ALERTS

NYDFS Proposes Detailed and Sweeping Cybersecurity Regulation for Financial Services Companies

September 15, 2016

On Sept. 13, 2016, the New York State Department of Financial Services ("NYDFS") issued a 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").[1] Given New York's importance in the financial services industry, not only would the effect of the Proposed Regulation be felt immediately across the country, other regulators may follow New York's example.

In some respects, the Proposed Regulation is consistent with the principles set forth in documents that other regulators have issued, such as the Information Technology Examination Handbook released by the Federal Financial Institutions Examination Council (FFIEC) and the Cybersecurity Framework released by the National Institute of Standards and Technology (NIST). This is true of the Proposed Regulation's basic requirement that Covered Entities create and implement a written policy — overseen by a qualified Chief Information Security Officer ("CISO") — to protect against, detect, document and respond to attempts to access, disrupt, or misuse Covered Entities' consumer information or technology systems.

But the NYDFS regulations also contain some specific commands that go significantly beyond what other regulators have suggested, much less required. Most notably, the Proposed Regulation has several directives

tied to "Nonpublic Information," and it defines that term broadly, including any information that would be considered nonpublic personal information under the Gramm-Leach-Bliley Act's privacy rule ("GLBA Privacy Rule"). As a result, it captures far more data than what New York's existing data protection law defines as "personal information."[2] The requirement that "Nonpublic Information" be encrypted at rest (and not just in transit) may therefore be a significant burden on Covered Entities, as may the requirement that the Superintendent be notified of any "Cybersecurity Event" that "affects" Nonpublic Information. Further, senior management must certify annually that the Covered Entity is in compliance.

The Proposed Regulation is open for public comment for the next 45 days and is slated to take effect Jan. 1, 2017.[3] The NYDFS states that the Proposed Regulation is intended to impose minimum standards on the industry while allowing sufficient flexibility for Covered Entities to adapt to the threats they face and the technologies available to secure their information and systems.[4] The NYDFS notes that it based the Proposed Regulation on extensive surveys of and discussions with Covered Entities; yet many of these surveys and the reports the NYDFS generated are already one or two years old.[5]

Who and What the Proposed Regulation Covers

The Proposed Regulation defines a "Covered Entity" as "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."[6] Recognizing that certain smaller entities may have difficulty reaching the NYDFS minimum standard, the Proposed Regulation exempts them from some but not all of the Proposed Regulation's requirements.[7] Nonetheless, the Proposed Regulation may exert influence beyond Covered Entities insofar as it affects the third-party vendors of those entities.

The goal of the Proposed Regulation is to secure "Nonpublic Information" from misuse, disruption and unauthorized access, and as noted above, such information is defined broadly.[8] It includes not only competitively sensitive information and intellectual property, but also numerous categories of information that a Covered Entity receives from or about consumers, including information considered nonpublic personal

information under the GLBA Privacy Rule.[9] Accordingly, the Proposed Regulation's definition of Nonpublic Information is far broader than what New York's existing data protection law defines as "personal information."[10]

Formalizing a Cybersecurity Program

Under the Proposed Regulation, Covered Entities must have a written cybersecurity policy that outlines every aspect of its cybersecurity program and explicitly addresses how the Covered Entity complies with each of the Proposed Regulation's requirements.[11] At a minimum, the written policy must address:

- Information security;
- Data governance and classification;
- Access controls and identity management;
- Business continuity and disaster recovery planning and resources;
- Capacity and performance planning;
- Systems operations and availability concerns;
- Systems and network security;
- Systems and network monitoring;
- Systems and application development and quality assurance;
- Physical security and environmental controls;
- Customer data privacy;
- Vendor and third-party service provider management;
- Risk assessment; and
- Incident response.[12]

In addition to outlining all the steps the Covered Entity is taking in these areas, the Covered Entity must also include an incident response plan that lays out how it will respond to any attempted or actual access, disruption or misuse of its systems and information. The incident

response plan must also identify and allocate the precise roles and responsibilities of the individuals who will carry out the actions it specifies.[13]

To helm those efforts, the Covered Entity must designate a "qualified" CISO who will oversee and implement the Covered Entity's written policy and cybersecurity program.[14] In addition, the Covered Entity must also employ sufficient cybersecurity personnel to carry out its program, who must undergo sufficient training to stay abreast of cybersecurity threats and best practices.[15] Further, the Covered Entity must provide *all staff* with "regular" cybersecurity training that makes them aware of the threats and best practices specific to the Covered Entity's risk assessment.

The CISO must complete that risk assessment (including the vulnerabilities posed by third parties' access to the Covered Entity's information and systems), penetration testing and a comprehensive review and update of the cybersecurity policy at least once a year, and report on the Covered Entity's efforts and any material attempts or attacks to the board and senior officers at least twice a year.[16]

Limiting Access to Information and Systems

In a major change, under the Proposed Regulation, Covered Entities will be required to encrypt their Nonpublic Information — by January 2018 for Nonpublic Information in transit and by January 2022 for Nonpublic Information at rest.[17] Covered Entities must also require multifactor authentication for remote access to its systems or for privileged access to the servers that contain Nonpublic Information. Web applications that capture, display or interface with Nonpublic Information must require risk-based authentication and must support multifactor authentication.[18] Because of the breadth of what the Proposed Regulation considers Nonpublic Information, implementation of those security measures may be costly for certain Covered Entities, as much of the electronic contact a Covered Entity has with its clients or customers will have to be conducted over secure platforms.

The Proposed Regulation requires Covered Entities to consider which employees need access to which information and systems, and to curtail access to the systems and information accordingly.[19] The Proposed Regulation also makes Covered Entities responsible for the cybersecurity

practices of the third parties who hold or can access Nonpublic Information. Covered Entities will be required to conduct due diligence on their third-party providers' policies and procedures and assess the risks that stem from using those third parties. The Proposed Regulation suggests that Covered Entities include in their written policy the preferred provisions the Covered Entity will include in its vendor contracts, for example, to have the right to audit the third party's cybersecurity capabilities.[20] Even with favorable contract terms, however, that level of responsibility over third parties will be challenging for many Covered Entities given that the third party's cybersecurity is in someone else's hands and the Covered Entity will in many cases not have full and direct access to examine or control the cybersecurity program the third party adopts.

Reporting

When something goes wrong, the Covered Entity must report it to the Superintendent. Specifically, any attempt or attack "that has a reasonable likelihood of materially affecting the normal operation of the Covered Entity or that affects Nonpublic Information" must be reported to the Superintendent within 72 hours after the Covered Entity becomes aware of the event. Any notice the Covered Entity provides to any government or self-regulatory agency must also be given to the Superintendent.[21] As a result, a Covered Entity may have to report a data breach or attempted breach to the Superintendent before the Covered Entity has established a full understanding of the nature and extent of the incident.

Recordkeeping on the One Hand; Timely Destruction on the Other

Covered Entities must maintain sufficiently detailed records to be able to reconstruct who accessed its digital and physical systems when, and to harness that information to successfully detect attempted and actual attacks. Covered Entities must also ensure that the logs that record such access are protected against tampering or alteration. Covered Entities must maintain those "audit trail" records for at least six years.[22]

Nonetheless, Covered Entities are to evaluate and destroy Nonpublic Information that is no longer necessary for the provision of the product or services for which such information was originally provided or obtained, unless some other law (such as, at a minimum, the Proposed Regulation)

requires that Nonpublic Information to be maintained.[23] It is often best practice to limit the personal information a business has about its customers to only what is necessary currently for legitimate business purposes, including so that any data breach that does occur will be less harmful to the customers and the business. However, Covered Entities are subject to extensive recordkeeping requirements from many sources and, in many cases, are under the threat of foreseeable litigation, for which they must preserve the materials they may need to exchange in discovery on pain of sanctions for spoliation.

Annual Certification

The Proposed Regulation provides that beginning Jan. 15, 2018, Covered Entities must have the chair of the board or another senior officer (if the Covered Entity has no board) certify in writing to the Superintendent that the Covered Entity is in full compliance with the Proposed Regulation.[24] The Proposed Regulation includes the text of that certification in an appendix. In addition to certifying that the signatory has reviewed all "necessary" material and that the Covered Entity is in compliance, the Covered Entity must provide a report on all remedial efforts planned or underway and all the attempts or attacks that occurred in the prior year that were required to be reported to the Superintendent. The records that support the certification must be maintained for at least five years and made available to the Superintendent upon request.[25] The fact that certification backup materials need only be maintained for five years, but the audit trail materials must be maintained for six years, suggests that the Superintendent may also rely on the audit trail to reach further back in time to find further errors when it enforces the Proposed Regulation.

In fact, the individuals who sign that certification may be exposed to personal liability if the Covered Entity is ultimately found to be noncompliant. The Superintendent may enforce the Proposed Regulation pursuant to her "authority under any applicable laws." Such laws include the provisions of the New York Banking Law, Insurance Law and Finance Law that impose civil and even criminal penalties for false disclosures made with an intent to deceive a regulator.[26]

Conclusion

While the Proposed Regulation is not yet law and remains open for public comment for the next 45 days, the NYDFS and the State of New York

have indicated that securing New York's financial services firms and consumers from the increasing threats posed by "nation-states, terrorist organizations, and independent criminal actors" is a top priority. In order to meet the Jan. 1, 2017 effective date, Covered Entities should now begin assessing their cybersecurity risks, policies and procedures to develop or enhance their cybersecurity program and to begin documenting and tracking their compliance efforts.

Authored by Joseph P. Vitale, Michael L. Yaeger and Noah N. Gillespie.

If you have any questions concerning this *Alert*, please contact your attorney at Schulte Roth & Zabel or one of the authors.

---

[1] Cybersecurity Requirements for Financial Services Companies ("Proposed Regulation") (Sept. 13, 2016) (to be codified at 23 NYCRR Part 500), *available at* http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.

[2] *See* N.Y. Gen Bus. L. § 899-aa2.

[3] Persons wishing to submit a public comment on the Proposed Regulation may write to comments@dfs.ny.gov or to Maria T. Vullo, Superintendent of Financial Services, New York Department of Financial Services, One State Street, New York, NY 1004-1511.

[4] Proposed Regulation at 2.

[5] *See* Press Release, Governor Cuomo Announces Proposal of First-in-the-Nation Cybersecurity Regulation to Protect Consumers and Financial Institutions (Sept. 13, 2016), *available at* http://www.dfs.ny.gov/about/press/pr1609131.htm; DFS Reports and Publications (last visited Sept. 14, 2016), *available at* http://www.dfs.ny.gov/reportpub/dfs_reportpub.htm#misc.

[6] Proposed Regulation § 500.01(c).

[7] Specifically, otherwise Covered Entities that have: (1) fewer than 1,000 customers in each of the last three calendar years; (2) less than $5 million in gross annual revenue in the last three fiscal years; *and* (3) less than $10 million in total GAAP year-end assets (including the assets of all their affiliates) enjoy an exemption from designating a CISO, hiring sufficient cybersecurity personnel, training, encryption and multifactor authentication, conducting penetration testing, maintaining an audit trail,

and verifying application security. Proposed Regulation § 500.18. In contrast, all Covered Entities (regardless of size) must undertake a cybersecurity program, draft a written cybersecurity policy, restrict access privileges, conduct a risk assessment, report material attacks to the NYDFS Superintendent (the "Superintendent") within 72 hours, destroy old information, and assess the vulnerabilities of the third parties with access to their information — and are subject to enforcement by the Superintendent for any failure to do so. *Id.*

[8] Proposed Regulation § 500.01(g).

[9] Nonpublic Information includes "[a]ny information that an individual provides to a Covered Entity in connection with seeking or obtaining any financial product or service from the Covered Entity" and "[a]ny information that can be used to distinguish or trace an individual's identity, including but not limited to … any information that is linked or linkable to an individual." By contrast, N.Y. Gen Bus. L. § 899-aa2 defines "personal information" to include: (1) a social security number; (2) a driver's license or non-driver ID number; or (3) an account number, credit card or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account. Personal information does not include publicly available info that is lawfully made available to the general public from federal, state, or local government records.

[10] *Id.* However, the Proposed Regulation does not require Covered Entities to secure information that is generally available to the public or which an individual can direct not to be made available to the public but has not so directed. *Id.* § 500.01(j).

[11] *See id.* § 500.02-.03.

[12] *Id.* § 500.03(a).

[13] *Id.* § 500.16.

[14] *Id.* § 500.04.

[15] *Id.* § 500.10.

[16] *Id.* § 500.03-.05, .08-.09, .11.

[17] *Id.* § 500.15.

[18] *Id.* § 500.12. "Multifactor authentication means authentication through verification of at least two of the following types of authentication factors: (1) Knowledge factors, such as a password; or (2) Possession factors, such as a token or text message on a mobile phone; or (3) Inherence factors, such as a biometric characteristic." *Id.* § 500.01(f). "Risk-based authentication means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions." *Id.* § 500.01(k).

[19] *Id.* § 500.07.

[20] *Id.* § 500.11.

[21] *Id.* § 500.17(a).

[22] *Id.* § 500.06.

[23] *Id.* § 500.13.

[24] *Id.* § 500.17(b).

[25] *Id.* § 500.17(b).

[26] *See, e.g.*, N.Y. Bank. Law § 672; *see also* "NYDFS Issues AML/Sanctions Programs and Annual Certification Requirements for Banks, Money Transmitters and Check Cashers," *SRZ Client Alert*, July 6, 2016 (discussing a similar provision in a new, final NYDFS anti-money laundering regulation).

Practices

BANK REGULATORY

CYBERSECURITY AND DATA PRIVACY

INSURANCE

Attachments

Download Alert