Clients&FriendsAlert

NEW YORK STATE REVISES "FIRST-IN-NATION" CYBERSECURITY RULES

January 10, 2017

INTRODUCTION

The New York Department of Financial Services ("DFS") recently issued a revised version of the cybersecurity rules[1] that it first announced in the fall of last year. The rules apply to a wide range of insurance, banking, and financial services companies under the DFS's supervision and require them to adopt robust cybersecurity programs to protect sensitive and confidential data from theft by cybercriminals. Although the revised rules appear to incorporate some of the comments made by the public and industry groups during a notice and comment period in the fall, they still impose a number of rigorous new cybersecurity requirements that will affect not just companies regulated by the DFS but many of the third party service providers who have access to confidential corporate data or systems. The new rules also leave open the question as to whether the DFS will bring enforcement actions against covered entities – and potentially their employees – for non-compliance.

BACKGROUND

On September 13, 2016, the DFS first announced and published its proposed cybersecurity rules (the "Original Rules"), which were subject to a notice and comment period.[2] On December 28, 2016, the DFS issued a revised version of the rules (the "Revised Rules"), which are subject to a new 30-day notice and comment period.[3] The Revised Rules are scheduled to become effective on March 1, 2017 and require "Covered Entities"[4] to comply with most of their provisions within six months of their effective date.[5]

---

1 N.Y.S. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies (Proposed) – 23 N.Y.C.R.R. Part 500, http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf (hereinafter "Part 500" or "Section 500.__").

2 *See* http://www.dfs.ny.gov/about/press/pr1609131.htm (hereinafter "Press Release ¶ __").

3 *See* http://www.dfs.ny.gov/about/press/pr1612281.htm.

4 The rules define "Covered Entity" as "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, Insurance Law, or the Financial Services Law [of New York]." Section 500.01(c). Certain entities may qualify for exemptions from the cybersecurity rules

When Governor Andrew Cuomo first announced the Original Rules in the fall, he stated that New York was "leading the nation in taking decisive action" to address potentially costly cybersecurity threats.[6] The significant concentration of insurance, banking, and financial services entities in New York ensure that the Revised Rules will play an important role in shaping cybersecurity programs across the nation.

I. THE REGULATIONS REQUIRE COVERED ENTITIES TO DEVELOP ROBUST CYBERSECURITY PROGRAMS AND POLICIES

The DFS views it as "critical" that Covered Entities develop and maintain robust cybersecurity programs designed to protect the integrity, confidentiality, and availability of their electronic information resources or "Information Systems".[7] Accordingly, the Revised Rules provide for the following:

- *Cybersecurity Programs*. Under the Revised Rules, Covered Entities must develop cybersecurity programs that perform the following functions, among others: (i) identify and assess internal and external cybersecurity risks; (ii) protect Information Systems and Nonpublic Information[8] from unauthorized access; (iii) detect, respond to, and recover from cybersecurity incidents; and (iv) fulfill applicable regulatory reporting requirements.[9]

- *Cybersecurity Policies*. The Revised Rules provide that each Covered Entity implement and maintain a written cybersecurity policy that is approved by a senior officer or the board of directors and that addresses (to the extent applicable), among other things: (i) information security; (ii) data governance and classification; and (iii) customer data privacy.[10]

---

including, for example, entities that (i) have fewer than 10 employees or (ii) have less than $5,000,000 in gross annual revenue for each of the last three years. Section 500.19.

5 Sections 500.21 and 500.22.

6 Press Release ¶ 2.

7 Sections 500.00, 500.01(e) and 500.02. The rules define "Information System" as 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 environment control systems." Section 500.01(e).

8 "Nonpublic Information" refers to "all electronic information" that is not publicly available and is either (i) business information, the unauthorized disclosure or use of which would have a materially adverse impact on a Covered Entity; (ii) personal identifying information such as a person's name in combination with other personal data records such as the person's social security number, account number, or password; or (iii) healthcare-related information. Section 500.01(g).

9 Section 500.02.

10 Section 500.03.

- *Cybersecurity Risk Assessments.* Covered Entities are required by the Revised Rules to periodically undertake a comprehensive assessment of the cybersecurity risks affecting their business operations, Information Systems, and Nonpublic Information.[11] These risk assessments are to be carried out according to developed written policies and procedures, which must include criteria for (i) evaluating and categorizing cybersecurity risks facing the company; (ii) assessing the security of the company's Information Systems and Nonpublic Information; (iii) evaluating the adequacy of existing controls in the context of the identified risks; and (iv) determining how risks identified by the risk assessment will be mitigated (or accepted) by the company.[12]

- *Appointment of a Chief Information Security Officer.* The Revised Rules also require the designation of a qualified individual, referred to as the Chief Information Security Officer ("CISO"), to be responsible for the oversight, implementation, and enforcement of the cybersecurity program and policies.[13] Unlike the original version of the rules, the Revised Rules do not require that the CISO serve exclusively in that function or that Covered Entities create a new CISO position.[14] Instead, companies can designate someone already employed by the company, one of its affiliates, or a third party service provider to take on the additional responsibilities of the CISO.[15] Under the rules, the CISO must provide a written report to the board of directors regarding the company's cybersecurity program at least once a year.[16]

- *Technical Security Requirements.* The Revised Rules further impose certain technical requirements on Covered Entities, including requiring that companies: (i) use Multi-Factor Authentication in certain circumstances[17]; (ii) encrypt Nonpublic Information where feasible[18]; and (iii) periodically engage in penetration and vulnerability testing to ensure the security and integrity of the company's Information Systems.[19] Multi-Factor Authentication must be used for access to the company's internal network from an external network (such as when employees access their employer's network from home or while traveling), unless

[11] Section 500.09(a).

[12] Section 500.09(b).

[13] Section 500.04(a).

[14] Public Comments at 2; *see* N.Y.S. Regis. at 25.

[15] Section 500.04(a).

[16] Section 500.04(b).

[17] Section 500.12. As defined in Section 500.01(f), Multi-Factor Authentication is the use of at least two different types of authentication factors (*e.g.,* a password and a token) to verify that a user is authorized to access Information Systems.

[18] Section 500.15.

[19] Section 500.05.

the CISO has approved the use of a reasonable equivalent (or more secure) access control.[20] The Revised Rules also require encryption, if feasible, of Nonpublic Information held in the company's Information Systems or in transit over external networks.[21] If encryption is not feasible, then the company can secure Nonpublic Information using effective alternatives approved by the CISO.[22]

II. THE REGULATIONS CREATE STANDARDS FOR RECORDS MAINTENANCE AND REGULATORY REPORTING

The Revised Rules also impose standards for recordkeeping and regulatory reporting, including the reporting of cybersecurity incidents and data breaches to the DFS.

- *Recordkeeping*. The Revised Rules require companies to design and maintain effective record-keeping systems. These systems must be tailored to the risks facing the company and must include (i) audit trails that are designed to detect and respond to cybersecurity events and (ii) systems that can reconstruct material financial transactions sufficient to support the company's normal operations.[23] Such records must be retained for at least five years.[24]

- *Annual Compliance Certification and DFS Oversight*. Boards of directors or senior officers of Covered Entities must provide DFS with an annual written certification of compliance with respect to the Revised Rules.[25] This requirement begins on February 15, 2018 and requires new compliance certifications on February 15 of every year thereafter. In addition, the Revised Rules require that a company must produce "[a]ll documentation and information relevant" to its cybersecurity program upon request by the DFS.[26]

---

[20] Section 500.12.

[21] Section 500.15(a).

[22] Section 500.15(a)(1) and (2).

[23] Section 500.06(a).

[24] Section 500.06(b).

[25] Section 500.17 and 500.21.

[26] Section 500.02(d). The Revised Rules provide that information given by a regulated entity to the DFS enjoys certain protections from public disclosure. *See* Section 500.18 ("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"). This provision was added based on concerns expressed by commentators about the confidentiality of notices provided to DFS. *See* Cybersecurity Requirements for Financial Services Companies, No. DFS-39-16-00008-RP, N.Y.S. Regis. 23, 26 (Dec. 28, 2016), https://docs.dos.ny.gov/info/register/2016/dec28/pdf/rulemaking.pdf#page=23 (hereinafter "N.Y.S. Regis. at __").

- *Cybersecurity Incident Reporting*. The Revised Rules require that Covered Entities must report to the DFS within 72 hours of determining that a "cybersecurity event"[27] has occurred that either (i) has a reasonable likelihood of materially harming its normal operations or (ii) must otherwise be reported to a governmental authority.[28] This 72-hour reporting requirement was the subject of many comments, particularly complaining that the time allowed for making a disclosure was too short; however, DFS believed that this time frame was "essential" to protecting financial markets.[29]

III. THE RULES REQUIRE OVERSIGHT OF THIRD PARTY SERVICE PROVIDERS

The Revised Rules also focus on the cybersecurity of third party service providers that have access to the sensitive information or computer networks of Covered Entities. Although the Revised Rules do not directly impose cybersecurity obligations on third parties that are not otherwise under the DFS's supervision, the rules do require that the Covered Entities themselves impose cybersecurity requirements on any third party service provider that has access to the Information Systems or Nonpublic Information of a Covered Entity.[30] Among other things, the rules require Covered Entities to (i) understand the cybersecurity risks posed by a third party service provider; (ii) assess the continued adequacy of any third party service provider's cybersecurity practices; (iii) identify the minimum cybersecurity practices that a third party service provider must meet; and (iv) create guidelines for due diligence and contractual protections with respect to third party service providers used by a Covered Entity, including contractual representations and warranties addressing the adequacy of a third party service provider's cybersecurity program.[31]

CONCLUSION

The Revised Rules reflect New York's strong belief that "time is of the essence regarding cybersecurity protections."[32] Although New York State is taking the lead in establishing these minimum standards for cybersecurity programs, it is the Covered Entities that bear the responsibility – and possibly liability – for failing to meet these new standards imposed by the proposed regulations.

---

[27] The rules define "cybersecurity event" as "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." Section 500.01(d).

[28] Section 500.17(a).

[29] N.Y.S. Dep't of Fin. Servs., Assessment of Public Comments for New Part 500 to 23 N.Y.C.R.R. at 4, http://www.dfs.ny.gov/legal/regulations/proposed/rp500apc.pdf; (hereinafter "Public Comments at __"); *see* N.Y.S. Regis. at 26.

[30] Section 500.11(a).

[31] Section 500.11(a) & (b).

[32] N.Y.S. Regis. at 26.

Indeed, failure to comply with the Revised Rules could result in DFS enforcement actions. The DFS is empowered to take any action that it "deems necessary to … protect users of financial products and services."[33] While it is not clear, at this point, how aggressively the DFS will seek to penalize Covered Entities that fail to comply with the Revised Rules, it is the Superintendent's view that cybersecurity is one issue where New York should lead.[34] In the past, the DFS has imposed steep fines on Covered Entities (and/or demanded the termination of compliance officers) that allegedly failed to implement and maintain appropriate policies and procedures in other contexts – such as with anti-money laundering compliance programs.

Accordingly, the Revised Rules create new areas of uncertainty, and potential liability, for Covered Entities, their boards, their senior officers, and CISOs. Moreover, third party service providers, including professional services firms, may find themselves facing new demands from their clients to adopt appropriate cybersecurity compliance programs.

* * * *

If you have questions, please contact any of the following Cadwalader attorneys:

John T. Moehringer	+1 212 504 6731	john.moehringer@cwt.com
Joseph Facciponti	+1 212 504 6313	joseph.facciponti@cwt.com
Howard Wizenfeld	+1 212 504 6050	howard.wizenfeld@cwt.com

[33] N.Y. Fin. Serv. Law § 301 (2012).

[34] "New York's New Bull on Wall Street," by C. Lane, WRVO Public Media, October 24, 2016. http://wrvo.org/post/new-york-s-new-bull-wall-street.