Cybersecurity Regulation for Financial Services Companies: New York State Leads the Way

Financial services companies are facing new and increased risks of cyber-attacks that have the potential to significantly disrupt both the companies and their customers, and potentially to impact the entire U.S. economy. As a result, the New York State Department of Financial Services has issued a far-reaching, "first-in-the-nation," cybersecurity regulation that requires financial services companies regulated in New York to adopt a program and policy to prevent, detect, and respond to cybersecurity threats. This article discusses who is subject to the regulation and the requirements that are imposed, and provides insight on how the regulation is likely to impact the financial services industry as a whole.

JOSEPH D. SIMON AND ELIZABETH A. MURPHY

The cyber-attack was extremely well coordinated. The hackers created an automatic sell-off in certain stocks through stolen administrator accounts, and then introduced counterfeit and malicious telecommunications equipment to divert attention from the sell-off. They then unleashed a custom computer virus, disrupted government websites through a distributed denial of service attack, and corrupted the source code of financial applications widely used in the financial services market. The attack impacted over 50 entities in the financial services industry.

Luckily, this cyber-attack, known as "Quantum 2" and conducted in 2013, was just an exercise that simulated a systemic cyber-attack on the U.S. financial system. But financial services regulators are fearful that actual cyber-attacks on banks and other financial services companies could have a devastating impact on companies, individuals, and the U.S. economy as a whole. It is against this backdrop that the New York State Department of Financial Services (DFS) issued a "first-in-the-nation" cybersecurity regulation on February 16, 2017, imposing significant requirements on financial services companies regulated in New York to adopt a program and policy to prevent, detect, and respond to cybersecurity threats.

DFS surveyed nearly 200 regulated financial institutions to obtain insight into the financial services industry's efforts to prevent cybercrime. The first version of the cybersecurity regulation was issued by DFS in September 2016 (the "Original Proposed Regulation"). Based on public comment, DFS issued an updated proposed regulation in December 2016 (the "Updated Proposed Regulation") that modified some of the requirements under the Original Proposed Regulation. After considering public comments on the Updated Proposed Regulation, DFS adopted the final cybersecurity regulation on February 16, 2017 (the "Cybersecurity Regulation" or "Regulation").

Found in new Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York,[1] the Cybersecurity Regulation requires 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 threats. The Regulation is highly detailed and far-reaching in scope, extending not just to customer or personal information, but also to business information and cybersecurity incidents that affect business operations.

Joseph D. Simon is a partner, and Elizabeth A. Murphy is an associate, in the Garden City, New York, office of Cullen and Dykman LLP. They both focus on regulatory and compliance matters for financial institutions. They may be reached by email, respectively, at jsimon@cullenanddykman.com and emurphy@cullenanddykman.com.

[1] N.Y. Comp. Codes R. & Regs. tit. 23, pt. 500 (2016).

In issuing the Regulation, DFS recognized the significant concentration of insurance, banking, and financial services entities in New York. In his announcement of the final version of the Cybersecurity Regulation, Governor Andrew Cuomo declared that "New York is the financial capital of the world and it is critical that we do everything in our power to protect consumers and our financial system from the ever increasing threat of cyber-attacks."[2] Therefore, the Cybersecurity Regulation is expected to play an important role in shaping cybersecurity programs across the nation.

Banks and other financial services companies that are chartered under federal law or the laws of a state other than New York, and that are not operating under an authorization from DFS, will not be subject to the Cybersecurity Regulation. However, a subsidiary or affiliate of such a bank might be, if the entity operates under a license, registration, charter, certificate, permit, accreditation, or similar authorization from DFS.

The Cybersecurity Regulation was effective March 1, 2017 ("Effective Date"), however there is a phase-in of compliance requirements. Compliance with certain provisions, such as the requirement to maintain a cybersecurity program and policy, is not required until August 28, 2017. DFS has provided extended transitional periods for other requirements under the Regulation. These transitional periods are as follows:

- *March 1, 2018,* to comply with the requirements regarding: (1) the Chief Information Security Officer's (CISO) annual report, (2) Penetration Testing[3] and vulnerability assessments, (3) Risk Assessment,[4] (4) Multi-Factor Authentication,[5] and (5) cybersecurity awareness training for all personnel;
- *September 3, 2018,* to comply with the requirements regarding: (1) audit trails, (2) application security, (3) limitations on data retention, (4) monitoring of Authorized Users,[6] and (5) encryption of Nonpublic Information[7]; and
- *March 1, 2019,* to comply with the requirements of the Third Party Service Provider[8] security policy.

APPLICABILITY OF THE CYBERSECURITY REGULATION

Covered Entities. The Cybersecurity Regulation applies to any "Covered Entity," defined as "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the [New York] Banking

[2] "Governor Cuomo Announces First-in-the-Nation Cybersecurity Regulation Protecting Consumers and Financial Institutions from Cyber-Attacks to Take Effect March 1," available at https://www.governor.ny.gov/news/governor-cuomo-announces-first-nation-cybersecurity-regulation-protecting-consumers-and (last updated Feb. 16, 2017).

[3] "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." 23 NYCRR § 500.01(h).

[4] "Risk Assessment means the risk assessment that each Covered Entity is required to conduct under" the Cybersecurity Regulation. 23 NYCRR § 500.01(k).

[5] "Multi-Factor Authentication means authentication through verification of at least two of the following types of authentication factors: (1) knowledge factors, such as a password; or (2) possession factors, such as a token or text message on a mobile phone; or (3) inherence factors, such as a biometric characteristic." 23 NYCRR § 500.01(f).

[6] "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." 23 NYCRR § 500.01(b).

[7] "Nonpublic Information shall mean all electronic information that is not Publicly Available Information and is: (1) 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; (2) any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records; (3) 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 (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual." 23 NYCRR § 500.01(g). "Publicly Available Information means any information that a Covered Entity has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law." 23 NYCRR § 500.01(j).

[8] "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." 23 NYCRR § 500.01(n).

Law, Insurance Law or Financial Services Law."[9] The types of entities subject to the Regulation include many companies that have already been focused on cybersecurity, such as banks, credit unions, and insurance companies. However, a plethora of other companies—including, e.g., insurance agents, mortgage bankers, mortgage brokers, check cashers, bail bond agents, and sales finance companies—subject to the Regulation may be focusing on cybersecurity for the first time, and may find compliance with the Regulation to be fairly challenging.

Banks and other financial services companies that are chartered under federal law or the laws of a state other than New York, and that are not operating under an authorization from DFS, will not be subject to the Cybersecurity Regulation since such entities do not fall within the definition of a Covered Entity. However, a subsidiary or affiliate of such a bank may be subject to the Regulation if the entity operates under a license, registration, charter, certificate, permit, accreditation, or similar authorization from DFS. For instance, a subsidiary or affiliate 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.

Exemptions. The Cybersecurity Regulation sets forth certain exemptions from the Regulation even if an entity is deemed to be a Covered Entity. Limited exemptions exempt a Covered Entity from only selected provisions; full exemptions, applicable to only a narrow group of Covered Entities, provide exemption from all provisions of the Regulation.

Limited Exemptions. The limited exemptions in the Cybersecurity Regulation are as follows:

- If a Covered Entity has (1) fewer than 10 employees, including any independent contractors, of the Covered Entity or its Affiliates[10] located in New York or responsible for the business of the Covered Entity, or (2) less than $5 million 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 (3) less than $10 million in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates, then the Covered Entity will be exempt from the requirements to (1) appoint a CISO, (2) conduct Penetration Testing and vulnerability assessments, (3) maintain audit trails, (4) maintain procedures to ensure application security, (5) utilize qualified cybersecurity personnel and conduct training for such personnel, (6) utilize Multi-Factor Authentication or Risk-Based Authentication,[11] (7) monitor Authorized Users and provide regular cybersecurity awareness training for all personnel, (8) maintain controls to protect Nonpublic Information held or transmitted, and (9) develop a written incident response plan.[12]
- An employee, representative, agent, or designee of a Covered Entity, who is itself a Covered Entity, is exempt from the Cybersecurity Regulation and is not required to create a cybersecurity program to the extent that the employee, representative, agent, or designee is covered by the cybersecurity program of the Covered Entity.[13]
- A Covered Entity that does not directly or indirectly operate, utilize, control, or maintain any Information Systems,[14] and that is not required to, and does not, directly or indirectly control, access, receive, own, generate, or possess Nonpublic Information will be exempt from the requirements to (1) maintain a cybersecurity program, (2) create a cybersecurity policy, (3) appoint a CISO, (4) conduct Penetration Testing and vulnerability assessments, (5) maintain audit trails, (6) limit user access privileges, (7) maintain procedures to ensure application security, (8) utilize qualified cybersecurity personnel and conduct training for such personnel, (9) utilize Multi-Factor Authentication or Risk-Based Authentication, (10) monitor Authorized Users and provide regular cybersecurity awareness training for all personnel, (11) maintain

[9] 23 NYCRR § 500.01(c). A Person is defined in the Cybersecurity Regulation as "any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association." 23 NYCRR § 500.01(i).

[10] "Affiliate means any Person that controls, is controlled by or is under common control with another Person. For purposes of this subsection, 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." 23 NYCRR § 500.01(a).

[11] "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." 23 NYCRR § 500.01(l).

[12] 23 NYCRR § 500.19(a).

[13] 23 NYCRR § 500.19(b).

[14] "Information System 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." 23 NYCRR § 500.01(e).

controls to protect Nonpublic Information held or transmitted, and (12) develop a written incident response plan.[15]

- An entity created under Article 70 of the New York Insurance Law (addressing captive insurance companies) that is a Covered Entity but that does not and is not required to directly or indirectly control, access, generate, own, receive, or possess Nonpublic Information other than information relating to its corporate parent company (or Affiliates) will be exempt from the requirements to (1) maintain a cybersecurity program, (2) create a cybersecurity policy, (3) appoint a CISO, (4) conduct Penetration Testing and vulnerability assessments, (5) maintain audit trails, (6) limit user access privileges, (7) maintain procedures to ensure application security, (8) utilize qualified cybersecurity personnel and conduct training for such personnel, (9) utilize Multi-Factor Authentication or Risk-Based Authentication, (10) monitor Authorized Users and provide regular cybersecurity awareness training for all personnel, (11) maintain controls to protect Nonpublic Information held or transmitted, and (12) develop a written incident response plan.[16]

Any Covered Entity that qualifies for one of the above exemptions is required to file a Notice of Exemption on the form set forth in Appendix B of the Cybersecurity Regulation. This Notice of Exemption must be filed electronically via the DFS Web Portal[17] within 30 days of the date that it is determined that the Covered Entity is exempt. In the event that a Covered Entity, as of its most recent fiscal year end, no longer qualifies for an exemption, the Covered Entity will then be required to comply with all applicable requirements of the Cybersecurity Regulation within 180 days from the end of that fiscal year.

Full Exemption. The full exemption from all of the provisions of the Cybersecurity Regulation applies to the following types of Covered Entities, so long as they do not otherwise qualify as a Covered Entity in another way:

- Persons subject to New York Insurance Law Section 1110 (certain charitable annuity societies);
- Persons subject to Insurance Law Section 5904 (certain risk retention groups not chartered in New York State); and
- Any accredited reinsurer or certified reinsurer that has been accredited or certified pursuant to Part 125 of Title 11 of the Official Compilation of Codes, Rules and Regulations of the State of New York.[18]

REQUIREMENTS OF THE CYBERSECURITY REGULATION

Cybersecurity Program. A Covered Entity is required to maintain a cybersecurity program. This program must be based on the risks that are identified in the Covered Entity's Risk Assessment and be designed to protect the confidentiality, availability, and integrity of all Information Systems. Every program must also perform the following core cybersecurity functions[19]:

- Identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems;
- Use defensive infrastructure and the implementation of 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;
- Detect Cybersecurity Events[20];
- Respond to identified or detected Cybersecurity Events to mitigate any negative effects;
- Recover from Cybersecurity Events and restore normal operations and services; and
- Fulfill applicable regulatory reporting obligations.

All documentation regarding a Covered Entity's cybersecurity program must be kept and made available to the Superintendent of Financial Services ("Superintendent") upon request.

Covered Entities are permitted to meet the requirement to maintain a cybersecurity program by adopting relevant and applicable provisions of a cybersecurity program that is maintained by any Affiliate of the Covered Entity. If a Covered Entity chooses to adopt such provisions, then the provisions of the Affiliate's cybersecurity program that are adopted must satisfy all of the requirements that are applicable to the Covered Entity itself.

[15] 23 NYCRR § 500.19(c).

[16] 23 NYCRR § 500.19(d).

[17] NYS Dept. of Fin. Serv., "Frequently Asked Questions Regarding 23 NYCRR Part 500," available at http://www.dfs.ny.gov/about/cybersecurity_faqs.htm (last updated Apr. 24, 2017).

[18] 23 NYCRR § 500.19(f).

[19] 23 NYCRR § 500.02(b).

[20] "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." 23 NYCRR § 500.01(d).

Cybersecurity Policy. A Covered Entity is also required to implement and maintain a written policy or set of policies which set forth the Covered Entity's policies and procedures for the protection of all Information Systems and all Nonpublic Information stored on the Information Systems. The cybersecurity policy must be based on the Risk Assessment and approved by the board of directors, an appropriate committee of the board of directors, an equivalent governing body, or a Senior Officer[21] of the Covered Entity. To the extent they are applicable to the Covered Entity's operations, the following areas are required to be addressed in the cybersecurity policy:

- Information security;
- Data governance and classification;
- Asset inventory and device management;
- Access controls and identity management;
- Business continuity and disaster recovery planning and resources;
- Systems operations and availability concerns;
- Systems and network security;
- Systems and network monitoring;
- Systems and application development and quality assurance;
- Physical security and environmental controls;
- Customer data privacy;
- Vendor and Third Party Service Provider management;
- Risk assessment; and
- Incident response.[22]

Chief Information Security Officer. Every Covered Entity must designate an individual to act as the CISO. The CISO must be qualified for such role and is responsible for overseeing and implementing the cybersecurity program, and enforcing the cybersecurity policy. Covered Entities are permitted to meet this requirement by using a CISO who is employed by a Third Party Service Provider or an Affiliate, so long as the Covered Entity retains responsibility for compliance with the Cybersecurity Regulation, requires the Third Party Service Provider to maintain a cybersecurity program that complies with the requirements of the Regulation, and designates a senior member of the Covered Entity's personnel to be responsible for direction and oversight of the Third Party Service Provider.

The CISO is required to develop a written report regarding the Covered Entity's cybersecurity program and material cybersecurity risks. This report must be presented annually to the Covered Entity's board of directors or equivalent governing body, or, if neither exists, to a Senior Officer of the Covered Entity who is responsible for the cybersecurity program. The CISO may report to the board on a more frequent basis, but is required by the Cybersecurity Regulation to report at least on an annual basis. In preparing reports, the CISO must consider the following, to the extent applicable:

A Covered Entity is required to implement and maintain a written policy or set of policies which set forth the Covered Entity's policies and procedures for the protection of all Information Systems and all Nonpublic Information stored on the Information Systems.

- The confidentiality of Nonpublic Information and the integrity and security of the Covered Entity's Information Systems;
- The Covered Entity's cybersecurity policies and procedures;
- Material cybersecurity risks to the Covered Entity;
- Overall effectiveness of the Covered Entity's cybersecurity program; and
- Material Cybersecurity Events involving the Covered Entity during the time period addressed by the report.[23]

Penetration Testing and Vulnerability Assessments. As part of its cybersecurity program, a Covered Entity must perform monitoring and testing of its Information Systems, in accordance with its Risk Assessment. The monitoring and testing must be designed to assess the effectiveness of the Covered Entity's cybersecurity program and must include continuous monitoring *or* periodic Penetration Testing and vulnerability assessments.

The Cybersecurity Regulation does not define or explain what "continuous monitoring" entails, but DFS has issued guidance on this topic:

> Effective continuous monitoring could be attained through a variety of technical and procedural tools, controls and systems [which] generally has the ability to continuously, on an ongoing basis, detect changes

[21] "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." 23 NYCRR § 500.01(m).

[22] 23 NYCRR § 500.03.

[23] 23 NYCRR § 500.04(b).

or activities within a Covered Entity's Information Systems that may create or indicate the existence of cybersecurity vulnerabilities or malicious activity.[24]

In contrast, DFS stated that "periodic manual review of logs and firewall configurations" would not be considered to constitute "effective continuous monitoring."[25]

If a Covered Entity does not conduct continuous monitoring or have other systems in place to detect changes in Information Systems that may create or indicate vulnerabilities on an ongoing basis, the Covered Entity is required to conduct:

- 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
- 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.[26]

Audit Trail. A Covered Entity is required to securely maintain systems designed to reconstruct material financial transactions sufficient to support its normal operations and obligations, to the extent such systems are applicable to the Covered Entity and may be required in accordance with the Risk Assessment. All of these records must be maintained for at least five years.

A Covered Entity is required to securely maintain systems designed to reconstruct material financial transactions sufficient to support its normal operations and obligations.

A Covered Entity must also securely maintain systems that include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of that entity's normal operations. These systems must also be maintained to the extent they are applicable to the Covered Entity and are required in accordance with the Risk Assessment. All records under this requirement must be maintained for at least three years.

[24] "Frequently Asked Questions Regarding 23 NYCRR Part 500," supra note 17.

[25] Id.

[26] 23 NYCRR § 500.05.

Access Privileges. A Covered Entity is also required, as part of its cybersecurity program, to limit user access privileges to Information Systems that provide access to Nonpublic Information.[27] These access privileges must be based on the Covered Entity's Risk Assessment and be periodically reviewed as well.

Application Security. The cybersecurity program of a Covered Entity must also include written procedures which address the security of all applications utilized by the Covered Entity. For in-house developed applications, a Covered Entity must have written procedures, guidelines, and standards designed to ensure the use of secure development practices with regard to such applications. For externally developed applications that are utilized within the context of the Covered Entity's technology environment, the Covered Entity must have written procedures for evaluating, assessing, or testing the security of all such applications.

All of the procedures, guidelines, and standards that are required under this section on application security must be periodically reviewed, assessed and updated as necessary by the CISO or a qualified designee of the Covered Entity.

Risk Assessment. A Covered Entity must conduct periodic Risk Assessments of its Information Systems. Such Risk Assessments must be sufficient for the Covered Entity to rely on in developing its cybersecurity program and cybersecurity policy. The Risk Assessment must take into account all risks that are a threat to the Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized, and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems. It must also be updated as reasonably necessary to reflect changes to the Covered Entity's Information Systems, Nonpublic Information, or business operations, and allow for the revision of controls in order to respond to evolving threats and technological developments.

The Risk Assessment must be executed in accordance with written policies and procedures which include the following:

- Criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity;
- Criteria for the assessment of the confidentiality, integrity, security, and availability of the Covered Entity's Information Systems and Nonpublic

[27] 23 NYCRR § 500.07.

Information, including the adequacy of existing controls in the context of identified risks; and
- Requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.[28]

Practice Pointer: Although the Cybersecurity Regulation does not set forth any more detail on how a Covered Entity is to perform a Risk Assessment, federal banking regulators have developed a tool that might be helpful in this regard. The Federal Financial Institutions Examination Council (FFIEC) issued a Cybersecurity Assessment Tool (the "Assessment Tool") in 2015 to help financial institutions identify their risks and determine their cybersecurity preparedness. The Assessment Tool considers five categories for determining an institution's inherent risk profile:

1. Technologies and connections types;
2. Delivery channels;
3. Online/mobile products and technology services;
4. Organizational characteristics; and
5. External threats.

These categories factor in the type, volume, and complexity of an institution's operations to help determine potential vulnerability to cyber threats.[29]

As noted earlier, the requirement to perform a Risk Assessment is not effective until March 1, 2018. However, this creates an issue for Covered Entities in that several requirements of the Cybersecurity Regulation that go into effect on August 28, 2017, are based on the Risk Assessment. DFS addressed this issue in subsequent guidance, stating that

> while Covered Entities will be required to have a cybersecurity program as well as policies and procedures in place by August 28, 2017, the Department recognizes that in some cases there may be updates and revisions thereafter that incorporate the results of a Risk Assessment later conducted, or other elements of Part 500 that are subject to longer transitional periods.[30]

Cybersecurity Personnel and Intelligence. In addition to the requirement to appoint a CISO, a Covered Entity must also manage cybersecurity risks through the use of its own qualified cybersecurity personnel, or the qualified cybersecurity personnel of an Affiliate or a Third Party Service Provider.[31] These personnel must also perform or oversee the performance of all core cybersecurity functions.

The Covered Entity must provide all cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks and verify that key cybersecurity personnel do what is necessary to stay up to date on the changing cybersecurity threats and countermeasures. An Affiliate or qualified Third Party Service Provider may assist the Covered Entity to ensure compliance with the foregoing requirements.

Third Party Service Provider Security Policy. A major focus of the Cybersecurity Regulation is on the protections a Covered Entity must adopt with respect to Third Party Service Providers. This is consistent with the focus of federal and other regulators on vendor management, and recognition of the fact that even if a Covered Entity employs various protections from cyber-attacks, if it uses a Third Party Service Provider that is vulnerable to a cyber-attack it can result in significant damage to the Covered Entity's business.

Although the Cybersecurity Regulation does not set forth extensive details on how to perform a Risk Assessment, the FFIEC's Cybersecurity Assessment Tool can help financial institutions identify their risks and determine their cybersecurity preparedness.

A Third Party Service Provider is broadly defined by the Regulation as a Person that (1) is not an Affiliate of the Covered Entity; (2) provides services to the Covered Entity; and (3) maintains, processes, or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity. This is due to the fact that Nonpublic Information includes not only nonpublic customer information, but also nonpublic business information. Accordingly, as defined under the Regulation, a Third Party Service Provider includes a vendor that has access to confidential business information, even if that vendor has no access to customer information.

For all Information Systems and Nonpublic Information that is accessible to or held by Third Party Service Providers, a Covered Entity is required under the Cybersecurity Regulation to implement written policies and procedures that will maintain the security

[28] 23 NYCRR § 500.09(b).

[29] Fed. Fin. Institutions Examination Couns., "Cybersecurity Assessment Tool," available at https://www.ffiec.gov/cyberassessmenttool.htm (last modified June 2, 2017 9:41 AM).

[30] "Frequently Asked Questions Regarding 23 NYCRR Part 500," supra note 17.

[31] 23 NYCRR § 500.10.

of such systems and information.[32] These policies and procedures must also be based on the Covered Entity's Risk Assessment and must address, to the extent applicable, the following:

- The identification and risk assessment of Third Party Service Providers;
- Minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity;
- Due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and
- Periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.[33]

The policies and procedures must also include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers including, to the extent applicable, guidelines addressing:

For any individual accessing the Covered Entity's internal networks from an external network, a Covered Entity is required to use Multi-Factor Authentication, unless the CISO has approved, in writing, the use of reasonably equivalent or more secure access controls.

- The Third Party Service Provider's policies and procedures for access controls, including its use of Multi-Factor Authentication, as required under the Cybersecurity Regulation, to limit access to relevant Information Systems and Nonpublic Information;
- The Third Party Service Provider's policies and procedures for use of encryption as required under the Regulation to protect Nonpublic Information in transit and at rest;
- Notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or the Covered Entity's Nonpublic Information being held by the Third Party Service Provider; and
- Representations and warranties addressing the Third Party Service Provider's cybersecurity policies and procedures that relate to the security of the Covered Entity's Information Systems or Nonpublic Information.[34]

An agent, representative, employee, or designee of a Covered Entity that itself is a Covered Entity is not required to create its own third-party information security policy *as long as* such agent, representative, employee, or designee follows the required policy of the Covered Entity.

Multi-Factor Authentication. The Cybersecurity Regulation also requires each Covered Entity to use "effective controls" to protect against unauthorized access to Nonpublic Information or Information Systems.[35] Controls that are considered effective and may be used include Multi-Factor Authentication or Risk-Based Authentication. For any individual accessing the Covered Entity's internal networks from an external network, a Covered Entity is required to use Multi-Factor Authentication, unless the CISO has approved, in writing, the use of reasonably equivalent or more secure access controls.

Limitations on Data Retention. Policies and procedures must also be included in a Covered Entity's cybersecurity program regarding the secure disposal of any Nonpublic Information that is personally identifiable of a particular individual or related to the health of the individual.[36] The secure disposal must be conducted on a periodic basis in order to dispose of this type of Nonpublic Information that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity. However, a Covered Entity may not dispose of any Nonpublic Information that it is required to retain by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Training and Monitoring. A Covered Entity is required, as part of its cybersecurity program, to regularly provide cybersecurity awareness training for *all* its personnel. This includes everyone from the chief executive officer to mailroom personnel. The training must be updated to reflect risks that the Covered Entity identifies in its Risk Assessment.[37]

Additionally, each Covered Entity must implement risk-based policies, procedures, and controls

[32] 23 NYCRR § 500.11.

[33] 23 NYCRR § 500.11(a).

[34] 23 NYCRR § 500.11(b).

[35] 23 NYCRR § 500.12.

[36] 23 NYCRR § 500.13.

[37] 23 NYCRR § 500.14(b).

to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users.[38]

Encryption of Nonpublic Information. Based on its Risk Assessment, and as part of its cybersecurity program, a Covered Entity must also create and maintain controls to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.[39] Such controls are required to include encryption; however, if a Covered Entity determines that encryption is infeasible, it may utilize effective alternative compensating controls that are reviewed and approved by the CISO to secure Nonpublic Information. These alternative compensating controls must be reviewed by the CISO on an annual basis to determine effectiveness and whether circumstances have changed such that encryption would now be feasible.

Incident Response Plan. A Covered Entity is also required to establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event that materially affects the availability, confidentiality, or integrity of the Covered Entity's Information Systems or the continuing functionality of any aspect of its business or operations. The incident response plan must be designed to specifically address the following:

- The internal processes for responding to a Cybersecurity Event;
- The goals of the incident response plan;
- The definition of clear roles, responsibilities, and levels of decision-making authority;
- External and internal communications and information sharing;
- Identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;
- Documentation and reporting regarding Cybersecurity Events and related incident response activities; and
- The evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.[40]

Notices to Superintendent. The Cybersecurity Regulation requires a Covered Entity to provide two types of notices to the Superintendent[41]:

- First, if a Cybersecurity Event occurs that (1) has a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity, or (2) impacts the Covered Entity in such a way that notice is required to be provided to any government body, self-regulatory agency, or any other supervisory body, then a Covered Entity is required to notify the Superintendent of such Cybersecurity Event as promptly as possible, but in no event later than 72 hours from a determination that such Cybersecurity Event has occurred.
- Second, each Covered Entity must submit an annual written statement to the Superintendent certifying compliance with the Cybersecurity Regulation. The annual written statement must be submitted by February 15th of each year and must cover the prior calendar year. The Covered Entity is required to use the form that has been provided in Appendix A of the Cybersecurity Regulation in meeting this requirement. All records, data, and schedules which support the annual certification must be maintained by the Covered Entity for five years for examination by DFS.

If a Covered Entity identifies areas, processes, or systems that require material improvement, updating, or redesign, it is further required to document the identification of such required improvements, as well as the remedial efforts that it has planned and underway to address the required improvements. All documentation concerning the foregoing must be made available for inspection by the Superintendent as well.

DFS has stated that all notices required under Section 500.17 of the Cybersecurity Regulation will eventually be reported through the secure DFS Web Portal. Until this secure reporting tool is set up to accommodate these notices, all notices should be sent to the Covered Entity's normal supervisory staff within DFS.[42]

Confidentiality. Information provided by a Covered Entity pursuant to the Cybersecurity Regulation is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law,

[38] 23 NYCRR § 500.14(a).

[39] 23 NYCRR § 500.15.

[40] 23 NYCRR § 500.16.

[41] 23 NYCRR § 500.17.

[42] "Frequently Asked Questions Regarding 23 NYCRR Part 500," supra note 17.

Public Officers Law, or any other applicable state or federal law.

PAVING THE WAY FOR THE FUTURE

As stated earlier, the Cybersecurity Regulation is the first of its kind in the nation on the state level. The Regulation is unique even when measured against federal cybersecurity requirements, which are spread out over a patchwork of regulations, policy statements, and examination manuals. By contrast, the New York State Cybersecurity Regulation is a comprehensive, self-contained set of requirements.

Federal cybersecurity requirements are spread out over a patchwork of regulations, policy statements, and examination manuals. By contrast, the New York State Cybersecurity Regulation is a comprehensive, self-contained set of requirements.

New York State has a history of being proactive on financial regulation, and other states and federal regulators alike often follow New York's lead. There is a sense that New York's Cybersecurity Regulation may continue that trend. New York DFS Superintendent Maria Vullo, is quoted as stating in an April 9, 2017, speech to the National Association of Insurance Commissioners (NAIC) that DFS believes "the best way for industry to focus on the threat of cyber security is to have a consistent framework," and that the New York Cybersecurity Regulation "is a road map with rules of the road."[43] The NAIC has been working on a model cybersecurity law that each state would be free to adopt in order to provide uniformity in this area.

Also, banking regulators for other states have shown interest in formalizing their own cybersecurity guidance. Connecticut, California, Massachusetts, Illinois, and Maryland have been identified as states that may take the Cybersecurity Regulation into consideration in creating their own cybersecurity regulation.[44]

CONCLUSION

New York's Cybersecurity Regulation imposes stringent requirements on certain entities that are regulated by DFS, through the prism of a "risk-based" approach. Each Covered Entity under the Regulation has the flexibility to design a cybersecurity policy and cybersecurity program that is based on the risks identified in that particular entity's Risk Assessment. The impact of the Regulation reaches beyond just the cybersecurity practices of financial services companies to the Third Party Service Providers that they interact with. The far-reaching scope of this stringent Regulation has sent a message to the rest of the nation that New York State intends to be a leader in the protection of Information Systems from cyber-attacks. ■

[43] Suzanne Barlyn, "New York Sees its Cyber Rules for Insurers as Model for Other States" (Ins. J., Apr. 10, 2017), available at http://www.insurancejournal.com/news/national/2017/04/10/447358.htm.

[44] Allison Grande, "NY Cybersecurity Rules Will Spur Action But Not Uniformity" (Law360, Mar. 9, 2017 10:26 PM), available at https://www.law360.com/articles/899971/ny-cybersecurity-rules-will-spur-action-but-not-uniformity.