alert Cybersecurity and Privacy Practice

Saul Ewing LLP

JANUARY 2017

# The New York Department of Financial Services' Cybersecurity Regulation Will Soon Take Effect

**Authors:**
April F. Doss
Frederic M. Garsson

**SUMMARY**

**The New York Department of Financial Services ("NYDFS") is in the final days of accepting public comment on its revised cybersecurity regulation, which would be codified at 23 NYCRR 500. As the comment period winds down to a close, most observers are expecting the NYDFS to issue its final regulation with very few additional changes – making this a perfect time for Covered Entities to consider what steps they should be taking now in order to be in compliance with the rules when they are likely to take effect on March 1, 2017.**

## Background

In September 2016, the NYDFS issued a proposed cybersecurity regulation that would require Covered Entities (defined below) to adopt and implement a set of cybersecurity protections considerably more robust and demanding than those that are required under Gramm-Leach-Bliley. It included a number of controversial provisions, such as a very broad definition of Nonpublic Information, requirements that Covered Entities encrypt all Nonpublic Information at rest and in transit, and a requirement that Covered Entities notify the NYDFS within 72 hours of any Cybersecurity Event (which was defined to include low-level security risks as well as actual data breaches). The NYDFS received extensive comments from industry groups and others, pointing out that some provisions would be extremely costly to implement, that some provisions would have a disproportionate impact on small and mid-sized Covered Entities, and that some provisions were simply not feasible (particularly some of the detailed technical and reporting requirements).

In light of those comments, the NYDFS issued a revised draft regulation on December 28th with a new 30-day comment period. It is this new regulation that commentators expect will be adopted and take effect on March 1, 2017. Covered Entities will then have 180 days to comply with most of the regulation's requirements, with timelines of up to two years to reach compliance with other provisions.

## Who does the cybersecurity regulation cover?

A "Covered Entity" is defined 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."

For the insurance industry, this includes, for example, New York licensed insurance companies, insurance agents, insurance brokers, excess line brokers, insurance producers, insurance consultants, insurance adjusters, reinsurance intermediaries and accredited reinsurers.

There are three exceptions to the regulation's applicability, but the one that is most useful will likely be the following:

> 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.

## Issues to Consider Now

Although it is possible that the NYDFS may make further substantive changes before issuing the final regulation, now is a good time for Covered Entities to examine the primary provisions of the regulation to assess what steps they will need to take to come into compliance with these new requirements. The top 10 components are the following:

1. Nonpublic Information that requires protection under the regulation is broadly defined to include business information as well as consumer personal data.
2. Covered Entities must create and implement a comprehensive cybersecurity program that:
    - is based on an individualized risk assessment;
    - addresses internal and external risks to cybersecurity;
    - incorporates defensive infrastructure and other measures to protect systems and information; and
    - addresses Cybersecurity Event detection, response, remediation and reporting.
3. Covered Entities must implement and maintain a written cybersecurity policy that:
    - is approved by a senior officer or the Board of Directors; and
    - addresses 14 detailed topic areas relating to cybersecurity.
4. Covered Entities must designate a "qualified individual" to serve as Chief Information Security Officer for the entity; this person can be a company employee or an external vendor.
5. Covered Entities must implement specific technical measures such as:
    - Penetration testing and vulnerability assessments;
    - Audit trails;
    - Identity and access privilege management processes;
    - Application security measures;
    - Use of multi-factor authentication or an appropriate alternative;
    - Limitations on data retention; and
    - Encryption or other protective measures, based on the risk assessment.
6. Covered Entities must carry out a tailored risk assessment that meets specified criteria.
7. Covered Entities must implement personnel training and monitoring programs.
8. Covered Entities must have a policy and process for managing third-party vendor liability.
9. Covered Entities must have in place an incident response plan, and must provide timely notifications to the Superintendent of Cybersecurity Events that involve a breach of personally identifiable data or that have a reasonable likelihood of "materially harming any material part of the normal operation" of the entity.
10. There are strict notice requirements in the event of a Cybersecurity Event, as well as annual compliance Certifications.

## Timing

The regulation is expected to become effective on **March 1, 2017.**

- The first Certification of Compliance is expected to be due on **February 15, 2018.**
- Covered Entities have **180 days** from the regulation's effective date to comply with all requirements of the regulation **except as specified below**:
- **One year from the effective date to comply with:** 500.4(b) (Annual Report to the Board), 500.5 (Penetration Testing), 500.9 (Risk Assessment), 500.12 (Multi-Factor Authentication), 500.14(a)(2) (Personnel Training)
- **18 months from the effective date to comply with:** 500.6 (Audit Trail), 500.8 (Application Security), 500.13 (Limitation on Data Retention), 500.14(a)(1) (Monitoring of Authorized Users), 500.15 (Encryption of Nonpublic Information)
- **Two years from the effective date to comply with:** 500.11(Third Party Service Provider Security Policy)

Attorneys in Saul Ewing's Insurance and Cybersecurity and Privacy practices are working with a number of clients across the business sectors that will be affected by this proposed regulation, to help those clients ensure they are taking steps now to prepare for the regulation's adoption. We can assist with drafting programs and policies, engaging technical consultants, reviewing incident response plans, creating and delivering personnel training, and other matters required under the regulation. For more information or assistance, please contact the authors or the attorney at the firm with whom you are regularly in contact.

This Alert was written by April F. Doss, Chair of the firm's Cybersecurity and Privacy Practice, and Frederic M. Garsson, Vice Chair of the firm's Insurance Practice. April can be reached at 410.332.8798 or adoss@saul.com. Frederic can be reached at 973.286.6719 or fgarsson@saul.com. This publication has been prepared by the Cybersecurity and Privacy Practice for information purposes only.