WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

WFG® CLE

Financial Regulations, Enforcement & Cybersecurity

Elizabeth P. Gray

May 16, 2017

Copyright © 2017 by Willkie Farr & Gallagher LLP. All Rights Reserved. These course materials may not be reproduced or disseminated in any form without the express permission of Willkie Farr & Gallagher LLP.

Cybersecurity as a Regulatory and Enforcement Priority Impacting Financial Services Firms

- Cybersecurity will be a top priority for financial regulators in 2017
  - SEC, CFTC, Treasury, State and International Regulators
- Treasury Secretary Mnuchin: Regulatory agencies should focus on incorporating cybersecurity in all oversight responsibilities (March 2017)
- Chair John Griffith-Jones, UK's FCA: Of the increasing risk areas that we have identified, one in particular stands out – cyber resilience (April 2017)
- Companies will face a myriad of regulations and enforcement regimes
  - Harmonization not yet a reality
- Unifying theme: Senior management and corporate boards are expected to embrace cybersecurity as an *enterprise risk* and to implement a well tested and evolving cybersecurity program -- including a well-considered *incident response plan*

Cybersecurity Risk Affects the Bottom Line

- The Yahoo! breaches present a stunning example of damage stemming from cybersecurity breaches
- SEC, DOJ and FTC investigations – civil and criminal exposure
- Shareholder lawsuits
- Loss of company value
- Loss of confidence in executives
- Board investigations and legal exposure

SEC Expectations concerning Cybersecurity

- SEC has implemented cybersecurity regulations and examinations, and initiated enforcement actions enforcing those rules
  - Focus has been on investment advisers and broker-dealers
- First series of cybersecurity-related examinations began in 2014
  - SEC has committed to continue cybersecurity exams
  - SEC's Office of Compliance Inspections and Examinations refers significant deficiencies to SEC Division of Enforcement for investigation
- The SEC has instituted multiple enforcement actions for failure to protect customer data, demonstrating its willingness to pursue punitive measures to ensure compliance with the Safeguards Rule of Regulation S-P (the "Safeguards Rule")
  - These actions signal that any informal grace period for implementing effective cybersecurity protocols, consistent with SEC guidance, has expired

What to Expect Under SEC Chair Jay Clayton?

- Clayton will expect public companies, investment advisers and broker-dealers to have comprehensive and appropriately evolving cybersecurity programs, with tested incident response plans in place
  - Cybersecurity due diligence expected in connection with IPOs and acquisitions
- Increased focus on adequacy and accuracy of disclosures about cybersecurity programs, cyber threats and breaches, and related impact
  - Jay Clayton at his confirmation hearing before the Senate Committee on Banking, Housing and Urban Affairs: "I don't think that the American…investing public…has a great appreciation for the cyber risks that our businesses face today….[A]s I look across the landscape of discussion and understanding of cyber threats and their possible impact on companies, I question whether the disclosure is where it should be."
- Enforcement Priorities: (1) Disclosure, (2) Violation of customer related rules, (3) Cyber breaches and insider/manipulative trading

SEC Enforcement of Existing Regulations

- *Morgan Stanley Smith Barney LLC* – 2016
  - An MSSB employee misappropriated data concerning 730,000 customer accounts associated with 330,000 different households over a three-year period
  - SEC found that MSSB failed to ensure its policies and procedures addressing customer information safeguards were reasonably designed to meet the objectives of the Safeguards Rule
  - ***MSSB was fined $1 million.***
- The Rule requires policies and procedures that: (i) "address administrative, technical, and physical safeguards for the protection of customer records and information" that (ii) are reasonably designed to:
  - insure the security and confidentiality of customer records and information;
  - protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
  - protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

SEC Enforcement Priorities regarding Cybersecurity

- Insider and Manipulative Trading involving a breach – "hacking to trade"
  - *SEC v. Iat Hong, Bo Zheng and Hung Chin, 2016*
  - SEC alleged three Chinese nationals reaped $3 million in unlawful profits by trading on stolen material nonpublic information; ongoing litigation
  - Defendants allegedly, directly and indirectly, hacked into the nonpublic networks of two New York-headquartered law firms and stole confidential information involving several publicly-traded companies that were engaged in merger acquisition discussions
  - Parallel criminal proceeding SDNY and foreign regulatory involvement
- Accuracy and Adequacy of public company and regulated entity disclosure
  - Track the SEC's enforcement investigation of Yahoo and its disclosure of two substantial data breaches to its senior management, Board and investors

Business Continuity / Transition Planning Rule Proposal

- In late June 2016, the SEC proposed a new rule to address potential ramifications of a temporary or permanent interruption of a registered adviser's ability to provide advisory services

- As proposed, the rule would require an adviser to:
  - Adopt and implement plans to ensure business continuity after a significant business disruption including a cybersecurity event; and business transition in the event the adviser is unable to continue providing advisory services;
  - Conduct an annual review of those plans; and
  - Comply with corresponding recordkeeping plans.

- Future of the proposed Business Continuity Rule is uncertain

State Data Security Laws – Massachusetts and New York

- The Massachusetts data protection regulation, Standards for the Protection of Personal Information of Residents of the Commonwealth ("MA Data Security Regs"), is the most detailed information data security rule in the United States

- The cornerstone of the MA Data Security Regs is the development of a comprehensive information security policy that is tailored to the size, scope and resources of the business, and to the amount of personal information to be safeguarded.

- On March 1, 2017, the New York Department of Financial Services Cybersecurity regulations ("DFS Cyber Regs") became effective. The DFS Cyber Regs impose cybersecurity requirements on entities supervised by the DFS that are doing business in New York and "operating under or required to operate under a license, registration…or similar authorization under the New York Banking Law, the Insurance Law or the Financial Services Law" -- such as banks and insurance companies.

State Data Security Laws – New York

- Some notable requirements in the DFS Cyber Regs are:
  - Implement written policies and procedures concerning third-party service providers;
  - Designation of a qualified individual to oversee and implement the Covered Entity's cybersecurity program and enforce its cybersecurity policy, serving as Chief Information Security Officer ("CISO") or comparable position;
  - Penetration testing and vulnerability assessments;
  - Notification of DFS superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred;
  - Annual reporting to the DFS superintendent, certifying that the Covered Entity is in compliance with the DFS Cyber Regs;
  - Annual reporting on cyber to the board of directors, a comparable governing body, or a Senior Officer if no such governing body exists;
  - Continuously Trained Cybersecurity Personnel;
  - Maintenance of audit trail systems.

International Regulation – UK's Financial Conduct Authority and GDPR

- Financial Conduct Authority ("FCA") views cyber resilience as top priority for financial industry
  - Committed to a cooperative approach with other international regulators
  - Expects a 'security culture' in firms of all sizes – with Board, senior management and employee commitment to cybersecurity
- FCA emphasizes:
  - Good governance
  - Identification and protection of key assets
  - Detection
  - Response and recovery
  - Information sharing with regulators and other parties

New European General Data Protection Regulation

- New European General Data Protection Regulation ("GDPR") went into effect May 2016
- Companies must come into compliance by May 25, 2018
- Establishes a number of new data protection requirements with respect to doing business with EU-resident individuals
  - New privacy notice requirements
  - New contractual requirements for service provider contracts
  - New data breach notification rules
    - Requires that as soon as data controller becomes aware of data breach it should notify EU supervisory authority without delay, where feasible within 72 hours
  - New rights for individuals
  - New accountability obligations
- Noncompliance with the GDPR could result in substantial monetary penalties