FERRAIUOLI LLC

CORPORATE AND INTELLECTUAL PROPERTY DEPARTMENTS

October 1, 2014

Notice to Clients and Friends

Duties of Board of Directors Regarding Cyber Security

Cyber security has become a great concern for companies and financial institutions as cyber-attacks have become more sophisticated and the increase in the number of successful attacks has been substantial. In 2013, these kinds of crimes cost companies in the United States over 10 million dollars. Due to the significant impact cyber-attacks have on companies, it has become the duty of Boards of Directors to oversee the cyber-risk management efforts of their companies.

Since the financial crisis in 2008, there has been an increased focus on Boards of Directors' oversight of risk management. In his June 10, 2014 speech during the "Cyber Risks and the Boardroom" Conference, the SEC's Luis Aguilar emphasized that it has become a duty of the Boards of Directors to ensure the proficiency of a company's cyber security measures. Although management has been primarily responsible for risk management, Boards are responsible for overseeing that the corporation has established appropriate risk management programs and that they have been properly implemented. Cyber-attacks may lead to significant business disruptions, substantial costs and negative publicity. In addition, there is also the threat of derivative lawsuits and potential liability of officers and directors for failing to implement measures to protect the company from cyber-threats. Recently, there have been a series of derivative lawsuits brought against companies and their officers and directors with regards to data breaches resulting from cyber-attacks.

According to Commissioner Aguilar, directors can begin to assess a company's possible cyber security measures by considering the Framework for Improving Critical Infrastructure Cyber security, released by the National Institute of Standards and Technology ("NIST") this past February. This Framework provides a set of industry standards and best practices for managing cyber security risks. However, in order to effectively oversee cyber-risk management and evaluate whether management is taking the appropriate steps to address cyber security issues, directors should educate themselves about cyber security and perhaps create a separate risk committee on the board. A company should also consider assigning full-time personnel to cyber security issues, as there is evidence such assignment helps prevent cyber-attacks and mitigate their impact.

In order to protect consumers and investors, companies need to constantly adapt to new circumstances. Directors need to establish the appropriate measures to prevent and respond to cyber-attacks, and also ensure that management is effectively implementing such measures. The failure to properly address these issues could lead to potential liability of officers and directors.

This document has been prepared for information purposes only and is not intended as, and should not be relied upon as legal advice. If you have any questions or comments about the matters discussed in this notice, wish to obtain more information related thereto, or about its possible effect(s) on policy or operational matters, please contact us.

Fernando J. Rovira-Rullán
frovira@ferraiuoli.com

Eugenio Torres-Oyola
etorres@ferraiuoli.com

Carlos Muñiz-Cotte
cmuniz@ferraiuoli.com

Maristella Collazo-Soto
mcollazo@ferraiuoli.com

221 Ponce de León Ave., Suite 500, San Juan, PR 00917 - **T** 787.766.7000 | **F** 787.766.7001 | www.ferraiuoli.com