Bond

INFORMATION MEMO
CYBERSECURITY AND DATA PRIVACY

JANUARY 2017

Proposed New York State Regulations Updated, Implementation Delayed

On September 16, 2016 we informed you of new proposed cybersecurity regulations that would cover all entities regulated by the New York State Department of Financial Services (DFS). Our original Information Memorandum can be found here.

On December 28, 2016, DFS released these revisions (Revised Regulations) to the cybersecurity regulations that had been set to go into effect on January 1, 2017. Chief among the revisions, which were made in response to approximately 150 public comments, was the delay of the effective date to March 1, 2017 and the scheduling of a new public comment period which ends on January 27.

DFS, in response to industry feedback, delayed the compliance dates for many of the provisions of the regulations. Originally, compliance with all aspects of the regulations was required by June 30, 2017. The Revised Regulations contain a series of compliance deadlines applicable to different provisions ranging from six to 24 months following the effective date.

Many of the comments received by DFS addressed the definition of "Covered Entities," which the regulations define 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." Despite comments from entities that did not feel they should be regulated, DFS opted not to change this definition.

DFS did, however, expand the types of covered entities entitled to an exemption from a subset of the regulations. DFS also changed some of the other more contentious elements of the regulations.

Exempt Entities

DFS expanded the categories of covered entities that are exempt from certain of the cybersecurity regulations. Originally entities had to have fewer than 1,000 customers ***and*** less than $5 million gross annual revenue for three year ***and*** less than $10 million in year-end total assets to earn a partial exemption. Now, to be exempt from a subset of the regulations, covered entities may have either fewer than 10 employees ***or*** less than $5 million gross annual revenue for three year ***or*** less than $10 million in year-end total assets.

Additional exemptions now exist for covered entities that do not operate, maintain, utilize or control any Information Systems and do not control, own, access, generate, receive or possess Nonpublic Information as those terms are defined by the regulations.

Covered entities that qualify for exemptions must file a "Notice of Exemption" with DFS affirming the basis for the exemption.

Cybersecurity Event Reporting

Originally, the regulations required covered entities to report cybersecurity events, which are defined as "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System," "as promptly as possible but in no event later than ***72 hours after becoming aware of such Cybersecurity Event***." The regulations provided examples of reportable events, including, but not limited to, events of which notice is provided to other governmental or self-regulatory agencies and those involving actual or potential unauthorized tampering with, access to, or use of nonpublic information.

Under the Revised Regulations, covered entities must still report cybersecurity events, but reports are due "in no event later than ***72 hours from a determination that a Cybersecurity Event . . . occurred***." DFS limited the types of events that must be reported to only include those cybersecurity events where entities are required to provide notice to another governmental body, self-regulatory agency or supervisory body and events that have a reasonable likelihood of harming any material part of the normal operations of the covered entity. These changes will result in far fewer reports, and expose covered entities to far less time pressure, giving them time to consult with counsel before deciding whether to report a cybersecurity event.

Tailoring Requirements to a Risk Assessment

In response to criticism that the regulations were too prescriptive and inflexible to account for the varied information systems, operations and security environment of differing organizations, the Revised Regulations added a reference to a risk assessment and "to the extent applicable" in key provisions, qualifying the requirements. For example, the section setting forth the general requirements for the cybersecurity program

and the section listing the required elements of a cybersecurity policy both state that the sections' requirements shall be based on the covered entity's risk assessment. Other sections were also revised to refer to a risk assessment, including the requirements for penetration testing and vulnerability, audit trails, and obligations with respect to third party service providers.

Chief Information Security Officer

While covered entities are still required to name a Chief Information Security Officer (CISO), commentary by DFS made clear that covered entities do not have to hire a new "C" level executive to fill this position, and can designate an existing officer as CISO. Covered entities are further permitted to retain a third-party vendor to handle cybersecurity operations and serve as CISO so long as the covered entities themselves remain ultimately responsible for their own cybersecurity.

Third Party Service Providers

One of the most contentious provisions in the original draft of the DFS cybersecurity regulations was the apparent requirement that covered entities monitor the activities of third party service providers who are not themselves covered entities, requiring those service providers to come into compliance with many of the cybersecurity regulations simply by virtue of doing business with a covered entity.

As revised, covered entities are required to implement written policies and procedures governing their own behavior as it relates to sharing with third party service providers, including minimum security practices that must be met by third party providers in order for them to do business with the covered entity, standards for due diligence and periodic assessment of the risk posed by third parties to data security. To the extent applicable, such policies must include guidelines that address third party use of use multifactor identification, encryption of information in transit and at rest, and practices to notify the covered entity of a cybersecurity event that directly impacts the covered entity's information systems and nonpublic information. Guidelines must also cover the representations and warranties that third party service providers will provide to the covered entity regarding its cybersecurity policies although the Revised Regulations are less prescriptive about the specific elements of such representations and warranties.

Rolling Compliance Dates

Compliance with many of the basic provisions of the regulations is required within 180 days of the new effective date (i.e. August 28, 2017), however the requirement that covered entities comply with some of the more onerous provisions has been delayed.

Compliance with the following categories of regulations is not required until March 1, 2018:

- creating a written report from the CISO to the covered entity's board of directors or trustees;
- conducting penetration testing, vulnerability assessments and monitoring;
- engaging in risk assessment;
- using multi-factor authentication; and
- providing employee training.

Compliance with the following categories regulations is required by September 1, 2018:

- creating an audit trail used to detect and respond to cybersecurity events;
- ensuring application security and standards for in-house development of software and evaluation of third-party software;
- limiting scope of data retention;
- monitoring employees; and
- encryption of data at rest and in transit

Covered entities have a full two years to comply with requirements relating to third party service providers.

If you have any questions about compliance with the new DFS cybersecurity regulations or this information memorandum, please contact Curtis A. Johnson, Tracy E. Miller or the attorney in the firm with whom you are regularly in contact.

BOND SCHOENECK & KING ATTORNEYS

Commitment · Service · Value · Our Bond