Cullen | Dykman

New York State Department of Financial Services Issues Updated Proposed Cybersecurity Regulation

January 3, 2017

The New York State Department of Financial Services ("DFS") has updated its proposed regulation requiring banks, insurance companies, and other financial services institutions regulated by DFS to establish and maintain a cybersecurity program designed to protect consumers and ensure the safety and soundness of New York State's financial services industry ("Updated Proposed Regulation"). According to DFS, it considered all comments submitted regarding the original proposed regulation issued in September ("Original Proposed Regulation") and incorporated those suggestions that DFS deemed appropriate in the Updated Proposed Regulation. Public comments on the Updated Proposed Regulation will be received until January 27, 2017, and the regulation becomes effective March 1, 2017.

This advisory highlights some of the differences between the Original Proposed Regulation and the Updated Proposed Regulation. Our advisory discussing the Original Proposed Regulation may be found here, and the text of the Updated Proposed Regulation may be found here: http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf

Definitions (Section 500.01)

The Original Proposed Regulation defined "Nonpublic Information" broadly to include "[a]ny information that an individual provides to a Covered Entity in connection with seeking or obtaining any financial product or service from the Covered Entity" and "[a]ny information that can be used to distinguish or trace an individual's identity, including but not limited to . . . any information that is linked or linkable to an individual." DFS amended this definition to align more with the definition of "private information" in New York's existing data security law found in New York General Business Law Section 899-aa. Under the Updated Proposed Regulation, "Nonpublic Information" is now defined to include "[a]ny 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."

DFS has added "Risk Assessment" as a defined term to mean "the risk assessment that each Covered Entity is required to conduct under Section 500.09." On a related note, DFS has revised Section 500.09 and other sections to clarify and/or make more explicit DFS's original intent to have risk-based requirements of a Covered Entity's cybersecurity program tied to the Covered Entity's Risk Assessment. Section 500.09 now requires each Covered Entity to conduct a periodic (changed from "annual") Risk Assessment encompassing, among other things, evaluation, categorization, and mitigation of risks, and to document the Risk Assessment in writing.

DFS has also added "Third Party Service Provider(s)" as a defined term to mean "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."

Chief Information Security Officer (Section 500.04)

DFS has revised Section 500.04, which requires that each Covered Entity designate a qualified individual to serve as Chief Information Security Officer ("CISO") and that the CISO develop a report which must be reviewed internally and which shall address specified cybersecurity issues. The DFS has clarified in the Updated Proposed Regulation that it is not requiring a specific title for the chosen qualified individual. Further, the individual need not be exclusively dedicated to CISO activity. Additionally, the timing requirement of the CISO report was changed from "at least bi-annually" to "at least annually."

Audit Trail (Section 500.06)

DFS has revised Section 500.06, which requires that the cybersecurity program for each Covered Entity include implementing and maintaining audit trail systems that meet specified requirements, to be explicitly based on each Covered Entity's Risk Assessment. Under this Section, each Covered Entity must securely maintain systems that: (i) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; 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 normal operations of the Covered Entity. Additionally, the record retention period was changed from six years to five years.

Third Party Information Security Policy (Section 500.11)

DFS has made several changes to Section 500.11, which requires each Covered Entity to develop policies and procedures designed to ensure the security of its Information Systems and Nonpublic Information that is accessible to, or held by, third parties doing business with the Covered Entity (i.e., Third Party Service Providers). These changes include:

- Removal of the requirement to conduct annual assessments of Third Party Service Providers. Covered Entities must still conduct "periodic assessment(s)" of such third parties "based on the risk they present and the continued adequacy of their cybersecurity practices."
- Modifications of "relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers" that must be included in Covered Entity's policies and procedures. DFS amended this section so that the requirements are more explicitly based on the Covered Entity's Risk Assessment,

and eliminated a provision that may have unintentionally suggested that Covered Entities are required to audit the systems of all Third Party Service Providers.

- Addition of "Limited Exception." Under the Updated Proposed Regulation, "[a]n agent, employee, representative or designee of a Covered Entity who is itself a Covered Entity need not develop its own Third Party Information Security Policy pursuant to this section if the agent, employee, representative or designee follows the policy of the Covered Entity that is required to comply with [the regulation]."

Encryption of Nonpublic Information (Section 500.15)

DFS has revised Section 500.15, which requires each Covered Entity to encrypt all Nonpublic Information held or transmitted by the Covered Entity both in transit and at rest and allows for the use of compensating controls if encryption of such information is infeasible. Under the Original Proposed Regulation, this Section allowed for the use of compensating controls for one year for Nonpublic Information in transit, if encryption of such is infeasible and allowed for the use of compensating controls for five years for Nonpublic Information at rest if encryption of such is infeasible. The Updated Proposed Regulation removed the one-year and five-year periods and also added another provision requiring each Covered Entity's CISO to review the feasibility of encryption and effectiveness of the compensating controls, to the extent applicable, at least annually.

Notices to Superintendent (Section 500.17)

Section 500.17 of the Original Proposed Regulation required each Covered Entity: (i) to submit to the Superintendent, on an annual basis, a written statement by January 15, certifying that the Covered Entity is in compliance with the requirements set forth in the proposed rule ("Certification of Compliance"); (ii) to maintain for examination by DFS all records, schedules and data supporting the certificate for a period of five years; to 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; (iii) to document the identification of areas that require material improvement, updating or redesign, as well as planned remedial efforts; and (iv) to the extent that a Covered Entity has identified any material risk of imminent harm to its Information System from a Cybersecurity Event, to notify the Superintendent within 72 hours and include such event in its annual report. The changes made to this Section in the Updated Proposed Regulation include:

- Modification of Certification of the Compliance deadline. Each Covered Entity must submit to the Superintendent a written statement by February 15 (changed from January 15) on an annual basis, in such form as set forth in Appendix A of the regulation. This requirement commences on February 15, 2018.
- Modification of 72-hour reporting timeframe. DFS has revised this Section to state that notice is required within 72 hours of a determination that a Cybersecurity Event as follows has occurred: (1) Cybersecurity Events of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body, and (2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

Confidentiality (Section 500.18)

With respect to the confidentiality of notices disclosed to DFS under Section 500.17, DFS has added Section 500.18, which states: "Information provided by a Covered Entity pursuant to this Part is subject to exemptions

from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law."

Exemptions (Section 500.19)

DFS has amended the limited exemption in Section 500.19(a) by adding Covered Entities with fewer than 10 employees including independent contractors, deleting Covered Entities with fewer than 1000 customers in each of the last three calendar years, and changing "and" to "or" in two locations. The new limited exemption provides:

a. **Limited Exemption. Each Covered Entity with:**

1. *fewer than 10 employees including any independent contractors*, *or*
2. less than $5,000,000 in gross annual revenue in each of the last three fiscal years, *or*
3. less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates,

shall be exempt from the requirements of Sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(*Emphasis added.*)

Although DFS declined to alter the definition of Covered Entities, it included in the Updated Proposed Regulation several exemptions based on the risk that particular entities or circumstances present. Specifically, DFS has included: (i) a limited exemption for a Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not control, generate, receive or possess Nonpublic Information; and (ii) an exemption for an employee, agent, representative, designee or Affiliate of a Covered Entity, who is itself a Covered Entity, to the extent that the employee, agent, representative, designee or Affiliate is covered by the cybersecurity program of the Covered Entity.

DFS has also added a notice of exemption filing requirement for entities claiming an exemption, in such form as set forth in Appendix B of the regulation.

Effective Date (Section 500.21)

DFS has extended the regulation's effective date from January 1, 2017, to March 1, 2017. Covered Entities will be required to annually prepare and submit to the superintendent a Certification of Compliance commencing February 15, 2018.

Transitional Periods (Section 500.22)

Covered Entities will generally have 180 days from the effective date to comply with these rules. In response to concern about implementation timeframes, DFS has included a number of additional transitional periods to

Section 500.22:

Covered Entities shall have:

1. One year from the effective date of this Part to comply with the requirements of sections 500.04(b) [annual CISO report], 500.05 [Penetration Testing and Vulnerability Assessments], 500.09 [Risk Assessment], 500.12 [Multi-Factor Authentication], and 500.14(a)(2) [cybersecurity awareness training].
2. Eighteen months from the effective date of this Part to comply with the requirements of sections 500.06 [Audit Trail], 500.08 [Application Security], 500.13 [Limitations on Data Retention], 500.14 (a)(1) [implementation of risk-based policies, procedures and controls designed to monitor access to Nonpublic Information] and 500.15 [Encryption of Nonpublic Information].
3. Two years from the effective date of this Part to comply with the requirements of section 500.11 [Third Party Service Provider Security Policy].

Additional Information

If you have any questions regarding the Updated Proposed Regulation or cybersecurity procedures in general, please feel free to contact Joseph D. Simon at 516-357-3710 or via email at jsimon@cullenanddykman.com, Kevin Patterson at 516-296-9196 or via email at kpatterson@cullenanddykman.com, or Adam Barazani at 516-357-3767 or via email at abarazani@cullenanddykman.com.

1. "Covered Entity" means "any Person 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." "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. "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."
4. "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."

Practices

- Banking and Financial Services
- Regulatory and Compliance

Industries

- Financial Institutions

Attorneys

- Kevin Patterson
- Joseph D. Simon