VENABLE LLP

Cybersecurity Alert

February 27, 2017

New York's Department of Financial Services Finalizes Cybersecurity Requirements for Financial Institutions

AUTHORS

Ari Schwartz

Jami Mills Vibbert

RELATED PRACTICES

Privacy and Data Security

Banking and Financial Services Regulatory

Risk and Compliance (RCOM)

RELATED INDUSTRIES

Cybersecurity Risk Management Services

Financial Services

ARCHIVES

2017 2013 2009

2016 2012 2008

2015 2011 2007

2014 2010

On March 1, 2017, the New York State Department of Financial Services' (DFS) mandatory **cybersecurity requirements** for financial services entities will become effective, with implementation to occur within 180 days (or by September 1, 2017). The requirements broadly cover all entities operating under or required to operate under DFS licensure, registration, or charter, or which are otherwise DFS-regulated, as well as, by extension, unregulated third-party service providers to regulated entities. This not only includes state-chartered banks, licensed lenders, private bankers, service contract providers, trust companies, and mortgage companies, but also foreign banks licensed to operate in New York and any insurance company doing business in New York. It does exempt small companies, though, including those with fewer than 10 employees, less than $5 million in gross annual revenue for three years, or less than $10 million in year-end total assets.

The regulation delineates various minimum standards and requires a risk-based cybersecurity program tailored to each company's specific risk profile. Significantly, the regulation requires covered entities to file an annual certification of compliance with the regulation; Certifications of Compliance will commence February 15, 2018.

As discussed in a **prior alert**, DFS proposed similar regulations on September 13 of last year, but that set of regulations elicited significant feedback. Still, the regulations require potentially significant changes and focus on cybersecurity for many institutions.

Requirements

Generally, the regulation's requirements are focused on steps to increase security awareness and to encourage a risk-based, holistic, and robust security program at covered entities. To ensure compliance, covered entities must implement the following:

1. *Risk Assessments:* Periodic risk assessments that consider threats, particular risks to the entity, and an examination of existing controls in the context of identified risk.

2. *Cybersecurity Program:* The creation of a cybersecurity program based on the periodic risk assessments and designed to identify and assess risks; protect information systems and nonpublic information; detect, respond to, and recover from cyber events; and fulfill all reporting obligations. The program must include annual penetration testing and biannual vulnerability assessments. The cybersecurity program referenced here follows the general mandates of those delineated in the NIST Cybersecurity Framework.

3. *Cybersecurity Policies:* The creation and maintenance of written policies and procedures for the protection of information systems and nonpublic information and based on the risk assessment. These must include a written incident response plan.

4. *CISO:* The designation of a chief information security officer to oversee the cybersecurity program.

5. *Minimum Standards:* Implementation of minimum cybersecurity standards, including systems designed to recover material financial transactions following an event and audit trails to detect events, the institution of appropriate access privileges, procedures for evaluating and testing the security of applications, multifactor authentication, data disposal, mandatory cybersecurity awareness training, and encryption measures.

6. *Third-Party Risk Management:* Implementation of a third-party risk management program, including a review of the cybersecurity practices of those providers and periodic assessment and audit thereof.

These new requirements, which are the first of their kind, signal an increased focus on risk-prioritized and managed cybersecurity.

Save the Date: On March 14, the article's authors will lead a discussion in **Venable's New York City office** concerning conducting cybersecurity due diligence in M&A deals. Sellers and purchasers subject to this regulation should consider such due diligence an important aspect of maintaining an appropriate cybersecurity program. Please email **tfacey@Venable.com** for more information on the program.