Harvard Law School Forum on
Corporate Governance and Financial Regulation

SUPPORTED BY:
pwc

NYDFS' Revision of Proposed Cybersecurity Regulation for Financial Services Companies

Posted by Joseph P. Vitale, Schulte Roth & Zabel LLP, on Tuesday, January 10, 2017

Editor's note: Joseph P. Vitale is a partner at Schulte Roth & Zabel LLP. This post is based on a Schulte Roth publication by Mr. Vitale, Michael L. Yaeger, and Noah N. Gillespie.

On Dec. 28, 2016, the New York State Department of Financial Services ("NYDFS") issued revisions to its proposed regulation that would impose new, rigorous cybersecurity requirements on banks, consumer lenders, money transmitters, insurance companies and certain other financial service providers (each a "Covered Entity") regulated by the NYDFS (the "Proposed Regulation"). The Proposed Regulation's effective date was delayed two months, from Jan. 1, 2017 to March 1, 2017. In the meantime, a new 30-day public comment period will run until Jan. 27, 2017.

Even as revised, the Proposed Regulation still exceeds what other regulators have suggested, much less required, and given the scope and footprint of many New York financial institutions, the impact of the Proposed Regulation will likely far exceed the state of New York. However, the NYDFS did make several significant modifications, mostly in response to industry concerns. This post focuses on those changes. For more information on the aspects of the Proposed Regulation that remain unchanged, please refer to our Sept. 15, 2016 post on the original version.

Key Modifications

Tailored to Risk

Many of those commenting on the original version of the Proposed Regulation complained that it was too much of a "one-size-fits-all" approach and advocated that it should be made more flexible and risk-based. In response, the NYDFS clarified that the specific obligations of a Covered Entity under a number of the Proposed Regulation's requirements would be based on the results of the entity's required periodic risk assessments (each a "Risk Assessment"). However, the NYDFS stressed that this flexibility is not intended to allow a Covered Entity to employ a "cost-benefit analysis" approach to cybersecurity.

As revised, the Proposed Regulation now makes clear that while all Covered Entities are required to maintain a cybersecurity program and a written cybersecurity policy, a particular Covered Entity's program and policy should be based on the findings of its own Risk Assessment. Similarly, it is now clear that:

- Penetration testing and vulnerability assessments are to be tailored towards the risks and vulnerabilities identified in the Risk Assessment, and such testing and assessments are not necessary if the entity otherwise maintains "effective continuous monitoring, or other systems to detect, on an ongoing basis, changes … that may create or indicate vulnerabilities";
- Audit trail systems are only required to the extent applicable and should be based on the Risk Assessment;
- Limitations on user access privileges to systems that provide access to "Nonpublic Information" should be based on the Risk Assessment;
- The required components of policies and procedures regarding the security of systems and information accessible to, or held by, third parties will depend on the applicable facts and the Risk Assessment;
- Whether multifactor authentication should be used to protect against unauthorized access will be determined based on the Risk Assessment; and
- The decision to encrypt Nonpublic Information or to employ alternative compensating controls should be determined based on the Risk Assessment.

Nonpublic Information

As discussed in our Sept. 15, 2016 post, the goal of the Proposed Regulation is to secure "Nonpublic Information" from misuse, disruption and unauthorized access, and the original version of the Proposed Regulation defined such information very broadly (e.g., far broader than what New York's existing data protection law defines as "private information"). Accordingly, many of those commenting on the Proposed Regulation complained that it was overbroad, unclear or unnecessarily inconsistent with other existing standards. In response, the NYDFS revised the definition, significantly decreasing its scope.

Most importantly, the original proposal defined Nonpublic Information to include any information (unless otherwise available to the general public from government records or widely distributed media):

that an individual provides to a Covered Entity in connection with the seeking or obtaining of any financial product or service from the Covered Entity, or is about an individual resulting from a transaction involving a financial product or service between a Covered Entity and an individual, or a Covered Entity otherwise obtains about an individual in connection with providing a financial product or service to that individual.

Now, however, that prong of the definition is limited to merely any information (again, unless otherwise available to the general public from government records or widely distributed media):

concerning an individual which because of name, number, personal mark or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number; (ii) driver's license number or non-driver identification card number; (iii) account number, credit or debit card number; (iv) any security code, access code or password that would permit access to an individual's financial account; or (v) biometric records.

Apart from the addition of "biometric records," the amended language is substantially the same as the definition of "private information" in New York's general data breach notification statute.

However, overall, the definition of Nonpublic Information is still broader than "private information" because the definition includes: (1) healthcare information; and (2) "[b]usiness related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity."

Encryption of Nonpublic Information

In a significant change, the Proposed Regulation now allows Covered Entities to either encrypt Nonpublic Information or use alternative compensating controls. As originally drafted, the Proposed Regulation would have permitted the use of compensating controls only for a limited transition period—one year to start encrypting data in transit and five years to commence encrypting data at rest. Now, the Proposed Regulation permits the use of alternative compensating controls indefinitely, provided such controls are reviewed and deemed effective by the Covered Entity's chief information security officer ("CISO"). Moreover, to the extent that encryption is not used, the CISO must review "the feasibility of encryption and effectiveness of the compensating controls" at least annually. The Proposed Regulation now also clarifies that information in transit refers to transit "over external networks."

Chief Information Security Officer

The Proposed Regulation requires that each Covered Entity designate a CISO to oversee and implement the Covered Entity's cybersecurity program and written cybersecurity policy. Some commentators expressed concerns regarding the feasibility or practicality of hiring or appointing an individual whose exclusive job would be to serve as CISO, under that specific title. In response, the NYDFS clarified the Proposed Regulation to provide that the person carrying out the duties of the CISO does not need to be exclusively dedicated to such activities and does not need a specific title. In fact, the revisions explicitly permit the CISO requirement to be satisfied by an employee of an affiliate or third-party service provider (subject to certain requirements).

Audit Trail

As originally drafted, the Proposed Regulation required Covered Entities to maintain sufficiently detailed records to be able to, among other things:

- Completely reconstruct all financial transactions and accounting necessary to enable the Covered Entity to detect and respond to attempted and actual attacks; and
- Track and maintain data logging of all authorized user access to critical systems, including all physical access to hardware, that allows for event reconstruction.

Some commentators argued that this extensive audit trail requirement was excessive and would lead to the retention of too much information. In response, the NYDFS significantly reduced the requirement by adding multiple materiality qualifiers and, as noted above, tying it to the Covered Entity's Risk Assessment. Moreover, the applicable record retention period was shortened from six years to five, consistent with the retention requirements of other aspects of the Proposed Regulation.

Data Destruction

As originally drafted, the Proposed Regulation required Covered Entities to securely dispose of Nonpublic Information when it was no longer necessary for the provision of the products or services to which such information relates, except when maintenance of the information was required by law. A number of commentators asserted that this exception was too narrow, as it did not take into account other legitimate business purposes for which data may ordinarily be retained. In response, the NYDFS modified the Proposed Regulation so that the permissibility of data retention is not tied solely to the specific product or service at issue. Instead, data may be retained whenever necessary "for business operations or for other legitimate business purposes." As revised, the data destruction requirement now also includes a feasibility exception. Secure disposal need not occur "where targeted disposal is not reasonably feasible due to the manner in which the information is maintained."

Third Party Service Providers

Prior to the current revisions, the Proposed Regulation required Covered Entities to: (a) implement written policies and procedures to ensure the security of systems and Nonpublic Information accessible to, or held by, third parties with which they do business ("Third Party Service Providers"); and (b) negotiate for certain "preferred provisions" to be included in contracts with Third Party Service Providers. While the Proposed Regulation still retains the requirement to maintain written policies and procedures, it now makes clear that they should be based on the Covered Entity's Risk Assessment. For example, whereas previously the Proposed Regulation required a Covered Entity to conduct an annual assessment of each of its Third Party Service Providers and the adequacy of their cybersecurity practices, now such assessments are only required based on the risk a particular Third Party Service Provider presents.

Moreover, in response to the concern expressed by numerous Covered Entities that they would not always have sufficient leverage to force Third Party Service Providers to accept the preferred provisions, the NYDFS modified the requirement to permit the use of "relevant guidelines for due diligence" instead of actual contractual provisions. Further, the NYDFS eliminated a preferred provision that seemed to suggest that Covered Entities were required to conduct cybersecurity audits of all Third Party Service Providers. Significantly, the NYDFS also amended a preferred provision that would have previously required Third Party Service Providers to warrant that no viruses, trap doors, time bombs and other security threats existed. As revised, the Proposed Regulation simply advises Covered Entities to obtain "representations and warranties addressing the Third Party Service Provider's cybersecurity policies and procedures that relate to the security" of the Covered Entity.

Cybersecurity Event Reporting

Prior to the revisions, the Proposed Rule required that all "Cybersecurity Events" that have "a reasonable likelihood of materially affecting the normal operation of the Covered Entity *or that affects Nonpublic Information*" (including any "actual *or potential* unauthorized tampering with, or access to or use of, Nonpublic Information)" be reported to the superintendent ("Superintendent") of the NYDFS within 72 hours. Many commentators understandably complained that the requirement was overly broad and, therefore, would result in many reports that were of little value. In addition, many commentators asserted that the 72-hour time frame was too short and would not afford a Covered Entity enough time to gather necessary information prior to reporting.

The revised Proposed Regulation still raises Covered Entities' notification obligations beyond what existing law requires, but it reduces their obligations as compared to the original draft. The requirement that the superintendent be notified "in no event later than 72 hours" remains, but that time period now begins only once the Covered Entity determines that a Cybersecurity Event with "a reasonable likelihood of *materially harming any material part* of the normal operations of the Covered Entity" occurred (unless notice is otherwise required to a government body, self-regulatory agency or other supervisory body, in which case the Covered Entity must notify the NYDFS within 72 hours of the determination that the Cybersecurity Event occurred).

New Exemptions

The NYDFS added several new exemptions or partial exemption in the Proposed Regulation. If a Covered Entity has: (1) fewer than 10 employees or independent contractors; (2) less than $5 million in gross annual revenue each of the past three fiscal years; or (3) less than $10 million in it and its affiliates' GAAP year-end total assets, it is exempt from the CISO, penetration testing, audit trail, application development, cybersecurity personnel, multifactor identification, training, encryption and incident response plan obligations of the Proposed Regulation. Moreover, a Covered Entity need not adopt its own program if it is an "employee, agent, representative, or designee" of a Covered Entity and is covered under that Covered Entity's program.

Finally, a Covered Entity that does not directly or indirectly maintain "Information Systems" or have Nonpublic Information is exempt from most requirements of the Proposed Regulation. It must still conduct a risk assessment, develop a written Third Party Service Provider Security Policy, abide by the data retention requirement and provide notice to the Superintendent under the Proposed Regulation.

Any Covered Entity that wishes to benefit from an exemption must file a "Notice of Exemption" with the Superintendent.

Timeline for Compliance

While the NYDFS did not change the Proposed Regulation's 180-day conformance period, it did add three exceptions to that deadline.

- First, Covered Entities are now given until March 1, 2018 to comply with:
    - The reporting obligations of the CISO;
    - The requirement to conduct periodic risk assessments;
    - Any requirement to conduct annual penetration testing and bi-annual vulnerability assessments;
    - Any requirement to implement multifactor authentication or risk-based authentication; and
    - The obligation to provide regular up-to-date cybersecurity awareness training for all
- Second, Covered Entities are now given until Sept. 1, 2018 to comply with:
    - Any requirement to maintain audit trail systems;
    - The requirements to implement:
        - Written procedures, guidelines and standards on application security;

        - Policies and procedures for the secure disposal of Nonpublic Information; and
        - Policies, procedures and controls to monitor authorized users; and
    - Any requirement to encrypt Nonpublic
- Finally, Covered Entities are now given until March 1, 2019 to comply with the requirement to implement written policies and procedures regarding the security of systems and information accessible to, or held by, Third-Party Service providers.