COVINGTON

COVINGTON & BURLING LLP

ADVISORY | Securities
Privacy and Data Security

October 17, 2011

SEC GUIDANCE ON DISCLOSURE RELATED TO CYBERSECURITY

Last week, the Division of Corporation Finance (the "Division") of the Securities and Exchange Commission (the "SEC") published interpretive guidance regarding the application of federal securities law disclosure requirements to cybersecurity.[1] The guidance comes at a time when cybersecurity risks are seen to have increased, particularly in tandem with dependence on digital technologies, and there is a resulting concern as to how companies should manage these risks and properly disclose related operational and financial impacts.[2]

APPLICATION OF EXISTING DISCLOSURE RULES TO CYBERSECURITY ISSUES

In the interpretive guidance, the Division acknowledges that no existing disclosure requirement refers specifically to cybersecurity risks or cyber incidents. Nonetheless, the guidance highlights disclosure requirements that companies should consider on an ongoing basis when assessing the adequacy of disclosure related to cybersecurity risks and cybersecurity incidents.

Risk Factors

Under Item 503(c) of Regulation S-K, a company is required to disclose "the most significant factors that make an investment in the company speculative or risky."[3] In light of this obligation, the Division reminds companies to evaluate their cybersecurity risks fully, taking into account a variety of information, such as the occurrence, frequency and severity of prior cybersecurity incidents, as well as the potential costs and other consequences associated with such incidents. Based on such evaluation, a company may need to craft appropriate risk factor disclosure, including a discussion with respect to (1) aspects of its business or operations giving rise to material cybersecurity risks and potential costs and consequences, (2) risks associated with outsourcing functions that have material cybersecurity risks and how those risks are addressed, (3) any cybersecurity incidents that are material, individually or in the aggregate, and the costs and consequences of such incidents, (4) risks related to undetected incidents and (5) any relevant insurance coverage.

---

[1] Securities and Exchange Commission Division of Corporation Finance, CF Disclosure Guidance: Topic No. 2: Cybersecurity (Oct. 13, 2011) (available at: http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm). CF Disclosure Guidance is a new form of Division guidance in which it provides views on disclosure issues that have garnered significant public attention. The first CF Disclosure Guidance, published in September 2011, discussed disclosure obligations in connection with reverse merger transactions.

[2] Earlier this year, a group of U.S. Senators submitted to SEC Chairman Mary Schapiro a request that the SEC clarify the existing disclosure rules as they relate to information security and related issues. *See* Letter to SEC Chairman Mary Schapiro from U.S. Senators John D. Rockefeller IV, Robert Menendez, Sheldon Whitehouse, Mark Warner and Richard Blumenthal, dated May 11, 2011. In a letter responding to such request, Chairman Schapiro outlined some of the points set forth in the CF Disclosure Guidance and indicated that she was seeking the advice of the SEC staff as to whether additional guidance was necessary. *See* Letter to U.S. Senator John D. Rockefeller IV from SEC Chairman Mary Schapiro, dated June 6, 2011.

[3] *See also* Form 20-F, Item 3.D.

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

Under Item 303 of Regulation S-K, a company is required to disclose, among other things, any "material event, trend, or uncertainty that is 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."[4] Here, the Division reminds companies to consider whether the costs or other consequences associated with known data breaches or the risk of such events could require MD&A disclosure. As an example of when disclosure might be appropriate, the Division describes a theft of intellectual property that is expected to have a material impact on a company's results of operations, liquidity or financial condition. The guidance suggests that disclosure regarding such a theft should cover such effects, as well as the impact that such theft may have on future revenues, including the potential increase in cybersecurity protection costs and litigation.

Description of Business

In its "Description of Business," a company should include any cyber incidents that materially affect the company's products, services, relationships with customers or suppliers or competitive conditions, including with respect to reportable segments.[5] As an example, a company should discuss a cyber-incident and its potential impact, if material, relating to a new product in development where the incident may materially affect that product's future viability.

Legal Proceedings

When disclosing legal proceedings under Item 103 of Regulation S-K, a company must consider whether it (or any of its subsidiaries) has any material pending legal proceeding that relates to a cybersecurity incident. An example in this area could include theft of a significant amount of customer information that results in material litigation.

Financial Statement Disclosures

The guidance reviews a number of respects in which cybersecurity risks and cyber incidents could impact a company's financial statement disclosures, including the disclosures regarding the accounting treatment of (1) capitalized costs of preventing cyber incidents,[6] (2) incentives provided to customers to mitigate business relationship damages from cyber incidents,[7] (3) various losses from asserted and unasserted claims related to the incidents,[8] (4) impairment of certain assets, including goodwill, customer intangible assets, trademarks, patents, capitalized software or other long-lived assets associated with hardware or software, and inventory, and (5) risk of changes in estimates made in preparing financial statements that may be affected by cybersecurity incidents.[9]

---

[4] *See also* Form 20-F, Item 5.
[5] Item 103 of Regulation S-K; and Form 20-F, Item 4.B.
[6] *See, e.g.,* Accounting Standards Codification ("ASC") 350-40, *Internal-Use Software*.
[7] *See, e.g.,* ASC 605-50, *Customer Payments and Incentives*.
[8] *See, e.g.,* ASC 450-20, *Loss Contingencies*.
[9] *See, e.g.,* ASC 275-10, *Risks and Uncertainties*.

Disclosure Controls and Procedures

To the extent a cybersecurity incident affects a company's ability to record, process, summarize, and report information that is required to be disclosed in SEC filings, the company's management should consider whether there are any deficiencies in disclosure controls and procedures that render them ineffective.[10]

ANTICIPATED IMPACT OF CF DISCLOSURE TOPIC NO. 2 ON FUTURE DISCLOSURES

CF Disclosure Topic No. 2 is not a new disclosure rule and should not be viewed as creating additional disclosure obligations, or expanding a public company's existing disclosure obligations, relating to cybersecurity. Much like previous interpretive guidance regarding high profile issues such as Y-2K, climate change, and most recently, reverse merger transactions, the Division's recent guidance is intended to answer questions regarding the application of federal securities law to a new front-page issue. While we expect that the publication of this guidance will draw additional attention to disclosures regarding cybersecurity, it likely will not result in significant structural changes to SEC filings by public companies. On the other hand, the guidance clearly lays out a series of topics and questions on which the Division's program will focus. And, inasmuch as these are also topics and questions of broad public interest, companies should re-evaluate their current disclosure obligations with cybersecurity in mind.

If you have any questions concerning the material discussed in this client advisory, please contact the following members of our privacy and data security group:

Kurt Wimmer	202.662.5278	kwimmer@cov.com
David Fagan	202.662.5291	dfagan@cov.com
Stephen Satterfield	202.662.5659	ssatterfield@cov.com

Or the following members of our securities practice group:

David Martin	202.662.5128	dmartin@cov.com
Keir Gumbs	202.662.5500	kgumbs@cov.com
Brandon Gay	202.662.5808	bgay@cov.com

[10] *See* Item 307 of Regulation S-K; and Form 20-F, Item 15(a).