LATHAM & WATKINS

Number 1247 October 24, 2011

Client Alert

Latham & Watkins Corporate Department

SEC Staff Issues Disclosure Guidance on Cybersecurity Risks and Cyber Incidents

On October 13, 2011, the Staff of the Division of Corporation Finance of the Securities and Exchange Commission (the SEC Staff) issued guidance on the disclosure of cybersecurity risks and cyber incidents.[1] Data security breaches and other cybersecurity incidents were repeatedly in the headlines in 2011, with several large public companies reporting breaches, attempted breaches or service and website shutdowns by "hacktivists" and other actors. Some companies that were in the headlines for cyber incidents were not attacked, but simply experienced systems failures that nonetheless exposed sensitive data or resulted in a degradation or complete loss of service.

It is important to note that the guidance is not itself a new rule, regulation or statement of the Securities and Exchange Commission itself. Rather, the guidance simply seeks to clarify the application of *existing* disclosure obligations in this area.[2] At the same time, the guidance reiterates that disclosure in compliance with the securities laws does not require registrants to reveal information that might negatively impact their cybersecurity efforts. This *Client Alert* reviews and summarizes the new guidance, specifically the scope of cybersecurity risks and cyber incidents and the types of disclosure obligations that may be implicated — risk factors, management's discussion and analysis, description of business, legal proceedings, financial statements, and disclosure controls and procedures. In the light of this new guidance, registrants should review their existing cybersecurity disclosures carefully and consider what, if any, improvements could be made.

> "The guidance is helpful, however, in clarifying the full extent and nature of such obligations and the expectations of the Division of Corporation Finance vis-à-vis such disclosures."

The Scope of Cybersecurity Risks and Cyber Incidents

One of the first points the guidance makes is the breadth of what might be considered a cybersecurity risk or cyber incident. The guidance points out that "cyber incidents can result from deliberate attacks or unintentional events."[3] Cybersecurity attacks include not just technologically sophisticated hacking attempts or denial-of-service attacks, but also social engineering and other conventional efforts to gather information, such as security credentials, in order to pass (or bypass) cybersecurity systems. Additionally, while much of the guidance focuses on cyber attacks, it is worth bearing in mind that the principles outlined (and the underlying securities laws) apply to unintentional incidents as well. These would include,

among other things, inadvertent cybersecurity lapses and other systems failures.

Regardless of the cause, cybersecurity risks and cyber incidents can have a material adverse impact on a registrant and remain subject to the same disclosure standards under the securities laws as other operational or financial risks or incidents.[4] A cybersecurity breach could result in the loss of valuable information or intellectual property, liability for stolen assets or information, remediation costs to repair damage caused by the breach (including business incentives to make amends with affected customers and business partners), additional security costs to mitigate against future incidents, litigation costs resulting from the incident, and lost revenues and reputational damage. To the extent that cybersecurity risks and cyber incidents could have a material adverse impact, the guidance discusses the extent and nature of disclosures that may be necessary in certain specific areas.

Risk Factors

Registrants are required to disclose "the most significant factors" that make an investment in their securities speculative or risky.[5] In determining if risks associated with cyber incidents should be disclosed, the guidance notes that registrants are expected to evaluate their cybersecurity risks and consider all relevant information, such as "prior cyber incidents and the severity and frequency of those incidents", "the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences", and "the adequacy of preventative actions … in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware."[6]

As with all risk factor disclosure, cybersecurity risk factors should be tailored to the facts and circumstances of the specific registrant. Depending on a registrant's particular facts and circumstances, examples of appropriately tailored disclosures might include:

- A discussion of aspects of the business or operations that give rise to material cybersecurity risks and the potential costs and consequences
- To the extent outsourced functions have material cybersecurity risks, a description of those functions and how the registrant addresses those risks[7]
- A description of cyber incidents experienced by the registrant that are, individually or in the aggregate, material, including the costs and other consequences of such incidents
- Risks related to cyber incidents that may remain undetected for an extended period
- A description of relevant insurance coverage

The guidance also reminds registrants that, as with other operational or financial risks, specific known or threatened cyber incidents may need to be discussed to put disclosed cybersecurity risks in context.[8] At the same time, the guidance provides reassurance that compliance with the securities laws does not require the provision of information that could compromise a registrant's cybersecurity measures, but only disclosure sufficient to "allow investors to appreciate the nature of the risks faced by the particular registrant in a manner that would not [compromise cybersecurity]."[9] Where investigation of a cybersecurity breach or other incident is ongoing, a registrant should consider, in light of the specific facts and circumstances, the nature and extent to which the breach or incident and the associated investigation are required to be disclosed under the securities laws.

Management's Discussion and Analysis of Financial Condition and Results of Operation (MD&A)

The guidance states that cybersecurity risks and cyber incidents should be discussed in a registrant's MD&A if the costs or consequences of a known incident or the risk of potential incidents are "reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition."[10] This is the same general standard that applies to events, trends or uncertainties that may affect a registrant's financial condition and results of operations. For example, the costs and consequences of a cybersecurity breach that resulted in the theft of intellectual property may include diminished revenues, increased costs for protective measures, and litigation costs incurred to defend or prosecute related lawsuits. To the extent such effects are material to the registrant, the registrant's MD&A should discuss the breach and such costs and consequences. If a breach attempt was unsuccessful but caused the registrant to incur material costs to improve its cybersecurity, MD&A should contain a discussion of such material costs even if the specific cybersecurity improvements may not need to be disclosed.

Description of Business

Disclosure of a cyber incident may be warranted if the incident materially affects a registrant's products, services, customer or supplier relationships or competitive conditions. Further, if the registrant has different reporting segments, the relevant threshold is the impact of such a cyber incident on each segment, and not the enterprise as a whole.[11]

Legal Proceedings

If a registrant or any of its subsidiaries is a party to a material legal proceeding related to a cyber incident (whether it is a cyber attack or an uninentional event), such a legal proceeding would be subject to the same disclosure requirements as any other legal proceeding under Item 103 of Regulation S-K.[12]

Financial Statement Disclosures

Cybersecurity risks and cyber incidents, and the measures taken in response to potential or actual incidents, may impact a registrant's financial statements in several different ways. First, costs and losses will need to be treated appropriately under the relevant accounting standards.[13] Second, a cyber incident could diminish future cash flows and affect the impairment accounting of a registrant's assets. Where the impact of a cyber incident is not immediately knowable, a registrant may need to develop estimates to account for different potential financial implications and, for future reporting periods, review the assumptions that underlie such estimates.[14] Third, if a cyber incident is discovered after a registrant's balance sheet date but before its financial statements are issued, the guidance notes the registrant should consider if the cyber incident should be disclosed as a recognized or unrecognized subsequent event. If the registrant decides to disclose the incident as a material nonrecognized subsequent event, then the financial statements should disclose the nature of the incident and either an estimate of its financial effect or state that the financial effect cannot be estimated.[15]

Disclosure Controls and Procedures

A registrant's principal executive and principal financial officers, or persons

performing similar functions, are required to disclose their conclusions regarding the effectiveness of the registrant's disclosure controls and procedures for each reporting period.[16] A cyber incident may adversely impact a registrant's disclosure controls and procedures, for example by shutting down its internal network or causing the loss of data. To the extent that a cyber incident causes a registrant's disclosure controls and procedures to be ineffective, the registrant would need to make appropriate disclosures concerning its conclusions on the effectiveness of such disclosure controls and procedures for the affected reporting periods.

Conclusion

Cybersecurity risks and cyber incidents are nothing new, and registrants' disclosure obligations with respect to such risks and incidents remain unchanged. The guidance is helpful, however, in clarifying the full extent and nature of such obligations and the expectations of the Division of Corporation Finance vis-à-vis such disclosures. Public companies' disclosures about cyber incidents are also receiving increased scrutiny from other quarters.[17] Registrants should carefully review their existing disclosures in this area in light of this new guidance, and be prepared for additional scrutiny in this area both from the SEC Staff and their investors.

Endnotes

1 CF Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 14, 2011), http://sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

2 The guidance notes that registrants with effective shelf registration statements should consider the necessity of filing a Form 6-K or Form 8-K containing additional disclosures on "the costs and other consequences of material cyber incidents" in order to maintain the accuracy and completeness of their registration statements. CF Disclosure Guidance: Topic No. 2, *Cybersecurity* (Oct. 14, 2011).

3 CF Disclosure Guidance: Topic No. 2, *Cybersecurity* (Oct. 14, 2011).

4 "Although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents. In addition, material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading." CF Disclosure Guidance: Topic No. 2, *Cybersecurity* (Oct. 14, 2011).

5 *See* Item 503(c) of Regulation S-K and Item 3.D of Form 20-F.

6 CF Disclosure Guidance: Topic No. 2, *Cybersecurity* (Oct. 14, 2011).

7 In a twist of timing, several days prior to the issuance of the guidance, the SEC informed its employees that the contractor operating its staff ethics compliance program may have shared their personal brokerage account information with an unauthorized subcontractor. See "Who's Watching the Watchdog? SEC Admits to Possible Data Breach" (Oct. 17, 2011), http://www.infosecurity-magazine.com/view/21414.

8 "For example, if a registrant experienced a material cyber attack in which malware was embedded in its systems and customer data was compromised, it likely would not be sufficient for the registrant to disclose that there is a risk that such an attack may occur. Instead, as part of a broader discussion of malware or other similar attacks that pose a particular risk, the registrant may need to discuss the occurrence of the specific attack and its known and potential costs and other consequences." CF Disclosure Guidance: Topic No. 2, *Cybersecurity* (Oct. 14, 2011).

9 CF Disclosure Guidance: Topic No. 2, *Cybersecurity* (Oct. 14, 2011).

10 CF Disclosure Guidance: Topic No. 2, *Cybersecurity* (Oct. 14, 2011). See also Item 303 of Regulation S-K and Item 5 of Form 20-F.

11 CF Disclosure Guidance: Topic No. 2, *Cybersecurity* (Oct. 14, 2011).

12 Item 103 states, in part: "Describe briefly any material pending legal proceedings, other than ordinary routine litigation incidental to the business, to which the registrant or any of its subsidiaries is a party or of which any of their property is the subject. Include the name of the court or agency in which the proceedings are pending, the date instituted, the principal parties thereto, a description of the factual basis

alleged to underlie the proceeding and the relief sought. Include similar information as to any such proceedings known to be contemplated by governmental authorities."

[13] The guidance lists Accounting Standards Codification (ASC) 350-40, *Internal-Use Software*, ASC 605-50, *Customer Payemnts and Incentives*, and ASC 450-20, *Loss Contingencies*, as examples of accounting standards that may need to be considered in reviewing the treatment of cybersecurity costs and losses in a registrant's financial statements.

[14] The guidance further notes that ASC 275-10, Risks and Uncertainties, could require a registrant to "explain any risk or uncertainty of a reasonably possible change in its estimates in the near-term that would be material to the financial statements." CF Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 14, 2011).

[15] *See* ASC 855-10, Subsequent Events.

[16] Item 307, Regulation S-K.

[17] On May 11, 2011, several senators wrote to Chairman Mary Schapiro to express their concerns over public companies' disclosures regarding cybersecurity, or lack thereof. See "Rockefeller Calls on SEC to Make Corporate Cyber Attacks Public", available at http://commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord_id=f2a73c1c-3567-4f86-b918-144e83666c52.

If you have any questions about this *Client Alert*, please contact one of the authors listed below or the Latham attorney with whom you normally consult:

Jeffrey A. Tochner
+1.212.906.1200
jeffrey.tochner@lw.com
New York

Kevin C. Boyle
+1.202.637.2245
kevin.boyle@lw.com
Washington, D.C.

Kee-Min Ngiam
+1.213.485.1234
kee-min.ngiam@lw.com
Los Angeles

Abu Dhabi
Barcelona
Beijing
Boston
Brussels
Chicago
Doha
Dubai
Frankfurt
Hamburg
Hong Kong
Houston
London
Los Angeles
Madrid
Milan
Moscow
Munich
New Jersey
New York
Orange County
Paris
Riyadh*
Rome
San Diego
San Francisco
Shanghai
Silicon Valley
Singapore
Tokyo
Washington, D.C.

* In association with the Law Office of Mohammed A. Al-Sheikh