BNA International

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 11, Number 11 November 2011

U.S. Securities And Exchange Commission Guidance On Disclosure Obligations Relating To Cybersecurity Risks And Cyber Incidents

By Mark S. Bergman and Jillian M. Lutzy, of Paul, Weiss, Rifkind, Wharton & Garrison LLP, London.

The Staff of the Securities and Exchange Commission's Division of Corporation Finance October 13, 2011, issued written guidance (CF Disclosure Guidance: Topic No. 2) setting forth the views of the Staff regarding disclosure obligations in respect of cybersecurity risks and cyber incidents. The guidance is the result of heightened risks related to cybersecurity and the increase in the frequency and severity of cyber incidents. These risks, in turn, have prompted registrants, counsel and auditors to focus on providing appropriate public disclosure without further compromising cybersecurity by conveying a roadmap to hackers through disclosures of vulnerabilities of systems and networks.

The guidance is intended to assist registrants in preparing disclosure under both the Securities Act of 1933 (the 1933 Act) and the Securities Exchange Act of 1934 (the 1934 Act). The Staff notes that, in addition to preparing line item disclosure, the guidance may also be relevant for registrants with shelf registration statements as they consider whether a Form 6-K or Form 8-K would be appropriate to disclose the costs or other consequences of material cyber incidents, and more generally for registrants as they consider their obligations under 1933 Act Rule 408 and 1934 Act Rules 12b-20 and 14a-9 and the antifraud provisions of the 1933 Act and the 1934 Act.

The guidance is effective immediately and applies to domestic SEC registrants as well as non-U.S. SEC registrants.

The guidance is effective immediately and applies to domestic SEC registrants as well as non-U.S. SEC registrants.

The guidance directs registrants to review, on an ongoing basis, the adequacy of their disclosures relating to cybersecurity risk and cyber incidents and addresses potential disclosure issues in the context of the following specific disclosure requirements.

Risk Factors

The risk of cyber incidents should be disclosed if these issues are among the significant factors that make an investment in the registrant speculative or risky. In determining whether disclosure is required, a registrant should take into account all available relevant information related to cybersecurity risks — including prior incidents and the severity and frequency of any such incidents. A registrant should also consider the adequacy of preventative measures in determining if risk factor disclosure should be provided. Disclosure should focus

on registrant-specific risks and must adequately describe the nature of the material risks and how each risk affects the registrant. As with risk factors generally, the risk factor should not simply be a boilerplate recitation of cyber risks. As noted above, the Staff acknowledged that a registrant should not provide disclosure that itself would compromise its cybersecurity; instead, the risk factors should enable investors to appreciate the nature of the risks without compromising cybersecurity.

Management's Discussion and Analysis

To the extent that the costs or other consequences of known or threatened cyber incidents, or risks of potential cyber incidents, represent a material event, trend or uncertainty that is reasonably likely to have a material effect on the 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, a registrant should address cybersecurity risks and cyber incidents in its Management's Discussion and Analysis of Financial Condition and Results of Operations ("MD&A"). Cyber threats can have cost implications associated with preventative measures. A successful attack could have a range of costs, depending in part on the objective of the attack (such as theft of assets, intellectual property or other proprietary information, or disruption of operations of the registrant or its business counterparties). Adverse financial impacts of successful attacks could include, for example, remediation costs, costs associated with increased protection, lost revenues, litigation costs, and reputational damage leading to lost customers.

Business Description

If one or more cyber incidents materially affect a registrant's products, services, relationships with customers or suppliers or competitive conditions, disclosure related to such cyber incident(s) should be included in the registrant's "Description of Business." In making such a determination, a registrant should consider the impact on each of its reportable segments.

Legal Proceedings

If a material pending legal proceeding to which a registrant or one of its subsidiaries is a party involves a cyber incident, the registrant may need to provide disclosure as part of "Legal Proceedings."

Financial Statement Disclosure

Cybersecurity risks and cyber incidents may have a broad impact on a registrant's financial statements, before, during and after any such incident. To the extent substantial costs are incurred, such costs may be required to be considered and accounted for under applicable Accounting Standards Codifications. To the extent the impact of a cyber incident is not readily known, a registrant may be required to develop estimates and should subsequently reassess the assumptions that underlie the estimates made in preparing its financial statements. A registrant must explain any risk or uncertainty of a reasonably possible change in its estimates in the near term that would be material to its financial statements. To the extent a cyber incident is discovered after a balance sheet date but before the issuance of the financial statements, a registrant would need to consider if the incident needs to be reflected as a subsequent event.

Disclosure Controls and Procedures

A registrant should consider the impact of any cyber attack on its ability to record, process, summarize and report information that is required to be disclosed in SEC filings, and if there is an adverse impact on such ability that renders the disclosure controls and procedures ineffective.

Comment

As is the case with other significant trends that apply broadly across the business community, the SEC expects registrants to address the implications of cyber incidents notwithstanding the fact that they are very much a fact of life in the digital age. The consequences of cyber incidents, both intentional and unintentional, can be significant, with risks ranging from increased costs to loss of customers and market confidence. As regulators in various jurisdictions focus on data privacy concerns, the risks of liability and regulatory sanctions may also increase.

The SEC guidance, while not creating new disclosure obligations, serves as a useful reminder that, as part of risk oversight and risk management processes, when registrants assess their vulnerabilities to cyber attacks, they should not lose sight of the importance of evaluating their conclusions in light of their public disclosure obligations.

The text of the SEC's Division of Corporation Finance guidance can be accessed on the SEC website at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

Mark S. Bergman is a Partner and Co-Head of the Securities and Capital Markets Group of Paul, Weiss, Rifkind, Wharton & Garrison LLP in London. He may be contacted at mbergman@paulweiss.com. Jillian M. Lutzy is an Associate and a member of the law firm's Securities and Capital Markets Group in London. She may be contacted at jlutzy@paulweiss.com.

  WDPR ISSN 1473-3579