Cullen | Dykman

New York State Adopts Cybersecurity Regulation

February 28, 2017

New York State has adopted a new regulation requiring banks, insurance companies and other persons and entities operating under certain provisions of New York law to adopt comprehensive programs for preventing, detecting and responding to cybersecurity events. This regulation is the first of its kind at the state level and imposes significant new requirements on financial service firms that qualify as a "Covered Entity" as defined below.

The final version of the cybersecurity regulation (the "Cybersecurity Regulation") was issued by the New York State Department of Financial Services ("DFS") on February 16, 2017, and takes effect on March 1, 2017 (although compliance is not required until 180 days – and with respect to certain provisions, one year, 18 months or two years — after the effective date). The Cybersecurity Regulation requires covered firms to, among other things, establish and maintain a cybersecurity program, create an immediate incident response plan for security breaches, and designate a qualified individual to serve as Chief Information Security Officer ("CISO").

I. Covered Entities

The Cybersecurity Regulation applies to any "Covered Entity," which is defined as a Person operating under or required to operate under a license, registration, charter, certificate, permit accreditation or similar authorization under the New York Banking Law, Insurance Law or Financial Services Law. This will include, for instance, New York State-chartered banks, licensed mortgage bankers, registered mortgage brokers, and licensed insurance companies and agencies.

A bank chartered under federal law or the laws of a state other than New York will not be subject to the Cybersecurity Regulation, but a subsidiary or affiliated entity of such a bank may be subject to the Cybersecurity Regulation if such entity operates under a license, registration, charter, certificate, permit, accreditation or similar authorization from DFS. For instance, a subsidiary of an out-of-state or national bank that is licensed in New York to sell insurance or other non-deposit products will be subject to the Cybersecurity Regulation.

Even if an entity is deemed a "Covered Entity" subject to the Cybersecurity Regulation, there are certain limited exemptions that might apply. The exemptions to otherwise being deemed a Covered Entity are as follows:

- If the Covered Entity has (i) fewer than ten employees, including any independent contractors, of the Covered Entity or its Affiliates located in New York or responsible for business of the Covered Entity; or (ii) less than $5,000,000.00 in gross annual revenue in each of the last three fiscal years from New York business operations of the Covered Entity and its Affiliates; or (iii) less than $10,000,000.00 in year-end total

assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates, it shall be exempt from certain requirements of the Cybersecurity Regulation, including the requirement to have a CISO, perform penetration testing and vulnerability assessments, and encryption requirements.

- If an employee, agent, representative or designee of a Covered Entity, is itself a Covered Entity, then they are exempt from requirements of the Cybersecurity Regulation and need not develop its own cybersecurity program to the extent it can be covered under the cybersecurity program of the other Covered Entity.
- If the Covered Entity does not directly or indirectly operate, maintain, utilize or control any Information Systems, and it does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information, it will be exempt from most of the requirements of the Cybersecurity Regulation.
- If a Covered Entity under Article 70 of the Insurance Law (addressing captive insurance companies) does not and is not required to directly or indirectly control, own, access, generate, receive or possess Nonpublic Information other than information relating to its corporate parent company (or Affiliates) then it will be exempt from most of the requirements of the Cybersecurity Regulation.

If a Covered Entity falls under any of the above-listed exemptions, the Covered Entity must file a Notice of Exemption in the form set forth in Appendix B of the Cybersecurity Regulation within 30 days of the Covered Entity's determination that it is exempt. In the event that a Covered Entity, as of its most recent fiscal year end, ceases to qualify for an exemption, it shall have 180 days from such fiscal year end to comply with the requirements of the Cybersecurity Regulation.

In addition, the Cybersecurity Regulation sets forth a separate exemption for the following people, if they do not already otherwise qualify as a Covered Entity: (i) Persons subject to Insurance Law Section 1110 (charitable annuity societies); (ii) Persons subject to Insurance Law Section 5904 (risk retention groups); and (iii) any accredited reinsurer or certified reinsurer that has been accredited or certified under New York insurance regulations.

II. Requirements of Cybersecurity Regulation

1.Cybersecurity Program

A Covered Entity is required to maintain a cybersecurity program designed to ensure the confidentiality, integrity, and availability of the Covered Entity's Information Systems. The cybersecurity program must be based on the Covered Entity's Risk Assessment (discussed in Section 3 below), and be designed to perform core cybersecurity functions, such as: (i) identifying and assessing internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems; (ii) using defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those systems, from unauthorized access, use or other malicious acts; (iii) detecting Cybersecurity Events; (iv) responding to identified or detected Cybersecurity Events to mitigate any negative effects; (v) recovering from Cybersecurity Events and restoring normal operations and services; and (vi) fulfilling applicable regulatory reporting obligations. A Covered Entity may meet the cybersecurity program requirement by adopting the relevant and applicable provisions of a cybersecurity program maintained by an Affiliate, provided that such provisions satisfy the requirements of this Part, as applicable to the Covered Entity.

2. Cybersecurity Policy

A Covered Entity is required to implement and maintain a written cybersecurity policy setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those systems, and how it plans to implement those policies and procedures. The policy must be approved by the Covered Entity's board of directors or a Senior Officer. The policy must be based on a Covered Entity's individual Risk Assessment (discussed in Section 3 below) and, to the extent applicable, must contain policies regarding: (i) information security; (ii) data governance and classification; (iii) asset inventory and device management; (iv) access controls and identity management; (v) business continuity and disaster recovery planning and resources; (vi) systems operations and availability concerns; (vii) systems and network security; (viii) systems and network monitoring; (ix) systems and application development and quality assurance; (x) physical security and environmental controls; (xi) customer data privacy; (xii) vendor and Third Party Service Provider management; (xiii) risk assessment; and (xiv) incident response.

3. Risk Assessment

A Covered Entity's cybersecurity program and cybersecurity policy must be based on the Covered Entity's periodic Risk Assessment of its Information Systems. The Risk Assessment must be ever-evolving to keep up with new potential threats as well as to understand how certain risks may change within the Covered Entity's own systems. The Risk Assessment must be carried out in accordance with written policies and procedures which must include the following: (i) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity; (ii) criteria for the assessment of confidentiality, integrity, security and availability of the Information Systems and Nonpublic Information given the Covered Entity's current risk environment and assessment; and (iii) requirements and procedures for how the Covered Entity will mitigate or remedy the identified risks in its Information Systems.

Compliance with the obligation to complete a Risk Assessment is required one year after March 1, 2017, effective date of the Cybersecurity Regulation. However, the cybersecurity program and cybersecurity policy, both of which must be based on the Risk Assessment, are required to be in place 180 days after the effective date.

4. Chief Information Security Officer

A Covered Entity is required to designate a qualified individual to serve as the Covered Entity's CISO responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy. This requirement may be met by using an Affiliate or a Third Party Service Provider, so long as the Covered Entity: (i) retains responsibility for compliance with the Cybersecurity Regulation; (ii) designates a senior member of its personnel responsible for oversight of the Third Party Service Provider; and (iii) requires the Third Party Service Provider to maintain a cybersecurity program that meets the requirements of the regulation.

A Covered Entity's CISO is required to develop a written report regarding the Covered Entity's cybersecurity program and material cybersecurity risks and present it to the Covered Entity's board of directors, or an equivalent governing body, annually. If a board of directors or the equivalent governing body does not exist, the CISO shall prepare and present the report to the Senior Officer in charge of overseeing the cybersecurity

program. The report should consider, to the extent applicable: (i) the confidentiality of Nonpublic Information and the integrity and security of the Covered Entity's Information Systems; (ii) the Covered Entity's cybersecurity policies and procedures; (iii) material cybersecurity risks; (iv) the overall effectiveness of the Covered Entity's cybersecurity program; and (v) material Cybersecurity Events that involved the Covered Entity during the time period addressed by the report.

5. Penetration Testing and Vulnerability Assessments

A Covered Entity's cybersecurity program must include monitoring and testing, in accordance with the Covered Entity's Risk Assessment, designed to assess the effectiveness of the Covered Entity's cybersecurity program. Monitoring and testing must include continuous monitoring or periodic Penetration Testing and vulnerability assessments.

Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities must conduct: (i) annual Penetration Testing of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and (ii) bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment.

6. Audit Trail

As part of its cybersecurity program, each Covered Entity must securely maintain systems that, based on the Covered Entity's Risk Assessment, are (i) designed to reconstruct material financial transactions sufficient to support normal operations and obligations; and (ii) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the Covered Entity's normal operations. Any records associated with subsection (i) above must be maintained by the Covered Entity for not fewer than five years while records associated with subsection (ii) above must be maintained for not fewer than three years.

7. Access Privileges

As part of its cybersecurity program, a Covered Entity must limit user access privileges to Information Systems that provide access to Nonpublic Information and must periodically review such access privileges.

8. Application Security

A Covered Entity must implement written procedures, guidelines, and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment. These written procedures must be periodically reviewed, assessed and updated, if applicable, by the Covered Entity's CISO (or a qualified designee).

9. Cybersecurity Personnel and Intelligence

A Covered Entity is required to utilize qualified personnel in managing its cybersecurity risks and performing and implementing its main cybersecurity functions under its cybersecurity program. The Covered Entity must also provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks, and verify that key cybersecurity personnel takes steps to maintain current knowledge of changing cybersecurity threats and countermeasures. A Third Party Service Provider or Affiliate may assist the Covered Entity to ensure compliance with this requirement.

10. Third Party Service Provider Security Policy

A Covered Entity must implement written policies and procedures designed to ensure the security of its Information Systems and Nonpublic Information when dealing with Third Party Service Providers. Such policies and procedures are to be based on the Covered Entity's Risk Assessment and shall address to the extent applicable: (i) the identification and risk assessment of Third Party Service Providers; (ii) minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity; (iii) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and (iv) periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

Furthermore, these policies and procedures must include relevant guidelines for ensuring certain contractual protections are implemented in all agreements with such Third Party Service Providers, including the use of encryption, access controls, proper incident response protocols and certain representations and warranties addressing the Third Party Service Provider's ability to properly protect the Covered Entity's Information Systems and Nonpublic Information. An agent, employee, representative or designee of a Covered Entity who itself is a Covered Entity does not need to create its own Third Party Information Security Policy as long as such agent, employee, representative or designee follows the required policy of the Covered Entity.

11. Multi-Factor Authentication

A Covered Entity must use effective controls, which may include, based on its own Risk Assessment, Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to its Information Systems and Nonpublic Information. Multi-Factor Authentication must be used by any individual attempting to access the internal system of a Covered Entity from an external location unless the CISO has approved in writing other reasonably equivalent or more secure controls.

12. Data Retention

As part of its cybersecurity program, a Covered Entity must implement policies and procedures regarding the periodic disposal of any Nonpublic Information that is no longer necessary for business operations or another legitimate business purpose, except where such information is otherwise required to be retained by law or regulation.

13. Training and Monitoring

As part of its cybersecurity program, 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 by such Authorized Users. In addition, the Covered Entity must provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.

14. Encryption or Nonpublic Information

As part of its cybersecurity program, and based on its Risk Assessment, a Covered Entity must implement controls, such as encryption, to protect any Nonpublic Information held or transmitted by the Covered Entity, while in transit and at rest. If a Covered Entity determines that encryption is infeasible, it may utilize effective alternative compensating controls as long as they are reviewed and approved by the CISO and subsequently reviewed by the CISO on an annual basis going forward.

15. Incident Response Plan

As part of its cybersecurity program, a Covered Entity must establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event which materially impacts the confidentiality, integrity and availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations. The plan should address the following areas: (i) the internal processes for responding; (ii) the ultimate goals of the incident response plan; (iii) the definition of clear roles, responsibilities and decision-making authority; (iv) external and internal communications and information sharing; (v) identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls; (vi) documentation and reporting regarding Cybersecurity Events and related incident response activities; and (vii) the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

16. Notices to Superintendent

A Covered Entity must notify the Superintendent of Financial Services as promptly as possible, but in no event later than 72 hours, after a determination that a Cybersecurity Event has occurred that is one of the following: (i) a Cybersecurity Event which would otherwise require notice to be provided to any government body, self-regulatory agency or other supervisory body; or (ii) a Cybersecurity Event that has a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity. Please note that the Cybersecurity Regulation's specific timing requirement is separate and in addition to the existing security breach notification obligations imposed in New York under General Business Law Section 899-aa.

In addition, a Covered Entity must provide the Superintendent of Financial Services with a written statement annually certifying that the Covered Entity was in compliance with the requirements set forth in the Cybersecurity Regulation for the previous year. The written statement shall be submitted no later than February 15 (in the form provided in Appendix A of the Regulation). All records used to support this compliance shall be kept by the

Covered Entity for at least five years. If the Covered Entity identifies areas, systems or processes that require material improvement, updating or redesign, the Covered Entity must document the identification and remedial efforts it has planned to address such areas, systems or processes and ensure such documentation is available for inspection by the Superintendent.

17. Compliance Dates

The Cybersecurity Regulation is effective on March 1, 2017, but compliance is not required until 180 days after the effective date. In addition, DFS has provided specific transitional periods for certain requirements. The additional transitional periods are as follows:

- One year from the effective date to comply with the requirements of the following sections: (i) the annual reporting to the board of directors or equivalent governing body by the CISO; (ii) Penetration Testing and Vulnerability Assessments; (iii) Risk Assessment; (iv) Multi-Factor Authentication and (v) training for all personnel.
- Eighteen months from the effective date to comply with the requirements of the following sections: (i) audit trails; (ii) application security; (iii) limitations on Data Retention; (iv) monitoring Authorized Users access to the systems; and (v) encryption of Nonpublic Information.
- Two years from the effective date to comply with the requirements of the Third Party Service Provider security policy.

III. Further Information

The DFS Cybersecurity Regulation may be found here: http://www.dfs.ny.gov/legal/regulations/adoptions/rf23-nycrr-500_cybersecurity.pdf

If you have any questions regarding the final Cybersecurity Regulation or cybersecurity policies and procedures in general, please feel free to contact Joseph D. Simon at 516-357-3710 or via email at jsimon@cullenanddykman.com or Jeff Fowler at 516-296-9134 or via email at jfowler@cullenanddykman.com.

1. "*Person*" means any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association.
2. "*Affiliate*" means any Person that controls, is controlled by or is under common control with another Person. For purposes of this subsection, the control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise.
3. *"Information System(s)"* means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.
4. *"Nonpublic Information"* shall mean all electronic information that is not publicly available information and is: (i) business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity; (ii) any information concerning an individual which because of name, number, personal mark, or other identifiers can be used to identify such individual, in combination with any one or more of the following data elements: (a) social security number; (b) drivers' license number or non-driver identification card number; (c) account number, credit or debit card number, (d) any security code, access code or password that would permit access to an individual's financial account, or (e) biometric records; and (iii) any information or data, except age or gender, in any form or medium created by or derived from a

health care provider or an individual and that relates to (z) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (y) the provision of health care to any individual, or (x) payment for the provision of health care to any individual.

5. *"Cybersecurity Event"* means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.
6. *"Senior Officer(s)"* means the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity, including a branch or agency of a foreign banking organization subject to this Part.
7. "*Third Party Service Provider(s)"* means a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity, and (iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity.
8. *"Penetration Testing"* means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside the Covered Entity's Information Systems.
9. "*Multi-Factor Authentication*" means authentication through verification of at least two of the following types of authentication factors: (i) knowledge factors, such as a password; (ii) possession factors, such as a token or text message on a mobile phone; or (iii) Inherence factors, such a biometric characteristic.
10. "*Risk-Based Authentication*" means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions.
11. "*Authorized User*" means any employee, contractor, agent or other Person that participates in the business operations of a Covered Entity and is authorized to access and use any Information Systems and data of the Covered Entity.

Practices

- Banking and Financial Services
- Regulatory and Compliance

Industries

- Financial Institutions

Attorneys

- Joseph D. Simon