MARCH 1 DEPARTMENT OF FINANCIAL SERVICES DEADLINE FOR VENDOR MANAGEMENT HAS LAPSED. HAS YOUR ORGANIZATION COMPLIED?

Hodgson Russ Cybersecurity & Privacy Alert
March 20, 2019

The Department of Financial Services (DFS) regulation titled "Cybersecurity Requirements for Financial Services Companies" took effect on March 1, 2017. Two years later, it is clear that the industry has not come into full compliance with its onerous requirements. However, one of the requirements, vendor management, will come under scrutiny in the months to come.

The DFS regulations apply to any person or entity that is required to operate under a license or registration under New York Banking Law, Insurance Law or the Financial Services Law. These so-called "Covered Entities" include banks, insurance companies and other financial service institutions, among others. The guiding principle of the regulations is that all Covered Entities must maintain a "robust" cybersecurity program designed to protect the confidentiality, integrity and availability of its Information Systems. This is not a new concept for some in the financial industry and, therefore, many Covered Entities have been compliant with certain mandates from the beginning, *i.e.*, maintaining written policies to protect their Information Systems. For others, it is a "strange new world."

Some of the requirements are cumbersome - both technically and financially. For example, Covered Entities are required to scrutinize the practices of third party service providers that access their information systems and nonpublic information. The Covered Entity must conduct periodic assessments of its third party service providers, with particular focus on access controls, encryption and periodic training. They must also seek representations and warranties addressing the Third Party Service Provider's cybersecurity policies and procedures. But, as a DFS FAQ clarified, these representations are not sufficient to satisfy the due diligence responsibilities of Covered Entities under the regulations.

Specifically, the December, 2017, FAQ asks if a Covered Entity may rely on a "Certification of Compliance with NYSDFS Cybersecurity Regulations" as adequate due diligence. The answer:

Attorneys

Jane Bello Burke
William Ciszewski III
Alfonzo Cutaia
Reetuparna Dutta
Michael Flanagan
Michelle Merola
R. Kent Roberts
Gary Schober
Amy Walters

Practices & Industries

Cybersecurity & Privacy

"No. The Department emphasizes the importance of a thorough due diligence process in evaluating the cybersecurity practices of a Third Party Service Provider. Solely relying on the Certification of Compliance will not be adequate due diligence. Covered Entities must assess the risks each Third Party Service Provider poses to their data and systems and effectively address those risks. The Department has provided a two year transitional period to address these risks and expects Covered Entities to have completed a thorough due diligence process on all Third Party Service Providers by March 1, 2019."

In fact, all regulated entities were required to file their second annual certification of compliance by February 15, 2019. And less than fifteen days later, the vendor management requirements became enforceable. Thus, as of this date, Covered Entities should have: (1) completed risk assessments for each vendor; (2) distributed to vendors tailored questionnaires regarding security practices; (3) vetted vendor answers and required modifications to those practices as appropriate; and (4) obtained representations and warranties from vendors detailing DFS compliance.

The governance framework set forth in the regulations, including the vendor management requirements, will be enforced through ongoing DFS oversight. Specifically, DFS intends to audit compliance through regular and target examinations that are intended to "assist in the bolstering of the industry's cybersecurity defenses, for the protection of the industry, over markets and consumers." *See* December 21, 2018, Memorandum from the Superintendent Maria T. Vullo. And the consequences for noncompliance are potentially severe.

The text of the regulation does not detail how the penalties will be imposed; however, it states that the regulation will be enforced through the Superintendent's authority under applicable laws. The Superintendent has the general authority to impose penalties as follows:

- up to $2,500 per day during which violation continues,
- $15,000 per day in the event that the violation is reckless or results from an unsound practice or pattern of conduct, and
- $75,000 per day in the event of a knowing and willful violation.

With penalties of this magnitude available to the Superintendent, Covered Entities ought to take heed.

Is your organization in compliance with either the March 1, 2017 DFS deadline or the March 1, 2019 DFS deadline?

If you received this alert from a third party or from visiting our website, and would like to be added to our Cybersecurity & Privacy mailing list or any other of our mailing lists, please visit us at: https://forms.hodgsonruss.net/sign-up-for-email-and-other-communications..html.