Client Update

New York's Proposed Cyber Regulations: Implications and Challenges

NEW YORK
Eric R. Dinallo
edinallo@debevoise.com

Jeremy Feigelson
jfeigelson@debevoise.com

Gregory J. Lyons
gjlyons@debevoise.com

James J. Pastore
jjpastore@debevoise.com

WASHINGTON, D.C.
Luke Dembosky
ldembosky@debevoise.com

Naeha Prakash
nprakash@debevoise.com

On September 13, 2016, the New York Department of Financial Services ("DFS" or the "Department") issued proposed regulations (the "Proposed Regulations") designed to guard against the onslaught of cyber-attacks faced by banks, insurance companies and other financial services providers.[1] Billed by Governor Andrew Cuomo as a means to assure that regulated banks and insurance companies "protect consumers and ensure that [their] systems are sufficiently constructed to prevent cyber-attacks to the fullest extent possible," the Proposed Regulations provide a baseline with respect to companies' cybersecurity practices regardless of the size, nature or complexity of the business.[2] Though they mirror expectations and guidance provided by the federal banking agencies and the Federal Financial Institutions Examination Council ("FFIEC"), they go well beyond any other existing state-level requirements and set an example for how other federal and state regulators may implement cybersecurity regulation.

The Proposed Regulations have a comment period of 45 days—ending on October 28, 2016—and are the culmination of a three-year effort by the Department that included surveys of the cybersecurity practices of nearly 200 banks and insurance companies. The Department summarized findings of those surveys in three reports focused on the banking and insurance sectors and their use of third-party service providers.[3]

---

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

[2] *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.

[3] *See* Report on Cyber Security in the Banking Sector (May 2014), *available at* http://www.dfs.ny.gov/reportpub/dfs_cyber_banking_report_052014.pdf; Report on Cyber Security in the Insurance Sector (Feb. 2015), *available at* http://www.dfs.ny.gov/reportpub/dfs_cyber_insurance_report_022015.pdf; Update on

WHO'S COVERED?

The requirements would cover all entities that are licensed, required to be licensed, or subject to other registration requirements under the New York banking, insurance or financial services laws ("Regulated Entities"), but would exempt (i) institutions with less than 1000 customers in three calendar years; (ii) institutions with less than $5 million in gross annual revenue in three fiscal years; and (iii) institutions with less than $10 million in year-end total assets (including assets of affiliates).

WHAT'S COVERED?

The Proposed Regulations would extend to all manner of "nonpublic information," including business-related confidential information, customer nonpublic personal information, healthcare-related information and any other information that may be used to trace an individual's identity (*e.g.*, social security number, date of birth or biometric information). This is a significant expansion beyond the personally identifiable information that is the focus of most data breach laws and regulations.

WHAT'S REQUIRED?

The regulations are dense and merit careful consideration. We provide here a few of the highlights:

Administrative and Notification Requirements

- The Proposed Regulations have an effective date of January 1, 2017, with phase-in periods for certain data encryption requirements.
- If enacted, they would establish perhaps the most stringent timeline in the country for reporting cybersecurity events: notification to DFS within 72 hours of discovery of any cybersecurity event "that has a reasonable likelihood of materially affecting the normal operation of" the business or "that affects Nonpublic Information."
- This notification obligation is *per se* triggered if notice is provided to "any government or self-regulatory agency." It is not clear whether "government agency" includes law enforcement.

Cyber Security in the Banking Sector: Third Party Service Providers (Apr. 2015), *available at* http://www.dfs.ny.gov/reportpub/dfs_rpt_tpvendor_042015.pdf.

- Moreover, the obligation goes beyond unauthorized exfiltration of data and includes the "actual or potential unauthorized tampering with, or access to or use of, Nonpublic Information."
- The Proposed Regulations also would require annual certification by Regulated Entities that they have complied with the Regulations. This is particularly noteworthy given the imposition of granular requirements, described in more detail below.

Overall Cybersecurity Program, Policy, and Governance

- The Proposed Regulations require that companies establish a comprehensive cybersecurity program that appropriately identifies cyber risks and documents the types of nonpublic information the company stores, together with how it protects that information.
- The program must include a written cybersecurity policy covering 14 distinct categories, which must be reviewed at least annually by the board of directors (or equivalent body or Senior Management for entities without boards).
- Other notable requirements include:
  - Appointment of a Chief Information Security Officer ("CISO"), who must provide biannual reports to the board covering six distinct categories of information;
  - Annual penetration testing and quarterly vulnerability scanning;
  - Annual risk assessments conducted in accordance with written procedures adopted by the company;
  - Development of guidelines for assessing security for applications, whether developed in-house or externally; and
  - Establishment of cybersecurity training for employees, with enhanced training for key cybersecurity personnel.

Access Controls

- The Proposed Regulations also continue the trend of converting data security "best practices" into regulatory requirements, mandating that Regulated Entities:
  - Encrypt all "Nonpublic Information" that is at rest or in transit. (The Proposed Regulations contemplate a phase-in period of one year for data

in transit and five years for data at rest if companies maintain suitable mitigating controls);

- Adopt the principle of "need-to-know" access to sensitive data;
- Deploy multi-factor authentication for all remote network access and privileged access to certain sensitive systems;
- Implement and maintain robust auditing to enable detection and response to a cybersecurity event, to track privileged user access to critical systems, and to protect the integrity of the audit trail. These records must be maintained for at least 6 years; and
- Develop data retention policies that mandate destruction of sensitive data when it is no longer needed.

Third-Party Vendor Management

- Not surprisingly, the Proposed Regulations devote substantial attention to oversight of third-party vendors, requiring companies to:
  - Implement written policies and procedures for vendor management that include minimum cybersecurity practices that the vendors must follow;
  - Outline due diligence processes used to evaluate the vendors;
  - Review third-party vendors at least annually regarding the adequacy of their cybersecurity practices; and
  - Establish "preferred provisions" for inclusion in vendor contracts that address multi-factor authentication, use of encryption, vendor obligations to notify the company of data breaches, the rights of the company to audit the vendor's cybersecurity, and representations and warranties from the vendor regarding its services or products.

Incident Response Planning

- Regulated Entities would be required to implement a written incident response plan covering seven distinct topics including:
  - Defining clear roles, responsibilities, and levels of decision-making authority in response to a breach;
  - External and internal communications and information sharing;
  - Documentation and reporting of events; and
  - Evaluation and revision of the incident response plan at the conclusion of an incident.

- This continues a trend of requiring continual improvement and incorporation of "lessons learned" from prior incidents into preparation for responses to future ones.

Takeaways

- If enacted, the new DFS cybersecurity regulations would raise the bar significantly for banks, insurers and other financial services providers under the Department's jurisdiction. The Proposed Regulations are far-ranging in scope, including not only specific technical safeguards but also requirements regarding governance, incident planning, data management and system testing, and an aggressive 72-hour time frame to notify DFS of certain cyber incidents.
- Although the Proposed Regulations echo a growing chorus of other regulators calling for improved cybersecurity measures by banks and insurers (notably the Financial Stability Oversight Council, FFIEC and the Federal Reserve Board), they go much further than any set forth before by requiring a comprehensive approach to mitigating cybersecurity risks.
- As cyber threats continue to increase in volume and complexity, DFS's proposals likely will influence the approach taken by federal and state regulators as they consider further regulation in this area and as they review the practices of organizations under their jurisdiction.

* * *

Please do not hesitate to contact us with any questions.