enable companies to evaluate cybersecurity risks and incidents, make timely disclosures regarding

[2] The federal securities laws do not impose a general affirmative duty on public companies to continuously disclose material information and, as acknowledged in Footnote 37 of the interpretive guidance, circuits are split on whether a duty to update exists. However, in circuits where a duty to update has been found to exist, a distinction has often been drawn between statements of a policy nature that are within the company's control and statements describing then current facts that would be expected to change over time. The former have been held subject to a duty to update while the latter have not. *See In re Advanta Corp. Securities Litigation*, 180 F.3d 525, 536 (3d Cir. 1997) ("[T]he voluntary disclosure of an ordinary earnings forecast does not trigger any duty to update."); *In re Burlington Coat Factory Securities Litigation*, 114 F.3d 1410, 1433 (3d Cir. 1997); *In re Duane Reade Inc. Securities Litigation* No. 02 Civ. 6478 (NRB), 2003 WL 22801416, at *7 (S.D.N.Y. Nov. 25, 2003), *aff'd sub nom. Nardoff v. Duane Reade, Inc.*, 107 F. App'x 250 (2d Cir. 2004) ("'company has no duty to update forward-looking statements merely because changing circumstances have proven them wrong.'").

[3] 17 CFR § 240.13a-14; 17 CFR § 240.15d-14.

such material risks and incidents, and allow the company's principal executive and principal financial officers to make the quarterly certifications regarding the design and effectiveness of the disclosure controls and procedures required by Exchange Act Rules 13a-14 and 15d-14.

III. Insider Trading

In the wake of certain recent cybersecurity incidents, the interpretive guidance reminds companies of the applicability of insider trading prohibitions in the cybersecurity context. The interpretive guidance underscores the importance of policies and procedures to prevent directors, officers and other corporate insiders with material non-public information relating to cybersecurity matters from trading in breach of their duty of trust or confidence. However, the Commission notes that corporate insiders are not precluded from relying on Exchange Act Rule 10b5-1, if all conditions of the rule are satisfied.

IV. Regulation FD and Selective Disclosure

Regulation FD prohibits selective disclosure of material non-public information, which, as noted in the interpretive guidance, would include a material cybersecurity incident. The interpretive guidance encourages companies to review their policies in order to ensure that any disclosure of material non-public information related to cybersecurity risks and incidents is not made on a selective basis.

Takeaways

To date, the Commission has not charged a public company with a disclosure violation related to cybersecurity risks or incidents. However, the issuance of interpretive guidance by the Commission could signal a shift in the Commission's enforcement posture. In fact, during a panel session at the 2017 International Association of Privacy Professionals' Global Privacy Summit, then-Acting Enforcement Director Stephanie Avakian (who has since been appointed Co-Director on a permanent basis) stated that while the Commission has "not brought an action in [the cybersecurity] space," she could "absolutely" see a circumstance where the Commission would do so. In addition, the plaintiffs' bar has also taken a strong interest in cybersecurity disclosure as evidenced by the increase in the number cyber-related securities class actions filed since January 2017.[4]

Against this backdrop, companies should take the opportunity to review their disclosures, policies and disclosure controls and procedures as they relate to cybersecurity matters. In particular:

Disclosure – Companies should review their disclosures in each of the areas identified by the interpretive guidance and the Division guidance (as well as any others where disclosure of cyber-related matters is relevant) and revise or update their disclosure such that it is tailored to the company's specific circumstances and framed in the relevant context. For example, the interpretive guidance specifically highlights that if a company has previously experienced a material cybersecurity incident, it would not be sufficient for the risk factors to state that such incidents *may* occur. Rather, the disclosure should describe the incident to provide appropriate context.

Disclosure Controls and Procedures – Companies should review their cybersecurity policies and cyber incident response plan ("cyber IRP") in light of the interpretive guidance. In particular, they should evaluate whether the disclosure controls and procedures are adequate to ensure cybersecurity matters are identified, that such information is processed and reported to the appropriate personnel, and that senior management is able to make disclosure decisions in a timely manner. Relatedly, companies should be mindful that Item 307 of Regulation S-K requires companies to disclose conclusions as to the effectiveness of disclosure controls and procedures on a quarterly basis.

[4] Alexis Kramer, *More Companies Face Securities Fraud Suits After Data Breaches*, Tech & Telecom on Bloomberg Law (Feb. 12, 2018), https://www.bna.com/companies-face-securities-n57982088684/.

Insider Trading – Companies should review their insider trading and other policies as well as their cyber IRP to determine whether any changes are appropriate in light of the interpretive guidance and recent events. While insider trading policies are generally sufficiently broad that modifications to address cybersecurity matters may not be necessary, we recommend that companies review their cyber IRP to include a step reminding companies to close the trading window, pursuant to the insider trading policy or if otherwise warranted under the circumstances.

Adequate disclosure controls and procedures are not only necessary to identify when a cybersecurity incident has occurred, but also to ensure directors, officers and other corporate insiders with material nonpublic information regarding the cybersecurity event do not trade in violation of the insider trading laws. Therefore, in reviewing their disclosure controls and procedures and cyber IRP, companies should also ensure that those responsible for pre-approving trades or closing the trading window are made aware of any material information relating to cybersecurity incidents.

Regulation FD – Although the federal securities laws do not require ongoing disclosure of cybersecurity events (absent the company or company insiders transacting in company securities), some cybersecurity events will lead companies to make required or voluntary disclosures about cyber-related matters. For example, most of the U.S. states and many foreign countries require consumers or others to be notified in the event that their personal or sensitive information has been compromised. Increasingly, parties to commercial arrangements negotiate provisions requiring a counterparty to provide notice in the event such counterparty's system has been breached in a way that may affect the other's data. Finally, some companies, because of the nature of their business or the type of data that has been compromised, may make voluntary disclosures to inform their customers or business partners about a breach. In each of these cases, and others, companies should be mindful of the application of Regulation FD.

…

CLEARY GOTTLIEB