KING & SPALDING

Public Company Advisor

Practical Insights for Public Company Counsel

January 2012

King & Spalding's Public Company Practice Group periodically publishes the Public Company Advisor *to provide practical insights into current corporate governance, securities compliance and other topics of interest to public company counsel.*

A Practical Guide to Implementing SEC Guidance on Disclosure of Cybersecurity Risks and Cyber Incidents

Recent, high-profile cyber attacks and cybersecurity lapses have resulted in a serious focus on cybersecurity from the Obama administration, the Senate and the SEC. In the past year, there were reports of cyber thieves hacking corporate networks to steal customer data from financial services firms and retailers, intellectual property from life sciences, technology and industrial companies and information regarding the location of major oil reserve from multinational oil companies. This proliferation of cyber attacks led to five U.S. senators writing to SEC Chairwoman Mary Schapiro asking the SEC to develop and publish interpretive guidance on the disclosure of cybersecurity risks by public companies. The SEC's Division of Corporation Finance staff did so in October 2011 (www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm).

Corp Fin's guidance is not a new disclosure rule, nor does it give the SEC specific authority to regulate a company's cybersecurity policy. Rather, the guidance is a clarification of existing disclosure obligations; and with 10-Ks due soon for a number of public companies, now is the time to understand and consider the disclosure impact of this guidance.

Understand the SEC Guidance

Corp Fin's guidance is designed to aid a public company in the disclosure exercise it undertakes for public filings. Just as with other items, if cybersecurity issues pose a material risk and/or cybersecurity-related costs materially impact operating results (for example, in the case of remediation of a breach), then the risk and/or the impact must be disclosed and described. Companies must consider vulnerability to third-party actors and events like hacker attacks, viruses and malware, as well as the potential for inadvertent disclosure of confidential information by the company or others. Corp Fin provided companies with a list of specific risks to consider, which you can view by clicking on the link above.

Draft a Risk Factor if Needed

Whether and to what extent disclosure of cybersecurity risks is needed is specific to each company. A number of public companies included a cybersecurity risk factor in their '34 Act filings before Corp Fin issued its guidance, and several others have updated their '34 Act filings

to include a cybersecurity risk factor since the October guidance. We believe that given current technology, outsourcing and IT processes, many companies will address cybersecurity in a '34 Act risk factor, regardless of industry, and that a wave of new cybersecurity risk factors will be included in 10-Ks for December 31 year-end companies.

As with all risk factors, specificity counts, particularly when a company has had a prior cybersecurity issue or has undertaken a particular cybersecurity initiative. Of course, Corp Fin acknowledged in its published guidance that specificity does not mean that a company must roadmap its potential weaknesses, which could increase vulnerability to an attack.

However, specificity does mean that each public company should carefully consider the types of cybersecurity risks it faces. Risk factors will be different for the retailer that relies on its website for a significant portion of its sales, the business services company that outsources its customer service function, or the company that could be an attractive target for a Domain Name Server (DNS) attack, because of its important role in global commerce. Accordingly, a company must evaluate the unique threats that it faces, rather than relying on boilerplate disclosure.

We have provided sample risk factor disclosure on Annex A to highlight the different risks faced by companies across industry groups. These samples have been excerpted from recent SEC filings, with specific company names omitted.

Describe Incidents If They Happen

If an incident occurs resulting in material costs or consequences (remediation cost; increased prevention efforts; reputational consequences) or that may indicate material future cybersecurity uncertainties, trends or events, it must be disclosed and described in MD&A. Disclosures in other sections of a company's '34 Act documents (for example, Description of Business; Legal Proceedings) may be required as well. Significant attacks may even warrant current reporting on Form 8-K or a press release.

Cybersecurity risks and events may impact a company's financial statements, and companies should consider discussing with their auditors the way in which costs related to prevention, remediation, loss recognition and/or loss mitigation would be classified.

Review Disclosure Controls and Procedures

Companies should consider reviewing their disclosure controls and procedures in light of potential cybersecurity risks. The SEC requires companies to disclose conclusions on the effectiveness of disclosure controls and procedures, and Corp Fin has noted that these controls and procedures should address cybersecurity risks as well. Again, this is not a new disclosure requirement, but a clarification of an existing one.

About King & Spalding's Public Company Practice Group

King & Spalding's Public Company Practice Group is a leader in advising public companies and their boards of directors in all aspects of corporate governance, securities offerings and regulatory compliance and disclosure.

About King & Spalding

Celebrating more than 125 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 800 lawyers in

17 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality and dedication to understanding the business and culture of its clients. More information is available at www.kslaw.com.

The Public Company Advisor *provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. For more information on this issue of the* Public Company Advisor*, please contact:*

Keith M. Townsend	**Laura O. Hewett**	**Brittain A. Rogers**
+1 404 572 3517	+1 404 572 2729	+1 404 572 2751
ktownsend@kslaw.com	***lhewett@kslaw.com***	***brogers@kslaw.com***

EXHIBIT A

Cybersecurity Risk Factor Disclosure

Distributor	Information security risks have generally increased in recent years because of the proliferation of new technologies and the increased sophistication and activities of perpetrators of cyber attacks. A failure in or breach of our operational or information security systems, or those of our third party service providers, as a result cyber attacks or information security breaches could disrupt our business, result in the disclosure or misuse of confidential or proprietary information, damage our reputation, increase our costs and/or cause losses. As a result, cyber security and the continued development and enhancement of the controls and processes designed to protect our systems, computers, software, data and networks from attack, damage or unauthorized access remain a priority for us. Although we believe that we have robust information security procedures and other safeguards in place, as cyber threats continue to evolve, we may be required to expend additional resources to continue to enhance our information security measures and/or to investigate and remediate any information security vulnerabilities. Third party service providers are responsible for managing a significant portion of our information systems. Our business and results of operations may be adversely affected if the third party service provider does not perform satisfactorily.
Metals Producer	We have put in place a number of systems, processes and practices designed to protect against intentional or unintentional misappropriation or corruption of our systems and information or disruption of our operations. These include, for example, the appropriate encryption of information. Despite such efforts, we are subject to breaches of security systems which may result in unauthorized access, misappropriation, corruption or disruption of the information we are trying to protect, in which case we could suffer material harm. Access to our proprietary information regarding new formulations would allow our competitors to use that information in the development of competing products. In addition, our systems could be subject to sabotage by employees or third parties, which could slow or stop production or otherwise adversely affect our operations. Any misappropriation or corruption of our systems and information or disruption of our operations could have a material adverse effect on our business.
Industrial	We and certain of our third-party vendors receive and store personal information in connection with our human resources operations and other aspects of our business. Despite our implementation of security measures, our IT systems are vulnerable to damages from computer viruses, natural disasters, unauthorized access, cyber attack and other similar disruptions. Any system failure, accident or security breach could result in disruptions to our operations. A material network breach in the security of our IT systems could include the theft of our intellectual property or trade secrets. To the extent that any disruptions or security breach results in a loss or damage to our data, or in inappropriate disclosure of confidential information, it could cause significant damage to our reputation, affect our relationships with our customers, lead to claims against us and ultimately harm our business. In addition, we may be required to incur significant costs to protect against damage caused by these disruptions or security breaches in the future.
Public Utility	We are subject to cyber-security risks primarily related to breaches of security pertaining to sensitive customer, employee, and vendor information maintained by us in the normal course of business, as well as breaches in the technology that manages natural gas distribution operations and other business processes. A loss of confidential or proprietary data or security breaches of other technology business tools could

	adversely affect our reputation, diminish customer confidence, disrupt operations, and subject us to possible financial liability, any of which could have a material affect on the our financial condition and results of operations. We closely monitor both preventive and detective measures to manage these risks.
Telecom	Attempts by others to gain unauthorized access to our information technology systems are becoming more sophisticated and are sometimes successful. These attempts, which might be related to industrial or other espionage, include covertly introducing malware to our computers and networks and impersonating authorized users, among others. We seek to detect and investigate all security incidents and to prevent their recurrence, but in some cases, we might be unaware of an incident or its magnitude and effects. The theft, unauthorized use or publication of our intellectual property and/or confidential business information could harm our competitive position, reduce the value of our investment in research and development and other strategic initiatives or otherwise adversely affect our business. To the extent that any security breach results in inappropriate disclosure of our customers' or licensees' confidential information, we may incur liability as a result. In addition, we expect to devote additional resources to the security of our information technology systems.
Manufacturer	A cyber-attack that bypasses our information technology (IT) security systems causing an IT security breach, may lead to a material disruption of our IT business systems and/or the loss of business information resulting in adverse business impact. Risks may include: • future results could be adversely affected due to the theft, destruction, loss, misappropriation or release of confidential data or intellectual property • operational or business delays resulting from the disruption of IT systems and subsequent clean-up and mitigation activities • negative publicity resulting in reputation or brand damage with our customers, partners or industry peers.
Grocery Store Chain	Our business is increasingly dependent on information technology systems that are complex and vital to continuing operations. If we were to experience difficulties maintaining existing systems or implementing new systems, we could incur significant losses due to disruptions in our operations. Additionally, these systems contain valuable proprietary and financial data, as well as debit and credit card cardholder data, and a breach, including cyber security breaches, could have an adverse effect on us.
Consumer Electronics and Online Marketplace	Our business requires us to use and store customer, employee, and business partner personally identifiable information (PII). This may include names, addresses, phone numbers, email addresses, contact preferences, tax identification numbers, and payment account information. Although malicious attacks to gain access to PII affect many companies across various industries, we may be at a relatively greater risk of being targeted because of our high profile and the amount of PII managed. We require user names and passwords in order to access our information technology systems. We also use encryption and authentication technologies to secure the transmission and storage of data. These security measures may be compromised as a result of third-party security breaches, employee error, malfeasance, faulty password management, or other irregularity, and result in persons obtaining unauthorized access to company data or accounts. Third parties may attempt to fraudulently induce employees or customers into disclosing user names, passwords or other sensitive information, which may in turn be used to access our information technology systems. To help protect customers and the company, we monitor accounts and systems for unusual activity and may freeze accounts under suspicious circumstances, which may

	result in the delay or loss of customer orders. We devote significant resources to network security, data encryption, and other security measures to protect our systems and data, but these security measures cannot provide absolute security. We may experience a breach of our systems and may be unable to protect sensitive data. Moreover, if a computer security breach affects the company's systems or results in the unauthorized release of PII, our reputation and brand could be materially damaged and use of our products and services could decrease. We would also be exposed to a risk of loss or litigation and possible liability, which could result in a material adverse effect on our business, results of operations and financial condition.
Financial Services	Our operations rely on the secure processing, storage and transmission of confidential and other information in our computer systems and networks. Although we take protective measures and endeavor to modify them as circumstances warrant, the security of our computer systems, software and networks may be vulnerable to breaches, unauthorized access, misuse, computer viruses or other malicious code and other events that could have a security impact. Additionally, breaches of security may occur through intentional or unintentional acts by those having authorized or unauthorized access to our or our clients' or counterparties' confidential or other information. If one or more of such events occur, this potentially could jeopardize our or our clients' or counterparties' confidential and other information processed and stored in, and transmitted through, our computer systems and networks, or otherwise cause interruptions or malfunctions in our, our clients', our counterparties' or third parties' operations, which could result in significant losses or reputational damage to us. We may be required to expend significant additional resources to modify our protective measures or to investigate and remediate vulnerabilities or other exposures arising from operational and security risks, and we may be subject to litigation and financial losses that are either not insured against or not fully covered through any insurance maintained by us.