THE
NATIONAL LAW REVIEW

New York Releases Revised Proposed Cybersecurity Regulations

Tuesday, January 10, 2017

The New York State Department of Financial Services ("DFS") has released a revised version of its proposed cybersecurity regulations, which set regulatory minimum standards for protecting the customer information and information systems of the financial services industry. The Revised Proposed Regulations will become effective on March 1, 2017.

According to its press release, DFS considered public comments from the first 45-day public comment period, which ended on November 14, and updated its proposed regulations in response. (For more on the original proposed regulations, see our article, Getting Prepared for the New York Department of Financial Services' Proposed Cybersecurity Regulations.) The Revised Proposed Regulations will be subject to an additional 30-day notice and comment period.

jackson lewis.

Article By Frank J. Fanshawe
Joseph J. Lazzarotti Rosemary McKenna
Damian J. Privitera Damon W. Silver
Jackson Lewis P.C. Publications

Communications, Media & Internet
New York

In addition to minor wording changes throughout, the Revised Proposed Regulations substantially revised the sections on exemptions, internal reports of the Chief Information Security Officer ("CISO"), third-party service providers, encryption, notices to the Superintendent, penetration testing, and the transitional periods.

Exemptions

The original proposal's exemptions have been expanded to exempt more entities from different aspects of the regulations' requirements.

The Revised Proposed Regulations revised the limited exemptions by substituting entities with fewer than 1,000 customers with entities with fewer than 10 employees (including independent contractors) and changed the requirements from which these entities would be exempt.

Covered Entities with fewer than 10 employees, with less than $5 million in gross annual revenue in each of the last three years, or with less than $10 million in year-end total assets (including assets of an Affiliate) are exempt from the following sections of the regulations:

- CISO,
- penetration testing and assessments,
- audit trail,
- application security,
- cybersecurity personnel and intelligence,
- multi-factor authentication,
- training and monitoring,
- encryption of Nonpublic Information, and
- incident response plan.

In addition, the Revised Proposed Regulations added limited exemptions for Covered Entities that do not "directly or indirectly operate, maintain, utilize or control any Information Systems," and that do not, and are not required to, "directly or indirectly control, own, access, generate, receive or possess Nonpublic Information." These entities are exempt from the following sections of the regulations:

- cybersecurity program,

- cybersecurity policy,
- CISO,
- penetration testing and vulnerability assessments,
- audit trail,
- access privileges,
- application security,
- cybersecurity personnel and intelligence,
- multi-factor authentication,
- training and monitoring,
- encryption of Nonpublic Information, and
- incident response plan.

Further, the Revised Proposed Regulations added unlimited exemptions for an employee, agent, representative, or designee of a Covered Entity who itself is a Covered Entity. In other words, those categories are wholly exempt from the regulations.

Chief Information Security Officer ("CISO")

The requirement for Covered Entities to designate a qualified CISO has not changed, nor has its core role. The reporting requirements of a CISO to its Covered Entity, however, have changed.

Under the Revised Proposed Regulations, reports are required at least annually, as opposed to bi-annually in the original proposal. The CISO's report also no longer needs to propose remedial steps for inadequacies identified in a Covered Entity's cybersecurity program.

In addition, the Revised Proposed Regulations removed language requiring the CISO's report be made available to the Superintendent upon request (although this appears to be a reshuffling as the new § 500.02(d) of the Revised Proposed Regulations requires that "all documentation and information relevant to [a] Covered Entity's cybersecurity program shall be made available to the superintendent upon request").

Under the Revised Proposed Regulations, the CISO need not be employed by the Covered Entity, but can be employed by an Affiliate of the Covered Entity or a Third Party Service Provider.

Third Party Service Provider

Third Party Service Provider is now defined in the Revised Proposed Regulations as:

> … a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity, and (iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity.

This is narrower than the original proposal, which stated that third party information security policy requirements applied to "third parties doing business" with a Covered Entity.

The Revised Proposed Regulations also did away with ascribing a time period on periodic reviews of Third Party Service Providers. They similarly removed Covered Entities' obligations to establish guidelines in their policies on preferred contractual provisions on providing identity protection services to customers materially affected by a Third Party Service Provider's negligence or willful misconduct, as well as guidelines on preferred contractual provisions relating to the right of a Covered Entity to perform cybersecurity audits of Third Party Service Providers. The rest of the guidelines on preferred contractual provisions remain, including the use of multi-factor authentication and access controls, notice to the Covered Entity for certain Cybersecurity Events, representations and warranties, and the use of encryption.

The Revised Proposed Regulations specifically referenced the section on encryption of Nonpublic Information, against which Covered Entities will assess Third Party Service Providers' policies and procedures.

Encryption

Section 500.15 on Encryption of Nonpublic Information is one of the sections that DFS announced in its State Register publication as being substantially revised. Under the Revised Proposed Regulations, that section requires Covered Entities to "implement controls, including encryption, to protect Nonpublic Information…." This demonstrates a more flexible approach by DFS, as the original proposal stated that "each Covered Entity shall encrypt all Nonpublic Information…." The section in the Revised Proposed Regulations went on to state that Covered Entities can use "effective alternative compensating controls reviewed and approved by the Covered Entity's CISO" in place of encryption when a Covered Entity determines encryption is not feasible. In those cases,

the CISO must nevertheless review the feasibility of encryption and the effectiveness of the compensating controls at least annually.

Although the original proposal also allowed for alternative compensating controls, it had deadlines after which encryption would be required. The Revised Proposed Regulations are more flexible both in what they require and when they require it according to the Transitional Periods section.

Notices

DFS also has demonstrated some flexibility in the Notices to Superintendent section of the Revised Proposed Regulations. While the requirement to notify the Superintendent within 72 hours of specific Cybersecurity Events is unchanged, one of the criteria of qualifying events has changed. Under the Revised Proposed Regulations, qualifying events include "Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity" — much narrower than the original language.

Penetration Testing

The Penetration Testing and Vulnerability Assessments section also is more flexible under the Revised Proposed Regulations. It provides for:

- annual penetration testing and bi-annual vulnerability assessments (reduced from quarterly), or
- continuous monitoring or systems that detect changes in Information Systems that may show vulnerabilities on an ongoing basis.

Transitional Periods

Substantial revisions were made to the Transitional Periods section. Covered Entities will have 180 days from the March 1, 2017, effective date to comply with these regulations. Again demonstrating some flexibility, the Revised Proposed Regulations give even longer transitional periods in certain parts. For example:

- 1 year – provisions on CISO reporting, penetration testing, vulnerability assessments and risk assessment provisions;
- 1.5 years – provisions on audit trail, data retention, and encryption/controls provisions; and
- 2 years – provisions on Third Party Service Provider Security Policy provisions.

Confidentiality

The Revised Proposed Regulations added a confidentiality section. It states that information Covered Entities provide under the regulations is subject to exemptions from certain disclosure laws.

Overall, these revisions appear to take into account some of the concerns voiced during the original public comment period, notably in the Notices to Superintendent section and internal CISO reporting requirements.

Source URL: https://www.natlawreview.com/article/new-york-releases-revised-proposed-cybersecurity-regulations