NSCP
THE NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

APRIL 2017 SPECIAL REPRINT
Currents

The New NYS Financial Services Cybersecurity Regulation

An Analysis of the NYS Department of Financial Services Cybersecurity Regulation

By John R. Hewitt and Leigh Wellington

The New York State Department of Financial Services (DFS) proposed on September 13, 2016 a cybersecurity regulation that was to be effective on January 1, 2017 (Regulation).[1] After considerable adverse commentary about the Regulation during the comment period, the DFS revised the regulation and reset its effective date to March 1, 2017.[2] DFS stated that it "carefully considered all comments submitted regarding the proposed regulation during the 45-day comment period . . . and has incorporated those suggestions that DFS deemed appropriate in an updated draft that will be subject to an additional final 30-day comment period."[3]

The DFS regulates mortgage banks, life insurance companies, savings and loans, charitable foundations and other financial services firms (Firms) and, with certain limited exemptions, all such entities will be subject to the Regulation. In its proposal, the DFS notes that it has been closely monitoring the increasingly serious cybersecurity problems experienced in the financial services industry and is proposing the Regulation to address this situation. It applauds the many firms that have developed and implemented cybersecurity programs (Programs) and directs those who have not to begin the development of one.

The Regulation is designed to provide a basic foundation upon which Firms can develop a Program and requires them initially to assess their risk profile and then to design a robust program to address any identified risks. The Regulation provides flexibility for each Firm to develop a Program that is designed to assess and control a Firm's specific risks as well as any new technological developments. The DFS emphasizes that senior management must take an active role in a Firm's Program and take direct responsibility for it.[4]

The Regulation is extensive, as it has twenty-three sections addressing such subjects as cybersecurity programs and policies, the necessity of appointing a Chief Information Security Officer, penetration testing, audits, risk assessment, third party service providers, multi-factor authentication, training, encryption, incident response plans, notice and exemptions. These topics are similar to those contained in the regulations and guidelines issued by the SEC, FINRA and certain states such as Massachusetts.[5]

Significant changes were made between the initial proposal and the revised Regulation, including the addition of the defined terms "risk assessment" and "third party service provider," an allowance for the Chief Information Security Officer to have additional Firm responsibilities, modified policies and procedures regarding the handling of nonpublic information by third parties, modification to the requirements for notice of a cybersecurity event and revised exemptions to the Regulation. The initial proposal also had an all-inclusive transitional period of 180 days from the effective date, while the revised version retains the 180 period but now includes additional transition periods of one, one and a half and two years for particular requirements such as risk assessments (1 year), multi-factor authentication (1 year), audit trials (1-1/2 years) and encryption (1-1/2 years).

The following provides an overview of the Regulation, as revised.

Definitions[6]

The Definitions section contains thirteen key terms that are specifically applicable to the Regulation. This includes the definitions of Cybersecurity Event, which is any act or attempt to gain unauthorized access to a Firm's Information System, and Multi-Factor Authentication, that is an authentication through at least two of the following three factors: knowledge (something the user knows such as a password), possession (something s/he possesses such as a token) or inherence (a biometric). The Regulation uses a rather broad definition of Nonpublic Information (Nonpublic Information) as it includes any business-related information the tampering with which would cause a materially adverse impact on a Firm's business; and information concerning an individual that can be used to identify such individual in combination with elements such as social security

About the Authors

John Hewitt is a Partner at Pastore & Dailey LLC, www.psdlaw.net. He can be reached at jhewitt@psdlaw.net.

Leigh Wellington is a Law Clerk at Pastore & Dailey LLC, www.psdlaw.net. She can be reached at lwellington@psdlaw.net.

numbers, driver's license numbers or financial account numbers or codes.[7] A Covered Entity (CE) is one that operates under or is required to operate under a DFS license, charter, registration or similar state authorization and an Information System (System) is a discrete set of electronic resources organized to provide a certain technological service.

Cybersecurity Program[8]

The Regulation requires each CE to maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of its Information Systems. The Program should be based on the CE's Risk Assessment. It must identify and assess internal and external cybersecurity risks that could threaten the security or integrity of Nonpublic Information stored on the CE's Information Systems. This must protect the information in these Systems from unauthorized access, use or other malicious acts and be designed to detect Cybersecurity Events. Finally, it must establish an incident response plan (IRP) to ensure that the Firm mitigates the effects of a Cybersecurity Event. A CE may use an Affiliate's cybersecurity program to meet these requirements.

Cybersecurity Policy[9]

A CE's written cybersecurity policy (Cybersecurity Policy) shall be implemented and set forth its policies and procedures to protect its Systems and any Nonpublic Information stored on these Systems. The policy must be based on the CE's Risk Assessment and address the following areas to the extent applicable to the CE's operations: 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. These written policies must be approved by a Senior Officer or the CE's board of directors or equivalent governing body.

Chief Information Security Officer[10]

Each CE shall designate a Chief Information Security Officer ("CISO") or the equivalent to be responsible for implementing, overseeing and enforcing the CE's cybersecurity program and policy. The CISO responsibility may be handled by a Third Party Service Provider, but the CE shall still be responsible for the CISO's responsibilities and shall designate a senior Firm member to ensure that the Third Party Service Provider complies with the CISO requirements. The CISO shall develop and file a report at least annually with the CE's board of directors or equivalent governing body, but, if no such governing body exists, then to the Senior Officer of the CE responsible for its cybersecurity program. The CISO report shall address the integrity and security of the CE's systems, the policies and procedures, material risks, effectiveness of the Firm's systems, and material cybersecurity events in the reported period.

Penetration Testing, Vulnerability Assessments, Audit Trails and Access Privileges[11]

Each Program shall include monitoring and testing of the Program, which shall include annual penetration testing of a Firm's Systems and bi-annual vulnerability assessments of them. The Firm is required to securely maintain systems designed to reconstruct material financial transactions to support normal business, include audit trails to detect and respond to Cybersecurity Events which could materially harm the business operations and maintain records required by this Section for not fewer than five years. Each Firm shall employ the principal of least privilege by limiting System access privileges solely to those who require such access and periodically reviewing such access privileges.

Application Security[12]

In developing its own applications or in using externally developed applications, a Firm must have written procedures, guidelines and standards designed to ensure the use of secure development practices and for evaluating, assessing and testing the security of them. All procedures, guidelines and standards shall be reviewed, assessed and updated as deemed necessary by the CISO.

Risk Assessment[13]

Each Firm shall conduct a periodic documented risk assessment of its Systems which shall be updated as reasonably necessary to address changes to the CE's Information Systems, Nonpublic Information or business operations. The assessment shall include criteria for the evaluation and categorization of identified risks and for the assessment of the confidentiality, integrity and availability of its Systems. This shall include documentation describing risks mitigation or acceptance.

Cybersecurity Personnel and Intelligence[14]

Each CE shall employ sufficient personnel to effectively execute its cybersecurity responsibilities and this personnel shall be properly trained and maintain current knowledge of changing cybersecurity threats and countermeasures. An Affiliate or qualified Third Party Service Provider may assist in complying with these requirements, subject to Section 500.11, Third Party Information Security Policy.

Third Party Information Security Policy[15]

Each CE must develop policies and procedures designed to address the cybersecurity responsibilities of all third parties including the security of Systems that are accessible to, or held by, Third Party Service Providers. Such policies and procedures shall address the identification and risk assessment of these Third Party Service Providers and establish minimum cybersecurity practices required to be met by them to do business with the CE. This must include due diligence procedures to evaluate their cybersecurity practices and a periodic assessment of such entities and the adequacy of their practices.

These policies and procedures shall include requirements for Third Party contract provisions and/or due diligence including

the Third Party Service Provider's policies and procedures for access controls and use of encryption, notice to the CE in the event of a Cybersecurity Event impacting the CE's Information systems or Nonpublic Information held by the Third Party Service Provider.

Multi-Factor Authentication[16]

Each CE shall use effective controls in order to protect against unauthorized access to Nonpublic Information or Information Systems. Any individual accessing the CE's internal networks from an external network shall use Multi-Factor Authentication unless the CE's CISO approves at least reasonably equivalent access controls.

Limitations on Data Retention[17]

Each CE shall have policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information that is no longer necessary for its business, except where such information is otherwise required to be retained by law or regulation or disposal is not reasonably feasible.

Training and Monitoring[18]

Each CE's Program shall implement risk-based policies and procedures designed to monitor authorized users, detect unauthorized access, use or tampering with Nonpublic Information and provide regular updated cybersecurity awareness training sessions.

Encryption of Nonpublic Information[19]

The Regulation requires the encryption of all Nonpublic Information both in transit and at rest. If this proves infeasible, CEs may employ alternative compensating controls that are approved by the CISO and reviewed at least annually.

Incident Response Plan[20]

Each CE shall establish a written IRP that shall effectively respond to and allow the Firm to recover from any Cybersecurity Event materially affecting the confidentiality, integrity or availability of its Systems or the continuity of its business. The IRP shall address, at a minimum, the CE's response to the incident and the IRP's goals. It must also clearly define roles, responsibilities and levels of decision-making authority, closely coordinate internal and external communications, identify requirements for remediation of any identified weakness in Information Systems and associated controls, document and report Cybersecurity Events and evaluate and improve the IRP after an event. It must also ensure that all required reports are filed with the appropriate regulatory authorities.

Notices to Superintendent[21]

CEs are required to provide a notice to the DFS Superintendent of a Cybersecurity Event where notice is required to be provided to any government body, self-regulatory agency or any other supervisory body or where there is a reasonable likelihood of material harm to the normal operations of the CE. Notice is to be given as soon as possible, but no later than 72 hours after the event.

A CE must also file a written statement on a DFS form by February 15 annually certifying that it is complying with the Regulation's requirements and these statements shall be maintained as well as all documents supporting it for five years. If the CE notes anything for improvement or redesign, it must document this and retain it for the DFS Superintendent's inspection.

Exemptions[22]

The Regulation contains an exemption from certain Sections of this Regulation for a CE with fewer than 10 employees or independent contractors, less than $5,000,000 in gross annual revenue in each of the last three fiscal years, or less than $10,000,000 in year-end total assets.

Employees, agents, representatives or designees of a CE, who is itself a CE, are exempt from developing its own Program to the extent that s/he is covered by the CE's Program.

Further, a CE that does not operate, maintain, utilize or control any Information Systems and that does not, and is not required to, control, own, access, generate, receive or possess Nonpublic Information is exempt from certain Sections of this Regulation.

If a CE ceases to qualify for an exemption, such CE will have 180 days from the effective date to comply with the Regulation's requirements. ★

For more information or to discuss the contents of this article, please contact **John R. Hewitt**.

Endnotes

1. The New York State Department of Financial Services (DFS) proposed on September 13, 2016 a cybersecurity regulation that was to be effective on January 1, 2017 (Regulation).
2. Ibid.
3. Press Release, New York State Department of Financial Services, DFS Issues Updated Proposed Cybersecurity Regulation Protecting Consumers and Financial Institutions (Dec. 28, 2016).
4. Ibid. at Section 500.0
5. 201 Mass. Code of Regs. 17.01; OCIE 2015 Cybersecurity Examination Initiative (September 2015) and FINRA 2015 Report on Cybersecurity Practices (February 2015).
6. Regulation at Section 500.0 (Hereinafter Section 500.___).
7. The latter definition is similar to that used in the NYS Information Security Breach and Notification Act; **https://its.ny.gov/eiso/breach-notification**.
8. Ibid. at Section 500.02.
9. Section 500.03
10. Section 500.04
11. Section 500.05, Section 500.06 and Section 500.07
12. Section 500.08
13. Section 500.09
14. Section 500.10
15. Section 500.11
16. Section 500.12
17. Section 500.13
18. Section 500.14
19. Section 500.15
20. Section 500.16
21. Section 500.17
22. Section 500.19