RUSKIN MOSCOU FALTISCHEK P.C.
Counselors at Law

Financial Services Industry in New York is About to be Pounded by Proposed New Cybersecurity Regulations*

On September 13, 2016, Governor Cuomo and the New York State Department of Financial Services ("NYDFS") proposed a sweeping new cybersecurity regulation for financial institutions in New York. The proposed regulation attempts to protect consumers from the consequences of a cyber-attack by forcing banks, insurance companies, and other financial institutions regulated or licensed by the New York Department of Financial Services (collectively "Covered Entities") to adopt an extensive set of cybersecurity protections. Perhaps due to Governor Cuomo's desire to set the standard with a "first-in-the-nation" regulation, New York's proposal goes significantly beyond what other regulators require, and if adopted in its present form will place heavy burdens on most Covered Entities. For instance, Covered Entities are mandated to appoint a Chief Information Security Officer, regularly conduct audits and vulnerability assessments, have their board of directors review and approve their cybersecurity policy and assess risks, encrypt certain information, and annually certify compliance to NYDFS.

Comments on the "Cybersecurity Requirements for Financial Services Companies" are due by November 12, 2016 and unless modified, will become a part of 23 N.Y.C.R.R. Pt. 500, effective on January 01, 2017. Covered Entities are required to comply by June 30, 2017 and NYDFS has the authority to impose civil and criminal penalties for noncompliance.

In other words, time is short for a Covered Entity to assess their cybersecurity risks and/or enhance their cybersecurity program. Thus, this article is designed to discuss the salient points of the proposed regulation and the potential ramifications and increased liability for Covered Entities and their senior officers.

A Chief Information Security Officer Must be Designated

A Covered Entity will be required to designate a qualified individual to act as the Chief Information Security Officer ("CISO"). The CISO will be responsible for overseeing the implementation of a cybersecurity program and policy for the financial institution. In addition to oversight, the CISO will be required to develop a report, at least bi-annually, and present it to the board of directors. The report must: (1) include an assessment of the confidentiality, integrity and availability of the Information System of the institution; (2) detail exceptions to the policy and procedures; (3) identify possible cybersecurity risks; (4) asses the effectiveness of the program; (5) propose steps to remediate any inadequacies; and (6) include a summary of all material Cybersecurity Events that effected the institution during the time period.

Compliance with this requirement can be costly. The average salary for a Chief Information Security officer in the United States is $204,000 and in New York, that salary can rise to $380,000. This requirement creates a short term and long-term cost that is above what many medium to small financial institutions will be able to afford.

There is a second option for Covered Entities. A third party service provider can fulfill this requirement as long as the Covered Entity: (1) retains responsibility for compliance; (2) designates a senior member of the Covered Entity's personnel responsible for oversight of the third-party service provider; and (3) requires the third-party service provider to maintain a cybersecurity program that meets the requirements of the regulation. However, this option comes with its own challenges, as the Covered Entity would still be liable for any breach or lack of oversight by the third-party service provider. While this option may be less costly, the Covered Entity will be giving up control but will remain subject to enforcement action for deficiencies in the work of the third-party service provider.

A Cybersecurity Program Must be Created

Covered Entities will be required to create and implement cybersecurity programs designed to include the following core security objectives:

(1) identify internal and external cyber risks by, at a minimum, identifying the Nonpublic Information stored on the Covered Entity's Information Systems, the sensitivity of such Nonpublic Information, and how and by whom such Nonpublic Information may be accessed;

(2) use defensive infrastructure and implement policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;

(3) detect Cybersecurity Events, defined as any act or attempt, successful or unsuccessful, to gain unauthorized ac-

(continued on other side)

cess to, disrupt or misuse an Information System or information stored on such Information System;

(4) respond to identified or detected Cybersecurity Events to mitigate negative effects;

(5) promptly recover from Cybersecurity Events and restore normal operations and services; and

(6) fulfill all regulatory reporting obligations.

As part of its cybersecurity program, a Covered Entity will also be required to establish a written cybersecurity policy that covers fourteen different areas: (1) information security; (2) data governance and classification; (3) access controls and identity management; (4) business continuity and disaster recovery planning and resources; (5) capacity and performance planning; (6) systems operations and availability concerns; (7) systems and network security; (8) systems and network monitoring; (9) systems and application development and quality assurance; (10) physical security and environmental controls; (11) customer data privacy; (12) vendor and third-party service provider management; (13) risk assessment; and (14) incident response.

Moreover, the proposed regulation explicitly requires the board of directors and senior management to be intimately involved with the cybersecurity program. As indicated above, the Board of Directors must review the cybersecurity policy and assess risks with the CISO at least twice annually. Indeed, the chairperson of the board or senior officer must provide a Certification of Compliance with the NYDFS regulation and maintain records that support the certification for at least five years and make the documentation available to NYDFS upon request. This annual compliance requirement opens the door to significant liability for board members and senior officers if the purported compliance is false or inadequate.

Cybersecurity Event Notification to NYDFS

A troubling provision is the mandated requirement for a Covered Entity to notify the NYDFS within seventy-two hours of becoming aware of a Cybersecurity Event reasonably likely to materially affect normal operations of the Covered Entity or when a Cybersecuirty Event involves "the actual or potential unauthorized tampering with, or access to or use of, Nonpublic Information." As an initial matter, seventy-two hours is unrealistic. In the vast majority of cybersecurity incidents, it is impossible to ascertain the facts surrounding a Cybersecurity Event (or whether one actually occurred) in such a short time frame given that a legal and technical team must determine the nature and scope of a cybersecurity incident through forensics, data analysis and an assessment of the affected systems. Moreover, Cybersecurity Event is defined broadly and it is unclear what constitutes an unsuccessful attempt. In other words, as it currently stands, a Covered Entity would be required to report an event before it can determine with certainty whether Nonpublic Information was even accessed.

How Does This Effect You?

The mandatory requirements are vast and will undoubtedly result in a material increase in operational and compliance costs for Covered Entities. Regardless of whether a Covered Entity has an established cybersecurity program, there will be limited time to assess cybersecurity risks and implement the stringent requirements of New York's proposed new regulations. Thus, it is essential that a Covered Entity immediately begin working towards compliance, including involving its board and senior management in assessing cyber-risks and making it part of the company's overall risk management framework.

What You Can Do Now.

Comments on the proposed new regulations should be submitted in order to help New York create a more realistic and viable plan. The proposed regulations are currently in a 45-day comment period and any comments must be submitted to the New York State Department of Financial Services by November 12, 2016. If you are interested learning more about proposed regulation or making a comment, please do not hesitate to contact us with any questions.

**John J. Cooney, Esq. is a partner at Ruskin Moscou Faltischek and chair of the Firm's Cybersecurity and Data Privacy practice group. He is also a member of the Firm's White Collar Crime and Investigations practice group and Health Law Department. Mr. Cooney was trained as a software engineer and had over a decade of experience analyzing and developing technology solutions for Fortune 500 companies. He can be reached via e-mail at jcooney@rmfpc.com. Nicole Della Ragione is a Law Clerk at the firm and a member of its cybersecurity and Data Privacy practice group. She can reached at 516-663-6687 or via email at ndellaragione@rmfpc.com. Melvyn B. Ruskin, Esq. is a partner at the firm, chair emeritus of the firms' Health Law Department and a member of the firm's Corporate and Securities Department and Cybersecurity and Data Privacy practice group. He can be reached via email at mruskin@rmfpc.com*

---

[1] Press Release, New York Department of Financial Services, Governor Cuomo Announces Proposal of First-in-the-Nation Cybersecurity Regulation to Protect Consumers and Financial Institutions, (Sept. 13, 2016), http://www.dfs.ny.gov/about/press/pr1609131.htm.

[2] Cybersecurity Requirements for Financial Services Companies, 23 N.Y.C.R.R. Pt. 500 (2016).

[3] 23 N.Y.C.R.R. § 500.04.

[4] Steve Morgan, Top Cyber Security Salaries in U.S. Metros Hit $380,000, Forbes (Jan. 9, 2016 03:59 PM), http://www.forbes.com/sites/stevemorgan/2016/01/09/top-cyber-security-salaries-in-u-s-metros-hit-380000/#7a6345e477b4 (citing Rising CISO Salary & Job Demands Infograph, SILIVERBULL, http://www.silverbull.co/rising-ciso-demand-salaries-infographic).

[5] 23 N.Y.C.R.R. § 500.02.

[6] 23 N.Y.C.R.R. § 500.03.

[7] 23 N.Y.C.R.R. § 500.17.