New York finalizes cybersecurity regulations for financial institutions

Jonathan G. Cedarbaum, Benjamin A. Powell, D. Reed Freeman, Leah Schloss and Reed Abrahamson

Abstract

Purpose – *To analyze the cybersecurity regulations for financial institutions issued by the New York State Department of Financial Services on February 16, 2017.*

Design/methodology/approach – *This article summarizes the regulations' scope and requirements including definition of Covered Entities and substantive requirements including periodic Risk Assessments, cyber policies, dedicated and trained personnel, testing, audit trails, control over Third Party Service Providers, authentication, secure disposal, encryption, and incident reporting.*

Findings – *The regulations go beyond federal requirements in a number of important respects.*

Originality/value – *This article provides a guide for regulated entities to start preparing for compliance with the new regulations from experienced lawyers with specialties in cybersecurity, privacy and communications.*

Keywords *Authentication, Risk assessment, Cybersecurity, Policies and procedures, New York State Department of Financial Services (NYDFS), Encryption*

Paper type *Technical paper*

Jonathan G. Cedarbaum (jonathan.cedarbaum@wilmerhale.com) is a partner, Benjamin A. Powell (benjamin.powell@wilmerhale.com) is partner and co-chair of the Cybersecurity, Privacy and Communications Practice, D. Reed Freeman, Jr. (reed.freeman@wilmerhale.com) is a partner and co-chair of the Cybersecurity, Privacy and Communications Practice, Leah Schloss (leah.schloss@wilmerhale.com) is a senior associate and Reed Abrahamson (reed.abrahamson@wilmerhale.com) is a senior associate, all are based at Wilmer Cutler Pickering Hale and Dorr LLP in Washington, DC, USA.

On February 16, the New York State Department of Financial Services (NYDFS) issued cybersecurity regulations for banks, insurance companies and other financial institutions subject to NYDFS jurisdiction. The regulations, which take effect March 1, 2017, are available at www.governor.ny.gov/sites/governor.ny.gov/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf. Entities subject to the regulations will have 180 days from the effective date to come into compliance with most requirements, though certain provisions allow up to two years after the effective date[1].

First proposed in September 2016 and revised after two rounds of public comment, the regulations establish requirements that in some respects duplicate federal data security obligations for financial institutions, but in some important respects differ from and go beyond federal requirements. Notably, the NYDFS regulations rely on a definition of "Nonpublic Information" that must be protected that is considerably broader than the definition of "customer information" under the federal Interagency Guidelines Establishing Information Security Standards[2], and the regulations impose:

- obligations to report cybersecurity incidents to NYDFS;
- an annual certification requirement concerning compliance with the regulations;
- requirements concerning oversight of third-party service providers;
- obligations concerning use of multi-factor authentication and encryption; and
- requirements concerning audit trail maintenance and document destruction.

DOI 10.1108/JOIC-04-2017-0020

Covered entities

The regulations apply to persons and organizations "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under" New York's Banking Law, Insurance Law, or Financial Services Law, with several exemptions. Smaller entities will be exempted from most of the regulations' specific requirements but will still have to establish a cybersecurity program, undertake regular risk assessments, use encryption, and report to NYDFS annually and in the event they suffer a breach meeting certain characteristics[3].

Substantive requirements

"Covered entities" are required:

- to "conduct a *periodic Risk Assessment* of the Covered Entity's Information Systems sufficient to inform the design of the cybersecurity program [. . .] updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations [. . .] carried out in accordance with written policies and procedures and [. . .] documented"; (500.09)
- to "maintain a *cybersecurity program*" designed "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"; (500.02)
- "to implement and maintain a written" *cyber policy* "approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems," addressing 14 functions, including data classification, access controls, business continuity, application development and security, and incident response; (500.03)
- to "designate a qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy (for purposes of this Part, '*Chief Information Security Officer*' or 'CISO')"; (500.04)
- to undertake *penetration testing and vulnerability assessments*; (500.05)
- to maintain *audit trails* "designed to reconstruct material financial transactions sufficient to support normal operations and obligations" for five years and "designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of [. . .] normal operations" for five years; (500.06)
- to establish *access privileges*; (500.07)
- to maintain policies and procedures to ensure the security of applications developed in-house or purchased externally; (500.08)
- to hire and train qualified *cybersecurity personnel*; (500.10)
- to "implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, *Third Party Service Providers*," including "relevant guidelines for due diligence and/or contractual protections" relating to access controls, including multi-factor authentication, encryption and breach notification; (500.11)
- to use *multi-factor authentication* "for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls"; (500.12)

- to adopt “policies and procedures for the *secure disposal* on a periodic basis” of certain categories of personally identifiable information; (500.13)
- to “implement risk-based policies, procedures and controls designed to *monitor the activity of Authorized Users* and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users; and provide regular cybersecurity awareness *training*”; (500.14)
- to *encrypt* Nonpublic Information “held or transmitted by the Covered Entity both in transit over external networks and at rest,” unless it determines that encryption is “infeasible” and its Chief Information Security Officer approves “effective alternative compensating controls”; (500.15) and
- to “establish a written *incident response plan* designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Covered Entity’s Information Systems or the continuing functionality of any aspect of the Covered Entity’s business or operations.” (500.16)

Reporting requirements

Covered entities will also face new reporting requirements:

- Covered entities must notify NYDFS “as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that either triggers an obligation to give notice to any government body, self-regulatory agency or any other supervisory body,” or that has “a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity”; (500.17(a)) and
- By February 15 each year, covered entities must submit a form certifying that the covered entity is in compliance with the regulations; covered entities must maintain for examination by NYDFS “all records, schedules and data supporting this certificate for a period of five years”; “{t]o the extent a Covered Entity has identified areas, systems or processes that require material improvement, updating or redesign, the Covered Entity shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes” and make the documentation “available for inspection by the superintendent”. (500.17(b))

Notes

1. Covered entities have until March 1, 2018, to comply with the following provisions: 500.04(b) (annual CISO reports to the board of directors); 500.05 (penetration and vulnerability assessments), 500.09 (risk assessments), 500.12 (multi-factor authentication) and 500.14(b) (cybersecurity awareness training). Covered entities have until September 1, 2018, to comply with the following provisions: 500.06 (audit trails), 500.08 (application security), 500.13 (data retention and destruction), 500.14 (a) (monitoring of authorized users) and 500.15 (encryption). Covered entities have until March 1, 2019, to comply with the third-party service provider provision, section 500.11.

2. See Subsection 500.01(g): (g) 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.

3. See Subsection 500.19(a): (a) Limited Exemption. Each Covered Entity with: (1) 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, or (2) less than $5,000,000 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 $10,000,000 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. Other exemptions include: (b) An employee, agent, representative or designee of a Covered Entity, who is itself a Covered Entity, is exempt from this Part and need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the Covered Entity. (c) 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 shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part. (d) A Covered Entity under Article 70 of the Insurance Law that does not and is not required to directly or indirectly control, own, access, generate, receive or possess Nonpublic Information other than information relating to its corporate parent company (or Affiliates) shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part. (f) The following Persons are exempt from the requirements of this Part, provided such Persons do not otherwise qualify as a Covered Entity for purposes of this Part: Persons subject to Insurance Law section 1110; Persons subject to Insurance Law section 5904; and any accredited reinsurer or certified reinsurer that has been accredited or certified pursuant to 11 NYCRR 125.

Corresponding author

Jonathan G. Cedarbaum can be contacted at: jonathan.cedarbaum@wilmerhale.com