Milbank

Global Securities Group

Client Alert

New York Los Angeles Washington, DC London Frankfurt Munich Beijing Hong Kong Singapore Tokyo São Paulo

December 21, 2011

SEC GUIDANCE ON CYBERSECURITY DISCLOSURE

On October 13, 2011, the staff of the Securities and Exchange Commission's ("SEC") Division of Corporation Finance issued guidance to all registrants regarding disclosure obligations related to cybersecurity risks and cyber incidents. Cybersecurity refers to "the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access." Cybersecurity has become an important part of operations as companies employ digital technologies to conduct their businesses. A breach of cybersecurity, or a cyber incident, may vary widely and can be intentional, such as gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data or causing operational disruption, or unintentional, such as failing to safe-guard customer information.

Although there are currently no disclosure requirements that specifically refer to cybersecurity risks and cyber incidents, existing requirements may impose an obligation on registrants to disclose information about their cybersecurity measures and any incidents they might have experienced in the past. The SEC staff has reminded registrants that they have a general duty to disclose material information regarding cybersecurity risks and cyber incidents when necessary "in order to make other required disclosures, in light of the circumstances under which they are made, not misleading." Aware of the risks associated with disclosure about a registrant's cybersecurity measures, the SEC staff's guidance is not intended to result in disclosure that would provide a "road map" to those who seek to infiltrate a registrant's network security, something which is not required under the federal securities laws. Instead, the SEC staff's guidance is intended to be "consistent with the relevant disclosure considerations that arise in connection with any business risk."

Risk Factors

Item 503(c) of Regulation S-K requires each registrant to disclose the most significant factors that make an investment in the registrant speculative or risky. Registrants are therefore advised to evaluate their cybersecurity risks, any prior cyber incidents, including the severity and frequency of those incidents, and the adequacy of any prophylactic measures they have taken to reduce such risks or the recurrence of such incidents given the industry in which they operate, in order to determine whether a risk factor or other disclosure is required. To the extent that a risk factor is warranted, a registrant

For further information about this Client Alert, please contact:

Rod Miller
Partner
212-530-5022
rdmiller@milbank.com

Marcelo A. Mottesi
Partner
212-530-5602
mmottesi@milbank.com

Robert W. Mullen, Jr.
Partner
212-530-5150
rmullen@milbank.com

Arnold B. Peinado III
Partner
212-530-5546
apeinado@milbank.com

Douglas Tanner
Partner
212-530-5505
dtanner@milbank.com

Robert B. Williams
Partner
212-530- 5516
rwilliams@milbank.com

You may also contact any member of Milbank's Global Securities group. Contact information can be found at the end of this Client Alert or in the Practice Areas section at www.milbank.com.

should avoid generic "boiler plate" disclosure. Instead, a registrant should tailor its cybersecurity risk factor to the registrant's individual facts and circumstances, including disclosing known or threatened cybersecurity threats and specific past incidents. The SEC staff has suggested that appropriate disclosure might include:

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

Management's Discussion and Analysis of Financial Condition and Results of Operation

Registrants that are the victims of cyber incidents can incur substantial additional costs or suffer other negative consequences that could have an impact on their financial condition, including remediation costs for stolen assets or strengthening the cybersecurity measures that failed, lost revenues, litigation and reputational damage. If cybersecurity risks or cyber incidents have had or are likely to have a material effect on a registrant's results of operations, liquidity or financial condition or are likely to cause reported financial information not to be necessarily indicative of future operating results or financial condition, then the registrant's MD&A should include a description of such risks and incidents pursuant to Item 303 of Regulation S-K.

Description of Business

To the extent that a registrant's products, services, relationship with customers or suppliers, or competitive conditions have been impacted materially by cyber incidents, the registrant should provide disclosure in its "Description of Business" pursuant to Item 101 of Regulation S-K, both for the registrant as a whole and for each of its reportable business segments. For example, if a cyber incident could materially impair the future viability of a registrant's new service or product, the registrant should discuss the incident and its potential impact.

Legal Proceedings

If a pending legal proceeding to which a registrant is a party involves a cyber incident, details of such litigation may need to be disclosed in its "Legal Proceedings" disclosure to the extent material. Such disclosure should include a description of the factual basis underlying the claim and the relief sought.

Financial Statement Disclosure

Cybersecurity risks and cyber incidents may have a material impact on a registrant's financial statements, including the costs of (1) developing or maintaining cybersecurity software, (2) incentives for customers harmed by any cyber incident to maintain their business relationship with the registrant, (3) losses from asserted and unasserted claims, including those related to warranties, breach of contract, product recall and replacement, and indemnification of counterparty losses from their remediation efforts, (4) diminished future cash flows and (5) the impairment of certain assets, including goodwill, customer-related intangible assets, trademarks, patents, capitalized software or other long-lived assets associated with hardware or software, and inventory. To the extent that a cyber incident occurs after the balance sheet date but before financial statements are available, if the cyber incident constitutes a material nonrecognized subsequent event not disclosed in the registrant's financial

statements, then the financial statements should disclose the nature of the incident and an estimate of its financial effect, or a statement that such an estimate cannot be made. Registrants are therefore encouraged to speak with their accountants regarding the appropriate treatment of the impact of, and costs and expenses attributable to, cybersecurity risks and cyber incidents.

Disclosure Controls and Procedures

Finally, the SEC staff's guidance encourages management to consider whether there are any deficiencies in a registrant's disclosure controls and procedures that would render them ineffective as a result of a cyber incident. For example, if there is a material risk that a hacker could hinder a registrant's ability to record, process, summarize and report information that is required to be disclosed in filings with the SEC, such controls may be considered ineffective and management would be required to disclose that fact to the public.

Additional Considerations

SEC staff guidance does not constitute "a rule, regulation, or statement" of the SEC and the SEC has not formally approved its content. Nevertheless, the guidance provides useful advice on cybersecurity for all registrants in the wake of several high profile cyber incidents and will likely be considered by a court in future litigation. As a result, registrants should take the guidance into consideration when reviewing their disclosure and, at a minimum, in designing their disclosure controls and procedures. In addition, all registrants should consider whether it is necessary to file reports on Form 8-K or Form 6-K to disclose the costs and other consequences of material cyber incidents and be prepared to do so if such events occur in the future in order to maintain the accuracy and completeness of information in any effective shelf registration statements. At least one commentator has suggested that the SEC staff may monitor news reports for cyber incidents and then review the filings of those companies impacted by such incidents to assess the adequacy of their disclosure in accordance with the guidance.

Please feel free to discuss any aspect of this Client Alert with your regular Milbank contacts or with any member of our Global Securities group listed below.

Beijing

Anthony Root	+86-10-5969-2777	aroot@milbank.com
Edward T. Sun	+86-10-5969-2772	esun@milbank.com

Frankfurt

Thomas Ingenhoven	+49-69-71914-3436	tingenhoven@milbank.com

Hong Kong

Anthony Root	+852-2971-4842	aroot@milbank.com
Gary S. Wigmore	+852-2971-4815	gwigmore@milbank.com
Dieter Yih	+852-2971-4888	dyih@milbank.com
Joshua M. Zimmerman	+852-2971-4811	jzimmerman@milbank.com

London

Peter Schwartz	+44-20-7615-3045	pschwartz@milbank.com
Tim Peterson	+44-20-7615-3106	tpeterson@milbank.com

Los Angeles

Kenneth J. Baronsky	+1-213-892-4333	kbaronsky@milbank.com
Deborah J. Ruosch	+1-213-892-4671	druosch@milbank.com
Neil J. Wertlieb	+1-213-892-4410	nwertlieb@milbank.com

Munich

Peter Nussbaum	+49-89-25559-3630	pnussbaum@milbank.com

New York

James H. Ball, Jr.	+1-212-530-5515	jball@milbank.com
Paul Denaro	+1-212-530-5431	pdenaro@milbank.com
Andrew Janszky	+1-212-530-5317	ajanszky@milbank.com
Rod Miller	+1-212-530-5022	rdmiller@milbank.com
Marcelo A. Mottesi	+1-212-530-5602	mmottesi@milbank.com
Robert W. Mullen, Jr.	+1-212-530-5150	rmullen@milbank.com
Arnold B. Peinado, III	+1-212-530-5546	apeinado@milbank.com
Douglas A. Tanner	+1-212-530-5505	dtanner@milbank.com
Robert B. Williams	+1-212-530-5516	rwilliams@milbank.com

São Paulo

Andrew Janszky	+55-11-3927-7701	ajanszky@milbank.com
Tobias Stirnberg	+55-11-3927-7702	tstirnberg@milbank.com

Singapore

Naomi J. Ishikawa	+65-6428-2525	nishikawa@milbank.com
Giles Kennedy	+65-6428-2425	gkennedy@milbank.com

Tokyo

Mark Plenderleith	+813-5410-2842	mplenderleith@milbank.com

Washington, DC

Winthrop N. Brown	+1-202-835-7514	wbrown@milbank.com