October 14, 2011

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or your regular Skadden contact.

Brian V. Breheny
202.371.7180
brian.breheny@skadden.com

Marc S. Gerber
202.371.7233
marc.gerber@skadden.com

Andrew J. Brady
202.371.7344
andrew.brady@skadden.com

Susie Lee
202.371.7579
susie.lee@skadden.com

1440 New York Avenue, NW, Washington, DC 20005
Telephone: 202.371.7000

Four Times Square, New York, NY 10036
Telephone: 212.735.3000

SEC Issues Disclosure Guidance on Cybersecurity Risks and Cyber Incidents

On October 13, 2011, the Division of Corporation Finance issued disclosure guidance on cybersecurity. The guidance is intended to assist companies in assessing what disclosure should be provided with respect to cybersecurity risks and cyber incidents and how cybersecurity risks and their impact should be described in Commission filings. Although there is no disclosure requirement explicitly referring to cybersecurity risks and cyber incidents, the guidance notes that a number of existing disclosure requirements may impose an obligation to disclose such matters. Examples include:

- Risk Factors – Risk of cyber incidents should be discussed if such risk is among the most significant risk factors that make an investment in the company speculative or risky. In evaluating risk, companies should consider prior cyber incidents, the severity and frequency of such incidents, the probability and magnitude of such incidents (including potential costs and consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption) and the adequacy of preventative actions to reduce cybersecurity risks. Appropriate disclosures may also include a discussion of the company's business or operations that give rise to material cybersecurity risks (including outsourced functions), a description of material cyber incidents experienced, a discussion of risks related to cyber incidents that may remain undetected for an extended period and a description of relevant insurance coverage. In some circumstances, it also may be appropriate to discuss specific attacks experienced in order to make investors aware of the potential impact on the company. Companies should provide disclosure tailored specifically to their circumstances and avoid generic risk disclosures.
- Management's Discussion and Analysis – Cybersecurity risks and cyber incidents should be addressed in the MD&A if costs or consequences associated with known incidents or risk of potential incidents present a material event, trend or uncertainty reasonably likely to have a material effect on the company's results of operations, liquidity or financial condition or would cause reported financials not to be necessarily indicative of future operating results

or financial condition. The guidance notes that companies that are victims of successful cyber attacks may incur substantial costs and suffer negative consequences, such as remediation costs (e.g., liability for stolen assets or information, repairing system damage and offering customer incentives), increased cybersecurity protection costs, lost revenues, litigation and reputational damage.

- Additional Examples – Depending on the circumstances, cybersecurity risks and cyber incidents also may require companies to include disclosure in their "description of business," "legal proceedings" or financial statements.

The Division, addressing potential concerns that detailed disclosures might compromise cybersecurity efforts by providing a "roadmap" of a company's network security, emphasized that "disclosures of that nature are not required under federal securities laws" and that "registrants should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular registrant in a manner that would not have that consequence."

The Division's cybersecurity disclosure guidance can be found here.