Clients&FriendsMemo

New York State Releases Final "First-In-Nation" Cybersecurity Rules

February 28, 2017

Introduction

The New York Department of Financial Services ("DFS") recently released the much-anticipated final version of its "first-in-nation" cybersecurity rules that it first announced in the fall of last year.[1] The rules require a wide range of insurance, banking, and financial services companies to adopt robust cybersecurity programs to protect sensitive and confidential data from theft or harm by cybercriminals.

This is the second, and final, time that DFS has revised the cybersecurity rules. We previously have summarized the key provisions of the rules after their initial revisions.[2] This final round of revisions clarifies (i) which cybersecurity events are subject to a notice requirement, (ii) the amount of time that entities are required to maintain records related to cybersecurity events, and (iii) when certain exemptions to the rules apply. Ultimately, however, the revised rules retain the rigorous new cybersecurity requirements imposed by the previous revision of the rules.

The DFS's cybersecurity rules affect not only companies regulated by the DFS, but many of the third party service providers who have access to confidential corporate data or systems. The rules also may expose financial services companies – and, potentially, their employees – to enforcement actions and penalties for non-compliance.

Background

On September 13, 2016, the DFS first announced and published its proposed cybersecurity rules, which were subject to a 45-day notice and comment period.[3] On December 28, 2016, the DFS issued a revised version of the rules, subject to a new 30-day notice and comment period.[4] The

---

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/adoptions/rf23-nycrr-500_cybersecurity.pdf (hereinafter "Section 500").

2 *New York State Revises "First-in-Nation" Cybersecurity Rules*, Cadwalader, Wickersham & Taft LLP, http://www.cadwalader.com/resources/clients-friends-memos/new-york-state-revises-first-in-nation-cybersecurity-rules.

3 *See* http://www.dfs.ny.gov/about/press/pr1609131.htm.

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

final version of the rules was released on February 16, 2017.[5] The rules will become effective on March 1, 2017 and require "Covered Entities"[6] to comply with most of their provisions within six months of their effective date.[7]

Governor Cuomo announced the final version of the cybersecurity rules by declaring that "New York is the financial capital of the world, and it is critical that we do everything in our power to protect consumers and our financial system from the ever increasing threat of cyber-attacks."[8] The significant concentration of insurance, banking, and financial services entities in New York ensure that the final rules will play an important role in shaping cybersecurity programs across the nation.

I. The Revisions Clarify Notice and Record-Keeping Requirements

The final version of the rules clarifies the length of time that records must be maintained by Covered Entities. Under the final rules, Covered Entities must preserve for five years records necessary to reconstruct material financial transactions sufficient to support the normal operations of a company,[9] but need only preserve for three years audit records that are designed to detect and respond to cybersecurity events that can materially harm the normal operations of a company. This is a departure from the prior version of the rules, which imposed a five-year retention period for all categories of records covered by the rules.

The final rules also clarify that Covered Entities are required to notify the DFS within 72 hours of a cybersecurity event when *either* (i) there is a pre-existing duty to notify a separate government body or regulatory agency, such as the SEC or the FTC, of a cybersecurity event that impacts the Covered Entity *or* (ii) the cybersecurity event at issue has a reasonable likelihood of materially harming *any* part of the normal operations of a Covered Entity.

---

5 *See* http://www.dfs.ny.gov/about/press/pr1702161.htm.

6 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, the Insurance Law, or the Financial Services Law [of New York]." Section 500.01(c). Certain entities may qualify for exemptions from the cybersecurity rules 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 fiscal years from New York business operations of the Covered Entity and its Affiliates, or (iii) less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates. Section 500.19.

7 Sections 500.21 and 500.22: "Covered Entities shall have 180 days from the effective date of this Part to comply with the requirements set forth in this Part, except as otherwise specified."

8 *Governor Cuomo Announces First-in-the-Nation Cybersecurity Regulation Protecting Consumers and Financial Institutions from Cyber-Attacks to Take Effect March 1*, New York State Pressroom (Feb. 16, 2017), https://www.governor.ny.gov/news/governor-cuomo-announces-first-nation-cybersecurity-regulation-protecting-consumers-and.

9 23 NYCRR 500.06.

II. The Revisions Provide New Exemptions to Certain Types of Entities

The final rules also modify the criteria for determining which entities are exempted from compliance with all or part of the rules. In general, the rules apply to entities, such as financial institutions and insurance companies, that are licensed by the DFS.[10] Prior versions of the rules already provided exemptions for entities employing less than ten people or with less than five million dollars in annual revenue.[11] The final version of the rules provide additional partial exemptions for entities that do not control or possess nonpublic information[12] and create new exemptions for (i) charitable annuity societies which are conducted without profit and solely in charitable or philanthropic activities,[13] (ii) insurance providers not chartered in New York state but nevertheless operating within the state,[14] and (iii) reinsurers who accept credits or assets from an assuming insurer not authorized in the state.[15]

Conclusion

The final version of the rules leave intact nearly all of the stringent requirements of New York's new cybersecurity regulations, sending a clear message that New York intends to lead the nation in protecting sensitive corporate systems and data from cyber attacks. These new rules impose significant new burdens on entities subject to regulation by the DFS and, potentially, significant penalties and sanctions for failure to comply with the rules. Entities covered by the rules now have only six months to comply with many of the rules' new requirements.

* * * *

If you have any questions, please feel free to contact any of the following Cadwalader attorneys.

Joseph Facciponti	+1 212 504 6313	joseph.facciponti@cwt.com
John T. Moehringer	+1 212 504 6731	john.moehringer@cwt.com
Howard Wizenfeld	+1 212 504 6050	howard.wizenfeld@cwt.com
Alejandra Contreras	+1 212 504 6017	alejandra.contreras@cwt.com

[10] Section 500.01 Definitions.

[11] Section 500.19 (a).

[12] Section 500.19 (c)-(d).

[13] Section 500.19 (f) Exemption for N.Y. Insurance Law Section 1100 individual or entity.

[14] Section 500.19 (f) Exemption for N.Y. Insurance Law Section 5904 individual or entity.

[15] Section 500.19 (f) Exemption for 11 NYCRR 125 individual or entity.