THE
NATIONAL LAW REVIEW

New York Department of Financial Services Modifies, Delays Implementation of Cybersecurity Rules

Morgan Lewis

Article By
Charles M. Horn
Mark L. Krotoski
Morgan, Lewis & Bockius LLP
Law Flash

- Communications, Media & Internet
- Financial Institutions & Banking

- New York

Wednesday, January 11, 2017

The modified rules, which still remain among the most prohibitive, could be adopted in final form as early as this month.

Since September 2016, the New York State Department of Financial Services (DFS) has been considering proposed "first-in-the-nation" cybersecurity rules (Proposed Rules) that would require banks, insurers, and other DFS-regulated financial services companies (Covered Entities) to adhere to new stringent cybersecurity requirements. (read the DFS press release.) The Proposed Rules, originally designed to take effect on January 1, 2017, were the subject of significant comments and criticism.

After the first comment period closed on December 28, 2016, the DFS revised its Proposed Rules and delayed the effective date until March 1 (read the DFS press release). While some modifications were made to the original Proposed Rules, all Covered Entities would still be subject to one of the most, if not *the* most, prohibitive and burdensome cybersecurity regimes.

We have previously written about the Proposed Rules and submitted a comment letter to the DFS on the Proposed Rules.

DFS Re-Issues Cybersecurity Proposed Rules

The DFS issued the revised rules after receiving comments and suggestions from various trade groups and interested parties. In some instances, the revised rules incorporate comments made by Morgan Lewis and others.

- The revised rules permit a Covered Entity's chief information security officer (CISO) and security personnel to be employed by an affiliate, which would increase a Covered Entity's organizational flexibility in complying with the CISO requirement. In addition, under the revised rules, the CISO appears not to be a required title but, rather, a description of functional responsibilities that a Covered Entity could assign to a person with another title.

- Covered Entities now have the flexibility to perform a risk assessment on which many of the other requirements are based, thereby limiting or reducing certain requirements. The risk assessment will allow a Covered Entity to develop and revise its controls to respond to technological developments and evolving threats. It also will take into account the particular risks of the Covered Entity's business operations related to cybersecurity, nonpublic information collected or stored, information systems utilized and the availability and effectiveness of controls to protect nonpublic information and information systems. In our view, this is an important and helpful change because it allows Covered Entities to take a materially more risk-based approach in complying with the Proposed Rules.

- Based on the risk assessment, Covered Entities may only need to use either multi-factor or risk-based authentication, other than in cases where persons may access the Covered Entity's internal network from an external network, in which case multi-factor authentication would still be required.

- DFS has modified the cybersecurity breach notification rules by revising the requirements to remove "potential" hacks. DFS further eliminated the requirement to notify DFS when a Covered Entity identifies any material risk of imminent harm. Because the definition of "Cybersecurity Event" includes "any act or attempt, successful or unsuccessful," however, the revised notification requirement may not reduce reporting requirements.

- DFS revised the "Small Covered Entity Exemption," eliminating the exemption for entities with less than 1,000 customers in each of the last three calendar years. The revised exemption, however, has been expanded to Covered Entities with fewer than 10 employees (including independent contractors).

DFS also made several other revisions that include reducing the audit trail requirement; limiting the frequency of certain reviews, reports, and assessments; and modifying several provisions on third party service providers.

Notably, DFS did not make changes to provisions that may prove burdensome for Covered Entities, including the notification and annual compliance certification requirements. Thus, among other things, the following remains the case:

- The Proposed Rules would apply to Covered Entities irrespective of whether

Covered Entities already adhere to cybersecurity regulations imposed at the federal or state level.

- The Proposed Rules create new cybersecurity standards that may conflict with other federal and state requirements.
- The first-in-the-nation regulation retains the strict 72-hour notification standard that requires Covered Entities to report cybersecurity events in broad-ranging circumstances—many of which occur frequently—such as unauthorized attempts to access a Covered Entity's systems.
- DFS did not amend the annual compliance certification requirement. Accordingly, Covered Entities will continue to be required to submit a certification stipulating that the board of directors has reviewed reports and other documentation and that, to the best of the board's knowledge, the cybersecurity program complies with DFS rules.

Since Morgan Lewis previously commented on several aspects of the Proposed Rules, and given the impact of the Proposed Rules, we plan to submit a second comment letter addressing our clients' concerns.

What Next?

The Proposed Rules would now become effective on March 1, 2017, with several transition periods for certain requirements. For example, Covered Entities will be required to submit the certification of compliance as of February 15, 2018, and will have

- one year from the effective date to comply with the CISO reporting requirement, penetration testing and vulnerability assessment, risk assessment, multi-factor authentication, and cybersecurity awareness training;
- 18 months to comply with audit trail, application security, limitations on data retention, monitoring procedures, and encryption of nonpublic information; and
- two years to comply with third party service provider security policy.

We do not expect that DFS will make material changes to the Proposed Rules when they are adopted in final form, which could happen as early as later this month. Therefore, Covered Entities should closely monitor DFS announcements for the final rules and ensure that they are ready for the Compliance Dates, which means that they should start taking steps necessary to comply with the fundamental requirements that the DFS likely will adopt in some fashion.

Copyright © 2019 by Morgan, Lewis & Bockius LLP. All Rights Reserved.

Source URL: https://www.natlawreview.com/article/new-york-department-financial-services-modifies-delays-implementation-cybersecurity