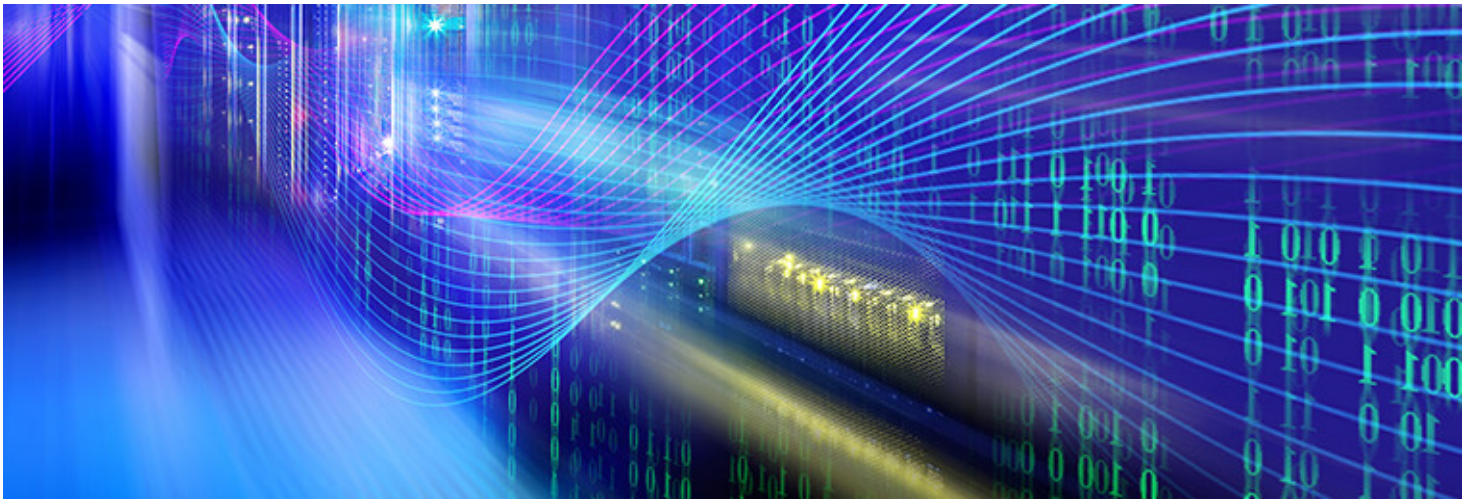

NYDFS announces final cybersecurity rules for financial services sector: key takeaways

Cybersecurity Law Alert

22 FEB 2017
By:

On February 16, 2017, Governor Andrew Cuomo announced final cybersecurity rules for New York's financial services sector. The Cybersecurity Requirements For Financial Services Companies (the Final Rule), promulgated by the New York Department of Financial Services (NYDFS), is the most specific cybersecurity regulation in the country to apply to companies that are not critical infrastructure operators.

The Final Rule takes effect very soon – on **March 1** – but includes transition periods of between one to two years for most of its requirements and is largely unchanged from a revised draft that NYDFS circulated on December 28, 2016.

The Final Rule broadly applies to all New York-licensed financial services companies, including banks, insurance companies and other financial services institutions regulated by the NYDFS, with very limited exceptions. Any entity that operates (or is required to operate) under a license, registration, charter, certificate, permit, accreditation or similar authorization under the banking, insurance and financial services laws of New York is covered to some extent.

The Final Rule includes high-level features of the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Handbook. However, it applies to many entities that have never been subject to FFIEC oversight, and it applies a broader range of customer information and includes more specific requirements, in addition to a 72-hour

cybersecurity incident notification deadline for material breaches and for any breach that requires notice to another regulator.

Together, these features present some operational challenges even for entities subject to FFIEC requirements. Although New York is the center of the financial services sector, the Final Rule raises the potentially very difficult prospect that other states may impose further or conflicting requirements. The two substantive changes in the Final Rule are reducing to three years (from five) a log retention requirement for non-financial transaction logs and expanding somewhat the exemptions from the Final Rule, including for a limited range of insurance and reinsurance companies (see the last section).

The reach of the Final Rule is very broad – which had been one major criticism of the rule when it was first issued for public comment. A particular challenge is its definition of "Nonpublic Information," which encompasses sensitive business information, a somewhat broader version of personal information than is covered by New York's breach notice law, as well as a broad range of health and health payment information that is not subject to HIPAA.[1] The definition covers a broader range of information than is covered separately by FFIEC guidance, by state breach notice laws and by health privacy laws. The Final Rule applies to sector businesses that are usually not subject to all three sets of existing regulatory requirements and requires securing more of the three types of data. Although there is no requirement in the Final Rule to map data assets, Covered Entities will likely need to consider if and where they hold these data *and* either reorient their cybersecurity programs to address new and somewhat expanded areas of risk *or* explain in their risk assessments why these new data elements do not pose significant risk to their enterprise.

The Final Rule requires covered entities to:

- **Conduct periodic risk assessments** updated as necessary in light of changes to the Covered Entity's systems, Nonpublic Information and business operations. The assessments must enable revision of controls in response to changes in technology and threats as they bear on risks to the enterprise and availability and effectiveness of controls that it uses. The risk assessment must be documented in writing and follow written policies and procedures that include (i) criteria for the evaluation and categorization of identified cybersecurity risks facing the Covered Entity; (ii) criteria for the assessment of the confidentiality, integrity, security and availability of the Covered Entity's information systems and Nonpublic Information and adequacy of current controls; and (iii) requirements describing how identified risks will be mitigated or accepted.

- **Maintain a cybersecurity program** based on the risk assessment, designed to:
  - Identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the entity's information systems
  - Use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's systems from unauthorized access, use, or other malicious acts
  - Detect, respond to and recover from cybersecurity events to mitigate any negative effects and restore normal operations and services
  - Fulfill regulatory reporting obligations and
  - Maintain documentation and information relevant to the program to be available to NYDFS upon request.

- **Adopt written cybersecurity policies** approved by a senior officer or the board, setting forth the Covered Entity's policies and procedures for the protection of its information systems and Nonpublic Information stored on those systems covering 14 specific topics.

- **Governance and staffing; compliance certifications and documentation:**
  - **Designate a Chief Information Security Officer** (CISO) responsible for implementing, overseeing, and enforcing its new cybersecurity program and policy. The CISO must report in writing at least annually to the Covered Entity's board of directors (or equivalent governing body, if either exists) about the confidentiality, integrity and security of the Covered Entity's Nonpublic Information and systems, its cybersecurity policies and procedures, the overall effectiveness of its cybersecurity program and material cybersecurity risks, and material cybersecurity events during the time period addressed by the report. The CISO function may be outsourced.
  - Covered Entities must use **qualified cybersecurity personnel** to perform or oversee the core cybersecurity program functions described above, provide those personnel with **updates and training**, and **verify** that "key personnel" (undefined) take steps to **maintain current knowledge of changing threats and countermeasures**

(participating in an ISAC or ISAO would suffice for this final requirements, but is not required).
    - Before February 15 of each year, the chair of the board or a senior corporate officer must file a certification with NYDFS (using a form attached to the Final Rule) certifying that to the best of that person's knowledge, the Covered Entity's cybersecurity program was in compliance with Final Rule as of a specific date. Documentation supporting the annual certification must be retained at least five years, as must any documentation of planned or ongoing remediation efforts. All this information must be available upon request to NYDFS.

- **Monitor, or conduct penetration testing and vulnerability assessments** of the effectiveness of the Covered Entity's cybersecurity program. Covered Entities must either (1) conduct effective continuous system monitoring or use some other systems to detect on an ongoing basis changes in Information Systems that may create or indicate vulnerabilities or else conduct *both* (2) annual penetration testing of the Covered Entity's systems focused on the relevant risks identified in the Risk Assessment *and* (3) bi-annual vulnerability assessments including systematic scans or reviews of information systems. No matter what, monitoring must include risk-based policies, procedures and controls designed to monitor activity of Authorized Users and to detect their unauthorized access to, use of, or tampering with Nonpublic Information.

- **Maintain transaction and server logs** designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity and to detect and respond to cybersecurity events that have a reasonable likelihood of harming any material part of the Covered Entity's normal operations. The transaction records must be kept for at least five years; other logs must be kept for at least three years.

- **Limit user access privileges** to systems that provide access to Nonpublic Information and periodically review those privileges.

- **Maintain application security** written procedures, guidelines and standards designed to ensure the secure development practices for applications developed in-house and of procedures for evaluating, assessing or testing the security of externally developed applications in the Covered Entity's technology environments must be reviewed and assessed periodically and updated as necessary by the CISO or a qualified designee.

- **Vendor risk management program, policies and procedures:** Implement written policies and procedures designed to ensure the security of information systems and Nonpublic Information that are accessible to third party service providers (vendors). The policies and procedures should be based upon the risk assessment and cover, to the extent applicable, risk assessments, minimum security practices for vendors, vendor due diligence, and periodic risk-prioritized vendor assessments. If applicable, these policies must include guidelines for vendor due diligence and/or contractual protections, including to the extent applicable for: the vendor's policies and procedures for meeting the multi-factor authentication, encryption requirements of the Final Rules, notice from the vendor of cybersecurity events that directly affect the Covered Entity's systems or Nonpublic Information the vendor holds, and reps and warranties regarding vendor security commitments. Representatives or designees of Covered Entities may comply by following the Vendor management policies of the Covered Entity and do not need to develop their own program.

- **Use multi-factor authentication** or risk-based authentication to protect against unauthorized access to information systems and Nonpublic Information. Multi-factor authentication is required for all remote access to a Covered Entity's network unless the CISO has given written approval for use of reasonably equivalent or more secure access controls.

- **Secure destruction of data:** Adopt policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information that is no longer necessary for business operations or for other legitimate business purposes unless this Information is required to be retained by law or regulation or is maintained in a way that it is not reasonably feasible to dispose of the Nonpublic Information without also disposing of other information.

- **Implement controls, including encryption or compensating controls** to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. If the Covered Entity does not choose encryption, the CISO must review annually the feasibility of encryption and effectiveness of the compensating controls.

- **Establish a written incident response plan** for responding to any cybersecurity event that materially affects the Covered Entity's confidentiality, integrity or availability of the Covered Entity's information systems or the continuing functionality of any aspect of its business or operations. The plan must define internal processes, the goal of the plan, and clear roles, responsibilities and levels of decision-making authority when incidents occur.

- **Provide regular cybersecurity awareness training** for all personnel that is updated to reflect risks identified in the risk assessment.

- **72-hour breach notification to NYDFS.** Notify the Superintendent not later than 72 hours after a determination that a cybersecurity event has occurred that has a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity, or that simply requires notice to any other government body, self-regulatory agency, or any supervisory body.

Exemptions in the Final Rule

The "small covered entity," "designees covered by another Covered Entity" and "entities that do not possess or handle Nonpublic Information" exemptions discussed below will provide some relief from the requirements for some persons or entities authorized under New York banking, insurance and financial services laws, but the exemptions from the Final Rule are otherwise very limited.

The following entities are generally exempted from the requirements of the Final Rule, except for three of the requirements. The three requirements that an exempt entity must continue to satisfy (unless otherwise indicated) are (i) conduct a risk assessment (Sec. 500.09); (ii) implement written policies and procedures designed to secure Nonpublic Information that is accessible to, or held by, third party service providers (Sec. 500.11); and (iii) establish policies and procedures for the secure disposal of Nonpublic Information that is no longer necessary for business operations or other legitimate business purposes (Sec. 500.13).

- **Small Covered Entities**. Covered Entities with:
  - fewer than 10 employees, including any independent contractors, of the Covered Entity or its Affiliates located in New York or responsible for business of the Covered Entity
  - 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
  - less than $10 million in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates.

- **Designees covered by other Covered Entities**. If a Covered Entity's cybersecurity program covers an employee, agent, representative or designee, then that other person or entity does not need to satisfy the requirements of the Rule. For example, if ABC Insurance Company has a cybersecurity program that covers its appointed agents, then even though the individual agent holds a license from the NYDFS (and would therefore be a Covered Entity), the agent will not have to comply with the requirements of the Rule because it is covered by ABC Insurance Company's cybersecurity program.

  These persons or entities are completely exempt from the Final Rule and do not have to satisfy the three requirements described above.

- **Covered Entities with no access to Nonpublic Information**. a Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information.

- **Captive insurance companies**, including pure captive insurance companies and industrial insured group captive insurance companies (as licensed under Article 70 of the Insurance Law) which do not and are not required directly or indirectly to control, own, access, generate, receive or possess Nonpublic Information other than information relating to its corporate parent company (or affiliates).

- **The following Persons**, as long as the Persons do not otherwise qualify as a Covered Entity and are not otherwise covered under the requirements:
  - Any **accredited reinsurer or certified reinsurer**. Accredited reinsurers and certified reinsurers are unauthorized

or alien assuming insurers that have obtained accreditation or certification from the NYDFS acknowledging that the entity meets certain standards of solvency and is in compliance with regulatory requirements under which a licensed ceding insurer may be allowed credit for reinsurance

- **Risk retention groups (RRG)** that were not chartered in New York but operate in New York subject to Insurance Law Section 5904. An RRG is an insurance company that is owned by the insureds and formed pursuant to the federal Risk Retention Act of 1981 (as amended in 1986) to allow insurers to underwrite all types of liability risks except workers compensation without having to comply with licensing laws on a multi-state basis and
- **Charitable annuity societies** that hold a permit under Insurance Law section 1110 . A charitable annuity society is a nonprofit organization engaged solely in charitable, religious, missionary, educational or philanthropic activities that obtains a permit from the NY Department of Financial Services so that it may make annuity agreements with donors.

These entities are completely exempt from the Final Rule and do not have to satisfy the three requirements described above. However, if any of these entities holds an insurance license for another purpose, then the entity is a Covered Entity and would be subject to the Final Rule.

A Covered Entity that qualifies for the (i) small Covered Entity; (ii) designees covered by other Covered Entities; (iii) Covered Entities with no access to nonpublic information; and (iv) the captive insurance company exemptions (as described above) must file a Notice of Exemption in a form set forth in Appendix B of the Final Rule within 30 days of determining that its Covered Entity is exempt.

Find out more about the implications of the Final Rule for your business by contacting any of the authors.

---

[1] The definition covers (1) business information that if tampered with or subject to unauthorized disclosure, access or use would cause material adverse impact to the Covered Entity or its security, (2) an individually identifiable information in combination with a breach notice data elements (SSN, account or payment card number, financial account password or security code, or biometric record), as well as (3) any information created by or derived from an individual or health care provider that relates to past, present or future health or condition of an individual or family member, provision of or payment for the provision of healthcare to any individual. § 500.1(g).