Goodmans LLP Update

Corporate Securities Law

June 2, 2014

ISS Recommends Ouster of Target Directors After Data Breach

On December 19, 2013, Target Corporation confirmed that hackers stole information associated with approximately 40 million credit and debit card accounts of its customers during November and December of 2013. The data breach had significant consequences for Target and its shareholders including over US$80 million of expenses being incurred by Target in the past two quarters in connection with the incident, the resignations of the company's Chief Executive and Chief Information Officers, the initiation of over 80 associated claims against the company and a significant decline in the trading price of the company's shares.

Institutional Shareholder Services Inc. (ISS) believes the data breach showed that Target was inadequately prepared for the risks associated with its business and that responsibility for the oversight of those risks lay with the Audit and Corporate Responsibility Committees. In that context, ISS recommends that Target's shareholders vote against the re-election of directors who were on those Committees (seven out of 10 directors in total). Glass Lewis, another leading proxy advisor, also raised corporate governance concerns relating to the data breach but concluded that it did not require voting against the incumbent directors.

In making its recommendation, ISS highlighted the role of the audit and corporate responsibility committees in providing risk oversight and management. In the context of Target's business, ISS found that these committees should have been more cognizant of the company's exposure to cyberattacks and that there was little evidence that the company was adequately prepared for "the significant risks associated with doing business in today's electronic commerce environment". For example, Target's chief information officer at the time of the breach apparently had little information technology or data security expertise and, prior to the data breach, the company had no chief information security officer or chief compliance officer.

Although Target responded to the data breach with a number of technology and corporate governance initiatives to strengthen its risk management and cybersecurity capabilities, ISS characterized these as reactionary measures that simply highlighted the committees' failure to implement a risk management structure that might have prevented that data breach. ISS (and Glass Lewis) also criticized Target for not having an independent chair of its board of directors and suggested that this may have played a role in the board's failure to provide effective risk oversight.

ISS' recommendation against the Target directors highlights the importance of a proactive approach to risk management at the board level and that, depending on the nature of a company's business, cybersecurity can be an important aspect of good corporate governance.

Please contact any member of our Corporate Securities Group for further information.

All Updates are available at www.goodmans.ca. If you would prefer to receive this client Update by e-mail, require additional copies or would like to inform us of a change of address, please e-mail: updates@goodmans.ca. This Update is intended to provide general comment only and should not be relied upon as legal advice. © Goodmans LLP, 2014.