Getting Prepared for the New York Department of Financial Services' Proposed Cybersecurity Regulations

By Joseph J. Lazzarotti, Jason C. Gavejian and Damon W. Silver

November 7, 2016

Taking aim at the growing threat posed by cyber-attacks to the financial services industry, the New York State Department of Financial Services ("DFS") has proposed a first-of-its kind, far-reaching, rigorous cybersecurity framework that could become the national standard.

DFS is accepting comments on these proposed rules ("Proposed Regulations"), which are expected to become effective January 1, 2017. The public comment period ends November 14.

Many robust cybersecurity programs may not be sufficient to meet these new rules as proposed. Accordingly, organizations that would be subject to these regulations, even those with rigorous cybersecurity programs, need plans for compliance. The FAQs below will help organizations develop such plans.

Who would be subject to the Proposed Regulations?

As is the case with many data privacy and security regulations, some organizations will be directly subject to the regulations, while others will be affected indirectly. The Proposed Regulations would apply directly to entities meeting the definition of "Covered Entity," which includes:

> *any [p]erson operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the [New York] banking law, the insurance law or the financial services law.*

Entities regulated by DFS include:

- Banks and trust companies, including state-licensed banks, savings banks, savings-and-loan associations, and private bankers;
- Licensed Consumer Lenders;
- Check Cashers;
- Money Transmitters;
- Insurance Companies;
- Trust Companies;
- Safe Deposit Companies;
- Credit Unions;
- Mortgage and other licensed lenders, brokers, originators, and servicers; and
- Branch, agency, and representative offices of non-U.S. banks.

Third-party service providers to these regulated entities would be indirectly affected by the Proposed Regulations because regulated entities must maintain written policies and procedures designed to ensure the security of information systems and nonpublic information accessible to, or held by, their service providers.

A regulated entity's written policies and procedures must:

1. identify and assess the data security practices of the third-parties that access or hold its nonpublic information;
2. require that such third-parties meet certain minimum requirements for cybersecurity practices; and
3. include periodic (at least annual) assessments of third parties and their cybersecurity practices.

The policies and procedures also would require regulated entities to bind these service providers to certain requirements by contract.

Meet the Authors

Joseph J. Lazzarotti

Principal
Berkeley Heights 908-795-5205
Email

Jason C. Gavejian

Principal
Berkeley Heights 908-795-5139
Email

Damon W. Silver

Principal
New York Metro
New York City 212-545-4063
Email

Practices

Privacy, Data and Cybersecurity

Industries

Financial Services

Is there an exception for smaller entities?

Yes, but it is limited. The exception applies to regulated entities that had:

1. fewer than 1,000 customers in each of the last three calendar years,
2. less than $5,000,000 in gross annual revenue in each of the last three fiscal years, and
3. less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all affiliates.

Regulated entities that meet these requirements would be exempt from certain obligations in the regulations. These include, for example, the requirement to appoint a chief information security officer, perform penetration testing, and maintain audit trails. However, these entities still would need to establish cybersecurity programs and policies, maintain record retention and destruction programs, conduct risk assessments, and have policies and procedures for ensuring the security of Nonpublic Information maintained by third-party service providers. Of course, these smaller regulated entities also may be bound by contractual obligations to do much more, even if the regulations would not require it.

The exemption may be short lived. If, at the end of its most recent fiscal year, an exempted entity ceases to meet the above requirements for exemption, it will have only 180 days from such fiscal year-end to become compliant with all requirements in the regulations.

What information and information systems would have to be protected?

The Proposed Regulations apply to "Nonpublic Information." This term is not limited, as are many other data privacy and security standards, to individually identifiable personal information. Nonpublic Information is defined much more broadly. It includes all electronic information that:

- is business-related information of a regulated entity that, if tampered with, or if there were an unauthorized disclosure, access, or use of, would cause a material adverse impact to the business, operations, or security of the entity;
- is provided by an individual to a regulated entity in connection with the seeking or obtaining of any financial product or service from the regulated entity, or is about an individual resulting from a transaction involving a financial product or service between a regulated entity and an individual, or a regulated entity otherwise obtains about an individual in connection with providing a financial product or service to that individual;
- is created by, derived or obtained from a health care provider or an individual and that relates to the past, present, or future physical, mental, or behavioral health or condition of any individual or a member of the individual's family or household, or from the provision of health care to any individual, or from payment for the provision of health care to any individual (information relating to an individual's age or gender is excluded from this category);
- can be used to distinguish or trace an individual's identity, including, but not limited to, an individual's name, social security number, date, and place of birth, mother's maiden name, biometric records, any information that is linked or linkable to an individual, including, but not limited to, medical, educational, financial, occupational, or employment information, information about an individual used for marketing purposes, or any password or other authentication factor.

Clearly, the Proposed Regulations cast a wide net around electronic information that must be protected. Likewise, the Proposed Regulations define "Information Systems" broadly as:

> *a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system, such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.*

This definition would cover just about any system with electronic information. It would include servers, desktops, laptops, smartphones, and other devices, such as thumb drives. It also could include copier hard drives, telephone exchange systems, video/audio monitoring systems, heating and cooling systems, security systems, and GPS monitoring systems. Systems that facilitate remote work arrangements also could be covered. Clearly, regulated entities and their service providers would need to be sure they have inventoried their information systems to be sure they are all covered.

Will the Proposed Regulations require us to hire additional cybersecurity personnel?

Maybe. The Proposed Regulations require a regulated entity to designate a qualified Chief Information Security Officer ("CISO") who will be responsible for overseeing and implementing the entity's cybersecurity program and enforcing its cybersecurity policy. Additionally, a regulated entity must employ cybersecurity personnel sufficient to manage its cybersecurity risks and to perform core cybersecurity functions, including: (a) identifying internal and external cyber risks; (b) using defensive infrastructure and implementing policies and procedures to protect the entity's Information Systems, and the Nonpublic Information stored on those systems, from unauthorized access, use or other malicious acts; (c) detecting Cybersecurity Events; (d) responding to identified or detected Cybersecurity Events to mitigate any negative effects; and (e) recovering from Cybersecurity Events and restoring normal operations and services.

What are some basic requirements for cybersecurity under the Proposed Regulations?

The Proposed Regulations would establish a number of requirements for regulated entities to secure Nonpublic Information. Many regulated entities may have already satisfied certain of these requirements. However, there likely will be a number of updates they will need to make if the Proposed Regulations are finalized in their current form.

Regulated entities with not-so-robust cybersecurity programs will have their work cut out for them. Below is a brief discussion of some of these requirements:

- **Establish a Cybersecurity Program.** A cybersecurity program must be designed to ensure the confidentiality, integrity and availability of the entity's information systems. This program must identify internal and external cyber risks; use a defensive infrastructure and policies and procedures to protect the entity's Information Systems and Nonpublic Information; detect, respond to, mitigate, and recover from cybersecurity events; and satisfy regulatory reporting obligations.
- **Implement and Maintain a Cybersecurity Policy.** Regulated entities need to implement and maintain written cybersecurity policies and procedures to protect their Information Systems and the Nonpublic Information stored on those systems. These include the policies and procedures many regulated entities are already familiar with – *e.g.*, data governance and classification, access controls and identity management, systems operations, and availability concerns, systems and network security, systems and network monitoring, customer data privacy, vendor and third-party service provider management, and incident response.
- **Appoint a Chief Information Security Officer.** Regulated entities must designate a qualified CISO responsible for overseeing and implementing their cybersecurity programs and enforcing their cybersecurity policies. If a regulated entity utilizes a third-party service provider to meet this requirement, it must (1) retain responsibility for compliance with the requirement, (2) designate a senior employee to oversee the actions taken by the third-party service provider, and (3) ensure that the third-party service provider maintains a cybersecurity program that meets the requirement.
- **Reporting to Board and Superintendent.** At least bi-annually, a regulated entity's CISO must present a report to the entity's board of directors or equivalent governing body; if no such governing body exits, the entity's CISO must present the report to the senior officer responsible for the entity's cybersecurity program. The report must: (1) assess the confidentiality, integrity and availability of the entity's Information Systems; (2) detail exceptions to the entity's cybersecurity policies and procedures; (3) identify cyber risks to the entity; (4) assess the effectiveness of the entity's cybersecurity program; (5) propose steps to remediate any inadequacies identified therein; and (6) include a summary of all material cybersecurity events that affected the entity during the time period addressed by the report. Upon request, the entity must make the report available to the Superintendent of the DFS.
- **Access Privileges.** Regulated entities, as part of their cybersecurity programs, must limit access privileges to Information Systems containing Nonpublic Information solely to those individuals who require such access in order to perform their job responsibilities. A regulated entity must periodically review its access privileges to ensure compliance.
- **Risk Assessment.** At least once a year, a regulated entity must conduct a risk assessment of its Information Systems. This assessment must adhere to the entity's written policies and procedures and must itself be documented in writing. The policies and procedures in accordance with which the entity conducts its risk assessment must include, at minimum: (1) criteria for the evaluation and categorization of identified risks; (2) criteria for the assessment of the confidentiality, integrity, and availability of the entity's Information Systems, including the adequacy of existing controls in the context of identified risks; and (3) requirements for documentation describing how identified risks will be mitigated or accepted based on the risk assessment, justifying such decisions in light of the risk assessment findings, and assigning accountability for the identified risks.
- **Third-Party Information Security Policy.** Regulated entities will have to develop and implement written policies and procedures to address the security risks of allowing third-party service providers to access their Information Systems and/or hold their Nonpublic Information. At a minimum, these policies will have to address: (1) identifying and assessing the risks posed by third parties accessing the entity's Information Systems or Nonpublic Information; (2) the minimum cybersecurity practices regulated entities will require a third party to meet before they do business with it; (3) the due diligence a regulated entity uses to evaluate whether a third party's cybersecurity practices are adequate; and (4) at least an annual periodic assessment of the third party and the adequacy of its cybersecurity practices. As discussed in detail in the next section, a regulated entity's policies and procedures also must provide for the inclusion of certain provisions in contracts with third-party service providers.
- **Multi-Factor Authentication.** Regulated entities must require Multi-Factor Authentication for (1) individuals who, from an external network, access their internal systems or data, (2) privileged access to their database servers that allow access to Nonpublic Information, and (3) individuals who access web applications that capture, display, or interface with Nonpublic Information. Regulated entities also must require Risk-Based Authentication for accessing web applications that capture, display, or interface with Nonpublic Information.
- **Training and Monitoring.** Regulated entities must provide regular cybersecurity awareness training sessions that are updated based on the entity's annual assessment of risks. They also must require all personnel to attend these sessions. Our outline provides useful guidance to entities on how best to implement or update their training policies. As part of their cybersecurity programs, regulated entities

also must implement risk-based policies, procedures and controls that allow them to monitor the activity of Authorized Users as well as detect unauthorized access, use, or tampering with Nonpublic Information by those Authorized Users.

- **Encryption.** Regulated entities are required to encrypt all Nonpublic Information that they hold or transmit, both in transit and at rest. If encryption in transit is infeasible, regulated entities may choose an appropriate alternative that is approved by their CISO, but only for the first year after the final regulations become effective. Likewise, if encryption at rest is infeasible, regulated entities can use an appropriate alternative approved by their CISO for up to five years after the final regulations take effect.
- **Incident Response.** Last, regulated entities must develop a written incident response plan to direct their response to, and recovery from, any Cybersecurity Event affecting the confidentiality, integrity or availability of their Information Systems or the continuing functionality of their business. At a minimum, this plan must address the following areas: (1) internal processes for responding; (2) goals of the response plan; (3) defining clear roles, responsibility, and levels of decision-making authority; (4) external and internal communications and information sharing; (5) remediation of identified weaknesses in Information Systems/association controls; (6) documentation and reporting of the Cybersecurity Events and incident response activities; and (7) evaluation and revision of the response plan following a Cybersecurity Event. On top of the requirements imposed by the Proposed Regulations, a regulated entity's incident response plan also should include any breach reporting that may be required by law or by contract with upstream or downstream business partners.

What can third-party service providers expect if they want to continue doing business with covered entities?

In a structure similar to what is in place under the Health Insurance Portability and Accountability Act's privacy and security regulations for "business associates" of covered entities, the Proposed Regulations require regulated entities to include certain provisions in service contracts with service providers. These provisions include:

- the use of Multi-Factor Authentication to limit access to sensitive systems and Nonpublic Information;
- the use of encryption to protect Nonpublic Information in transit and at rest;
- prompt notice of a cybersecurity event affecting the service provider;
- the obligation to provide identity protection services for any customers materially impacted by a cybersecurity event caused by the service provider;
- representations and warranties that the service provider's service or product is free of viruses, trap doors, time bombs, and other mechanisms that would impair the security of the regulated entity's Information Systems or Nonpublic Information; and
- the right of the regulated entity or its agents to perform cybersecurity audits of the service provider.

Accordingly, third-party service providers will need to re-evaluate their data privacy and security programs to ensure they can agree to these terms. In fact, contract negotiations will become significantly more important for both regulated entities and service providers, particularly for those regulated entities that craft contract requirements that are more stringent than those under the Proposed Regulations. Indemnification, limitation of liability, cyberinsurance, and other provisions, therefore, also will be critical.

If the Proposed Regulations cause these requirements to be pushed down to third-party service providers, those service providers likely will need and want to pass similar requirements on to their agents and subcontractors.

What should we be doing now?

The regulations are not finalized yet and the public comment period ends November 14. Still, there are steps you can take now.

- **Review the Proposed Regulations and comment where appropriate.** If you are concerned about some of the requirements in the Proposed Regulations and would like DFS to consider changes, you should submit your comments to the agency before November 14.
- **Tighten up your current cybersecurity program.** Any regulated entity should already have some form of a cybersecurity program in place. Your organization should review its key components with the responsible parties to assess your compliance with existing legal and contractual obligations. Start with making sure policies and procedures are in writing, conducting and documenting training, performing penetration testing, reviewing existing contracts with third-party service providers, and testing incident response plans.
- **Monitor the progress of the Proposed Regulations.** There may not be much time to get compliant with the rules if they are finalized. Accordingly, consider assembling an internal team that will be ready to efficiently tackle this added compliance challenge.

constitute legal advice nor does it create a client-lawyer relationship between Jackson Lewis and any recipient. Recipients should consult with counsel before taking any actions based on the information contained within this material. This material may be considered attorney advertising in some jurisdictions. Prior results do not guarantee a similar outcome.

Focused on labor and employment law since 1958, Jackson Lewis P.C.'s 950+ attorneys located in major cities nationwide consistently identify and respond to new ways workplace law intersects business. We help employers develop proactive strategies, strong policies and business-oriented solutions to cultivate high-functioning workforces that are engaged, stable and diverse, and share our clients' goals to emphasize inclusivity and respect for the contribution of every employee. For more information, visit https://www.jacksonlewis.com.

*The National Operations Center serves as the firm's central administration hub and houses the firm's Facilities, Finance, Human Resources and Technology departments.