PATTON BOGGS LLP

MAY 5, 2014

This alert provides only general information and should not be relied upon as legal advice. This alert may be considered attorney advertising under court and bar rules in certain jurisdictions.

For more information, contact your Patton Boggs LLP attorney or the authors listed below.

NORMA KRAYEM
nkrayem@pattonboggs.com

DEBORAH LODGE
dlodge@pattonboggs.com

MELODI GATES
mgates@pattonboggs.com

MARA GIORGIO
mgiorgio@pattonboggs.com

ABU DHABI
ANCHORAGE
DALLAS
DENVER
DOHA
DUBAI
NEW JERSEY
NEW YORK
RIYADH
WASHINGTON DC

CYBERSECURITY CLIENT ALERT

GLOBAL CYBERSECURITY RISKS CONTINUE TO RAISE RED FLAGS

WHITE HOUSE, EXECUTIVE BRANCH, CONGRESS, STATES AND EUROPEAN ALLIES CONTINUE CYBERSECURITY EFFORTS

In less than three months since the White House finalized the Cyber Framework, efforts continue across a host of fronts to secure Critical Infrastructure, retail institutions and universities against cyber threats:

→ The White House rolls out its "Big Data" report—designed to address privacy concerns amongst a growing trend to mine massive data sets of information.

→ The U.S. Department of Homeland Security (DHS) is working with all affected entities to implement the Framework and just announced a series of cyber workshops around the country for 2014-2015.

→ The Senate Intelligence Committee released a much awaited, draft cybersecurity information-sharing bill—nearly two years in the making.

→ 29 European countries kick-off a sophisticated cyber-exercise, Cyber Europe 2014 including 200 organizations and 400 cyber professionals.

→ The U.S. Department of Energy (DOE) recently issued new guidance for the electric grid's supply chain.

→ States like Connecticut are requiring more robust cybersecurity regimes from the electric utility sectors and others are looking at requiring the use of the Framework.

WHAT DO COMPANIES AND PUBLIC INSTITUTIONS NEED TO DO?

Companies and public institutions manage risk—on reputational harm, impact on customers and users, as well as on the bottom line—very differently. Regardless of the industry your business operates within, cybersecurity issues and concerns are here to stay. The best strategy to protect your institution and/or

shareholders is one that includes a comprehensive evaluation of how new and emerging policy, legal and regulatory issues will affect you.

SEC HOSTS CYBER ROUNDTABLE, BEGINS TARGETED OVERSIGHT

On March 26, 2014, the Securities and Exchange Commission (SEC) held the first ever Cyber Roundtable focusing on (1) the current landscape of cyber protections and cyber threats, (2) public company disclosures, (3) cyber impacts on market systems, and (4) impacts of cybersecurity on broker-dealers, investment advisers, and transfer agents. During the Roundtable, SEC Chairwoman Mary Jo White, who participated in the daylong event, reaffirmed that cyber threats do not discriminate and pose serious risks to critical infrastructures and financial markets.

Both the SEC and Congress have made clear that cybersecurity is an area of concern all companies need to address when considering risk. In what is considered a first round of oversight, the SEC announced on April 15, 2014 that the Office of Compliance Inspections and Examinations (OCIE) will be conducting examinations of more than 50 registered broker-dealers and registered investment advisers.

→ The OCIE examinations will focus on cybersecurity issues, including "cybersecurity governance, identification and assessment of cybersecurity risks, protection of networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and experiences with certain cybersecurity threats."

→ The OCIE examinations will assess companies' preparedness, as well as ways in which the SEC and the industry can work together to improve cybersecurity. The SEC will likely continue to focus its efforts in these areas and other sectors.

Increased SEC Focus on Cyber: This effort supports comments made by the SEC over the course of the last year and recent reports. It also reinforces a point made in November 2013 by the President's Council of Advisors on Science and Technology (PCAST) released a report entitled "Immediate Opportunities for Strengthening the Nation's Cybersecurity."

→ PCAST made six main recommendations, the most important includes a requirement that the SEC take new action: The "…SEC should mandate, for publicly held companies, the disclosure, as investment risks, of cybersecurity risk factors that go beyond current materiality tests."

NEW REPORTS HIGHLIGHT GROWING CYBER THREATS AND POSSIBILITIES OF POTENTIAL GLOBAL CYBER FAILURES

Zurich Insurance, working with the Atlantic Council, recently issued a report titled "Beyond Data Breaches: Global Interconnections of Cyber Risk." The report equates cybersecurity issues to "cyber sub-prime" and states the risk is

"…analogous to those risks that were overlooked in the U.S. sub-prime mortgage market." The report raises serious concerns over the future of increased "cyber global shocks" and identifies the seven aggregations of cyber risk.[1]

Verizon recently issued a report titled "2014 Data Breach Investigations Report," which focuses on the increasing nature of cybersecurity attacks. According to the report, "2013 may be remembered as the 'year of the retailer breach,' but a comprehensive assessment suggests it was a year of transition from geopolitical attacks to large scale attacks on payment card systems." The report tracks nine patterns of attack and analyzes the increasing nature of attacks on all sectors including Critical Infrastructure.[2]

FTC LITIGATION AGAINST WYNDHAM HOTELS: A WAKE-UP CALL FOR HOTELS, RETAIL INSTITUTIONS AND UNIVERSITIES

The Federal Trade Commission (FTC) case against Wyndham Hotels and Resorts involves a massive cybersecurity attack and data breaches that occurred on the Wyndham networks. On April 7, 2014, the federal District Court in New Jersey upheld the FTC authority to challenge the lack of sufficient data security practices as "unfair" acts or practices. The 42-page opinion included a number of key points:

→ **Substantial Injury to Consumers**: The Court found that "FTC adequately pleads 'substantial injury to consumers' and that [Wyndham] Hotels and Resorts' practices caused the injury:" "[E]xposure of consumers' personal information has caused and is likely to cause substantial consumer injury, including financial injury, to consumers and businesses. For example, Defendants' failure to implement reasonable and appropriate security measures resulted in the three data breaches . . . the compromise of more than 619,000 consumer payment card account numbers, the exportation of many of those account numbers to a domain registered in Russia, fraudulent charges on many consumers' accounts, and more than $10.6 million in fraud loss. Consumers and businesses suffered financial injury, including, but not limited to, unreimbursed fraudulent charges, increased costs, and lost access to funds or credit. Consumers and businesses also expended time and money resolving fraudulent charges and mitigating subsequent harm."

→ **Corporate Responsibility vs. Franchise Responsibility:** The Wyndham system includes hotels run by franchisees and "legally separate entities that each maintain their own computer networks and engage in their own data collection practices." Wyndham argued that the Corporation should not be held responsible for its franchisees' data security failures. However, the Court found that the FTC had asserted a legally viable claim that Wyndham had failed "to ensure Wyndham branded hotels implemented adequate information security policies and procedures prior to connecting their local networks to Hotels and Resorts' computer network."

[1] "Risk Nexus: Beyond Data Breaches: Global Interconnections of Cyber Risk." Zurich Insurance and The Atlantic Council. April 2014.
[2] "2014 Data Breach Investigations Report." Verizon. 2014.

→ While the FTC will need to prove these allegations, the case reinforces the FTC's authority to hold hotels, retailers, universities and other institutions to a "reasonableness standard," and assert that companies that fail to maintain reasonable data security practices, live up to the promises made to consumers, take preventive actions after suffering a compromise, and maintain reliable systems have engaged in "unfair" acts or practices under Section 5 of the FTC Act.