New York Announces a First-In-The-Nation Cybersecurity Regulation That Will Apply to Banks, Insurance Companies and Other Financial Institutions

hugheshubbard.com client advisory

On September 13, 2016, New York Governor Andrew M. Cuomo announced a new "first-in-the-nation" cybersecurity regulation, which will become effective January 1, 2017. The proposed regulation will require banks, insurance companies and other financial services institutions regulated by the New York State Department of Financial Services to establish and maintain a comprehensive cybersecurity program. The regulation, which will become 23 NYCRR Part 500 (Financial Services Law), is subject to a 45-day notice and comment period before it becomes final.

The proposed regulation requires "each company to assess its specific risk profile and design a program that addresses its risks in robust fashion." It calls for regulated companies that do not already have such programs in place to "move swiftly and urgently" to adopt one. The onus for compliance will be on senior management, which "must take this issue seriously and be responsible for the organization's cybersecurity program" and "file an annual certification confirming compliance with these regulations."

The proposed regulation contains detailed and particularized requirements with which a "Covered Entity" must comply. That includes any individual or entity operating under or required to operate under a license, registration, charter, certificate permit, accreditation or similar authorization under the banking law, the insurance law or the financial services law.

There are certain, limited exemptions for a Covered Entity with (1) fewer than 1000 customers in each of the last three calendar years, and (2) less than $5,000,000 in gross annual revenue in each of the last three fiscal years, and (3) less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates.

If the proposed regulation is implemented as written, Covered Entities will have 180 days from the effective date, January 1, 2017, to comply with the new requirements. The full text of the proposed regulation is available online at the Department of Financial Services website. We summarize the key requirements below.

Establishment of a Cybersecurity Program

Under the new regulation, a Covered Entity will have to maintain a cybersecurity program designed to "ensure the confidentiality, integrity and availability of the company's Information Systems." The regulation does not specify the form that the program must take, but requires that it be "designed to perform the following core cybersecurity functions:" (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 the implementation of policies and procedures to protect the company's Information Systems and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts; (3) detect

Cybersecurity Events - which are defined broadly to include "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on an Information System;" (4) respond to identified or detected Cybersecurity Events to mitigate any negative effects; (5) recover from Cybersecurity Events and restore normal operations and services; and (6) fulfill all regulatory reporting obligations.

Adoption of a Cybersecurity Policy

In addition to a cybersecurity program, each Covered Entity must also implement and maintain a written cybersecurity policy. This policy must be reviewed by the board of directors or its equivalent and approved by a Senior Officer of the company. Review and approval of the policy must occur "as frequently as necessary to address the cybersecurity risks applicable" to the company and at least annually. As for the policy itself, it must address (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.

Designation of a Chief Information Security Officer

Each Covered Entity is required to designate a Chief Information Security Officer ("CISO"), who must present a written report to the board of directors or its equivalent bi-annually. The report must (1) assess the confidentiality, integrity and availability of the company's Information Systems, (2) detail exceptions to the company's cybersecurity procedures and policies, (3) identify cyber risks to the company, (4) assess the effectiveness of the company's cybersecurity program, (5) propose steps to remediate any inadequacies identified in the company's cybersecurity program, and (6) include a summary of all material Cybersecurity Events that affected the company during the time period addressed by the report.

Penetration Testing and Vulnerability Assessments

As part of its cybersecurity program, a Covered Entity must conduct penetration testing of its Information Systems at least annually and vulnerability assessments of its systems at least quarterly.

Audit Trail Systems

The cybersecurity program must include implementing and maintaining audit trail systems capable of performing certain enumerated functions. Generally, these systems must be able to log user access and system events, as well as permit the reconstruction of financial transactions in the event of a Cybersecurity Event. The company must maintain records produced as part of an audit trail for at least six years.

Access Privileges

As part of its cybersecurity program, a Covered Entity must limit access privileges to Information Systems that contain Nonpublic Information. Only individuals who require access to these systems to perform their responsibilities may be granted access. The regulation requires the Covered Entity to periodically review these access privileges to ensure that they remain up-to-date.

Application Security

The cybersecurity program must include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications used by the company, and procedures for assessing and testing the security of all externally developed applications. The CISO must review, assess and update these procedures, guidelines and standards at least annually.

Annual Risk Assessment
A Covered Entity must conduct a risk assessment of its Information Systems at least annually. The risk assessment must be documented in writing and be done in accordance with written policies and procedures. These policies and procedures must include (1) the criteria for evaluating and categorizing identified risks; (2) the criteria for assessing the confidentiality, integrity and availability of the company's Information Systems, including the adequacy of existing controls; and (3) requirements for documenting how identified risks will be mitigated or accepted.

Cybersecurity Personnel and Intelligence
In addition to designating a CISO, a Covered Entity must have sufficient personnel to manage its cybersecurity risks and perform core cybersecurity functions. A Covered Entity may use qualified third-parties to assist with these tasks. With respect to its own cybersecurity personnel, a Covered Entity must provide for and require them to attend regular cybersecurity update and training sessions.

Third-Party Information Security Policy
A Covered Entity must have written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, third parties. These policies and procedures must address (1) the identification and risk assessment of third parties with access to Information Systems or Nonpublic Information; (2) minimum cybersecurity practices required to be met by such third parties; (3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such third parties; and (4) periodic assessment, at least annually, of such third-parties and the continued adequacy of their cybersecurity practices.

Multi-Factor Authentication
A Covered Entity must (1) require Multi-Factor Authentication for any individual accessing the Covered Entity's internal systems or data from an external network; (2) require Multi-Factor Authentication privileged access to database servers that allow access to Nonpublic Information; (3) require Risk-Based Authentication to access web applications that capture, display or interface with Nonpublic Information; and (4) support Multi-Factor Authentication for any individual accessing web applications that capture, display or interface with Nonpublic Information.

Limitations on Data Retention
A Covered Entity must have policies and procedures for the timely destruction of any Nonpublic Information that is no longer necessary or required to be retained by law or regulation.

Training of Personnel
A Covered Entity must provide for and require all personnel to attend regular cybersecurity awareness training sessions that are updated to reflect risks identified by the Covered Entity in its annual assessment of risks.

Monitoring of Authorized Users
A Covered Entity must implement risk-based policies, procedures and controls to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information.

Encryption of Nonpublic Information
A Covered Entity must encrypt all Nonpublic Information held or transmitted by the Covered Entity both in transit and at rest. To the extent that encryption of Nonpublic Information is currently infeasible, the regulation permits the use of alternative controls for specified amounts of time.

Incident Response Plan
A Covered Entity must have a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event affecting the confidentiality, integrity or availability of the company's Information Systems or the continuing functionality of any aspect of its business. The

response plan must address (1) the internal processes for responding to a Cybersecurity Event; (2) the goals of the incident response plan; (3) the definition of clear roles, responsibilities and levels of decision-making authority; (4) external and internal communications and information sharing; (5) remediation of any identified weaknesses in Information Systems and associated controls; (6) documentation and reporting regarding Cybersecurity Events and related incident response activities; and (7) the evaluation and revision of the incident response plan following a Cybersecurity Event.

Notification to the Superintendent

A Covered Entity must notify the superintendent of any Cybersecurity Event that has a reasonable likelihood of materially affecting the normal operation of the Covered Entity or that affects Nonpublic Information. The notice must be given as promptly as possible but no later than 72 hours after the Covered Entity becomes aware of the Cybersecurity Event.

Annual Certifications

Beginning in 2018, a Covered Entity must submit to the superintendent by January 15, a written statement certifying that the Covered Entity is in compliance with the regulation. All records, schedules and data supporting the certificate must thereafter be maintained for a period of five years.

While the proposed regulation is not yet final, Covered Entities should begin preparing to meet its requirements. If you would like assistance in doing so or you would like to submit a public comment regarding the proposed regulation, please contact us.

Dennis S. Klein, *Partner*
+1 (305) 379-5574
dennis.klein@hugheshubbard.com

Seth D. Rothman, *Partner*
+1 (212) 837-6872
seth.rothman@hugheshubbard.com

September 2016