Legal ALERT
Keeping you informed of noteworthy changes in the law.

PHILLIPS NIZER LLP

October 2011

SECURITIES LAW ALERT

SEC STAFF ISSUES DISCLOSURE GUIDANCE CONCERNING CYBERSECURITY RISKS

In October 2011, the Division of Corporation Finance ("Division") of the Securities and Exchange Commission ("SEC") issued guidance concerning the disclosure obligations of public companies in their periodic reports and registration statements relating to cybersecurity risks and cyber incidents such as when persons seek to gain unauthorized access to the digital systems of such companies for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruptions.

Although no existing SEC disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on public companies to disclose such risks and incidents in their periodic reports and registration statements. 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.

The following sections provide an overview of the Division's views on existing disclosure obligations under the federal securities laws that may require a discussion of cybersecurity risks and cyber incidents.

Risk Factors

A public company should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky. In determining whether risk factor disclosure is required, the Division expects companies to evaluate their cybersecurity risks and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents. As part of this evaluation, public companies should consider the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption.

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

A public company should address cybersecurity risks and cyber incidents in the "Management's Discussion and Analysis" section of its SEC reports if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the company'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.

Description of Business

If one or more cyber incidents materially affect a public company's products, services, relationships with customers or suppliers, or competitive conditions, the company should provide disclosure in the "Description of Business" section of

(Please see next page for more information.)

666 Fifth Avenue, 28th Floor • New York • NY 10103-0084
600 Old Country Road • Citibank Building • Garden City • NY 11530-2011
Court Plaza North • 25 Main Street, 6th Floor • Hackensack • NJ 07601-7015

212.977.9700 Tel • 212.262.5152 Fax
516.229.9400 Tel • 516.228.9612 Fax
201.487.3700 Tel • 201.646.1764 Fax

www.phillipsnizer.com

Resourceful Representation®

its SEC reports. In determining whether to include disclosure, public companies should consider the impact on each of their reportable segments. As an example, if a company has a new product in development and learns of a cyber incident that could materially impair its future viability, the company should discuss the incident and the potential impact to the extent material.

Financial Statement Disclosures

Cybersecurity risks and cyber incidents may have a broad impact on a public company's financial statements, depending on the nature and severity of a potential or actual incident.

Prior to a Cyber Incident

A public company may incur substantial costs to prevent cyber incidents. Accounting for the capitalization of these costs is addressed by Accounting Standards Codification (ASC) 350-40, *Internal-Use Software*, to the extent that such costs are related to software that is intended for internal use by such company.

During and After a Cyber Incident

A public company may seek to mitigate damages from a cyber incident by providing customers with incentives to maintain their business relationships. Public companies should consider ASC 605-50, *Customer Payments and Incentives*, to ensure appropriate recognition, measurement, and classification of these incentives.

Cyber incidents may result in 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. Public companies should refer to ASC 450-20, *Loss Contingencies*, to determine when to recognize a liability if those losses are probable and reasonably estimable. In addition, public companies must provide certain disclosures of losses that are at least reasonably possible.

Cyber incidents may also result in diminished future cash flows, thereby requiring consideration of 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.

Disclosure Controls and Procedures

A public company is required to disclose conclusions on the effectiveness of its disclosure controls and procedures in its periodic reports. To the extent cyber incidents pose a risk to a public company's ability to record, process, summarize, and report information that is required to be disclosed in SEC filings, management should also consider whether there are any deficiencies in its disclosure controls and procedures that would render them ineffective.

For additional information concerning the Division's cybersecurity disclosure guidance, see "CF Disclosure Guidance: Topic No. 2" at the following location: http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

We are available to provide counsel concerning these issues, as well as other Securities and Technology concerns. For additional information, please contact the attorney named below or contact the attorney with whom you have a primary relationship.

Contact:	R. Brian Brodrick	212.841.0700	bbrodrick@phillipsnizer.com
	Thomas G. Jackson	212.841.0765	tjackson@phillipsnizer.com
	Jonathan E. Silverblatt	212.841.0761	jsilverblatt@phillipsnizer.com
	Christopher J. Kula	212.841.0733	ckula@phillipsnizer.com