September 15, 2016

New York DFS Proposes New Rules on Cybersecurity

Proposed Rules Would Require Covered Financial Institutions to Establish Cybersecurity Programs and to Certify Compliance Annually with DFS

On Tuesday, the New York Department of Financial Services ("DFS") proposed new rules that would require covered financial institutions to establish and maintain cybersecurity programs designed to protect consumers and the financial services industry from the threat of cyberattacks. The rules were proposed following a survey by DFS of the cybersecurity practices of some 200 regulated banking institutions and insurance companies, as well as discussions with cybersecurity experts on emerging trends and risks.

Covered entities include banks, insurance companies, and other financial services institutions regulated by DFS. Certain limited exceptions would apply to smaller institutions.

The rules would require a covered entity to "assess its specific risk profile and design a program that addresses its risk in a robust fashion."[1] The board or senior officer(s) of each institution would be responsible for an organization's cybersecurity program and would be required to file an annual certification with DFS confirming compliance with the regulations.[2]

The proposed rules are subject to a 45-day notice and public comment period before final issuance. As drafted, the proposed rules have an effective date of January 1, 2017, and covered entities would have 180 days from that date to comply with the rules.

Summary of the Proposed Rules

Key provisions of the proposed rules include the following:

- **Cybersecurity Program**: The new rules would require each covered entity to establish and maintain a cybersecurity program designed to ensure the "confidentiality, integrity and availability" of its information systems. A qualifying program must be designed to perform several "core" cybersecurity functions, including:
  - Recognize internal and external cyber risks by identifying nonpublic information stored on the entity's information systems, the sensitivity of such information, and how and by whom it may be accessed;
  - Protect the entity's information systems from unauthorized access or other malicious acts;

- Detect attempts to gain unauthorized access to the entity's information systems, respond accordingly to mitigate negative effects, and recover from successful attempts; and
- Fulfill all regulatory reporting obligations.[3]

As part of its cybersecurity program, each entity would be required to encrypt all nonpublic information stored on its systems (both in transit and at rest),[4] establish policies for the destruction of nonpublic information on its systems that is no longer needed,[5] and provide regular cybersecurity awareness training to employees.[6]

- **Cybersecurity Policy**: The rules would also require each covered entity to implement and maintain a written cybersecurity policy setting forth the entity's procedures for the protection of its information systems and nonpublic information stored on those systems. Among other things, the policy would need to address information and systems security, access controls, disaster recovery plans, customer data privacy, risk assessment, and incident response. The proposed rules would require that the policy be reviewed at least annually by the entity's board of directors or equivalent governing body and approved by a senior officer.[7]

- **Chief Information Security Officer**: Under the proposed rules, each covered entity would need to designate a qualified individual to serve as Chief Information Security Officer ("CISO"). The CISO would be responsible for overseeing and implementing the entity's cybersecurity program and enforcing its cybersecurity policy.

  A covered entity would be permitted to fulfill this obligation using a third party service provider, so long as the covered entity (1) retains responsibility for compliance with the provision; (2) designates a senior member to oversee the third party service provider; and (3) requires that the third party service provider maintain a cybersecurity program that meets the requirements of the provision. The rules would also require the CISO to develop a bi-annual report on the entity's cybersecurity program, attempted attacks, and risks to the entity, and present the report to the entity's board of directors or equivalent governing body.[8]

  Additionally, an entity would be required to employ cybersecurity personnel sufficient to manage its cybersecurity risks and to perform the "core" cybersecurity functions listed above. An entity would be permitted to use a qualified third party service provider to assist in fulfilling this requirement, subject to additional requirements.[9]

- **Testing and Audit Trail**: The proposed rules require that each covered entity conduct penetration testing and vulnerability assessments of its information systems at least annually, and that it track and maintain data on its systems to the extent necessary for complete and accurate reconstruction of financial transactions to detect and respond to cyberattacks. An entity would also be required to track

access by authorized users to its information systems and protect the integrity of data stored as part of any audit trail. Records produced as part of the audit trail would need to be maintained for at least six years.[10]

- **Risk Assessment**: The rules would require a covered entity to conduct a written risk assessment of its information systems at least annually.[11]

- **Multi-Factor Authentication**: Under the proposed rules, a covered entity would be required to institute multi-factor authentication for individuals accessing its internal systems or data from an external network. Multi-factor authentication, as defined by the proposed rules, means authentication through verification of at least two of the following: (1) knowledge factors, such as a password; (2) possession factors, such as a token or text message; and (3) inherence factors, such as a biometric characteristic.[12]

- **Notices to Superintendent**: The proposed rules would require covered entities to notify DFS within 72 hours of any attempted cyberattacks that have "a reasonable likelihood of materially affecting the normal operation" of the entity or that affect nonpublic information.[13] Covered institutions may want to consider whether they can submit these notices in a manner that garners protection from liability under the federal Cybersecurity Information Sharing Act of 2015 (CISA).[14]

- **Board or Senior Officer Annual Certification**: The rules would also require a covered entity to submit to DFS a written statement by January 15 of every year, through a form provided as an exhibit to the proposed rules, certifying that the entity is in compliance with the requirements set forth in the rules. The certification would require the signature of the chairperson of the board of directors of the entity or of a senior officer of the entity. An entity would need to maintain for examination by DFS all records and data supporting the certificate for a period of five years.[15]

Application of Proposed Rules

Limited Exemption. The proposed rules provide a limited exemption for covered entities that satisfy all three of the following criteria: (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. The exemption releases these institutions from the requirements of the rules, except for, among other requirements, a cybersecurity program and policy, risk assessments, destruction of nonpublic data and notices to DFS.[16]

Effective Date. If finalized, the rules would become effective on January 1, 2017, and covered entities would have 180 days from that date to comply with the rules. Covered entities would be required to submit compliance certifications to DFS beginning on January 15, 2018.[17]

Key Observations from DFS Survey Results

DFS stated that the rules were informed by its survey of regulated banking institutions and insurance companies and discussions with cybersecurity experts. DFS previously issued three reports on its findings. The following are key observations from each report:

- **Report on Cybersecurity in the Banking Sector (May 2014)**: (1) the vast majority of depository institutions surveyed relied on both in-house and external vendor-provided resources to manage their information technology systems; (2) nearly all institutions surveyed (almost 90%) reported having an information security framework in place that included the five "key pillars" of such programs: (i) a written policy, (ii) employee training, (iii) risk identification, (iv) audits, and (v) incident monitoring and reporting; (3) a wide variety of security technologies aimed at improving systems security and preventing cyber breach were employed by institutions of all sizes, including anti-virus software, spyware and malware detection, firewalls, server-based access control lists, intrusion detection tools, intrusion prevention systems, vulnerability scanning tools, encryption for data in transit and encrypted files; (4) penetration tests were conducted by almost all institutions; (5) most institutions surveyed experienced intrusions or attempted intrusions of their information systems over the prior three years; and (6) large and medium institutions were more likely than smaller institutions to have a documented information security strategy in place for the future.

- **Report on Cybersecurity in the Insurance Sector (February 2015)**: (1) a wide array of factors (not just reported assets) affected the sophistication and comprehensiveness of insurers' cybersecurity programs, including the variety of business lines written and the sales and marketing technologies associated with those lines; (2) 95% of insurers already believed they had adequate staffing levels for information security and only 14% of CEOs received monthly briefings on information security; (3) 56% of insurers surveyed relied on both internal and external resources to manage their information technology systems (the remaining 44% managed their systems entirely in-house); (4) nearly all insurers surveyed (almost 98%) reported having an information security framework in place that included the five "key elements" of cybersecurity programs discussed above; (5) insurers employed a number of security technologies, and 100% of those surveyed used anti-virus software, tools to detect malicious code such as spyware or malware, firewalls, intrusion detection tools and encryption for data in transit—nearly all institutions surveyed employed data loss prevention tools, file encryption and vulnerability scanning tools; (6) 100% of insurers surveyed reported that they engaged in penetration testing; (7) 58% of insurers reported that they experienced no successful breaches in the three years preceding the survey, 35% reported experiencing between one and five breaches, 2% reported experiencing between six and ten breaches and 5% reported experiencing more than ten breaches; (8) over half of the insurers surveyed reported that their organization's information security strategy adequately addressed new and emerging risks, while 40% reported a need to modify their strategies to address new and emerging risks.

- **Update on Cybersecurity in the Banking Sector: Third Party Service Providers (April 2015)**: (1) almost all banking organizations surveyed classified their third-party service providers by risk and 95% of the surveyed institutions conducted specific information security assessments of their high-risk vendors; (2) all of the institutions surveyed had written vendor management policies, and all but three had written procedures for selecting third-party vendors; (3) 90% of the surveyed institutions utilized encryption for any data transmitted to or from third parties, but only 38% used encryption for data "at rest."

Conclusion

The proposed rules would create new cybersecurity requirements for covered entities. Many of these requirements are consistent with existing guidance from other financial industry regulators and, according to the DFS survey data, are already reflected in industry best practices. However, implementing these new DFS requirements alongside the extensive federal regulatory guidance in this area could prove costly and complex. It is also possible that other states may soon follow suit and seek to issue similar rules.

The proposed regulation can be found here and the DFS press release can be found here. The three DFS reports that resulted from its surveys of regulated institutions can be found here.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Jack Baughman
212-373-3021
jbaughman@paulweiss.com

H. Christopher Boehning
212-373-3061
cboehning@paulweiss.com

Susanna M. Buergel
212-373-3553
sbuergel@paulweiss.com

Jessica S. Carey
212-373-3566
jcarey@paulweiss.com

Jay Cohen
212-373-3163
jaycohen@paulweiss.com

Roberto Finzi
212-373-3311
rfinzi@paulweiss.com

Michael E. Gertzman
212-373-3281
mgertzman@paulweiss.com

Roberto J. Gonzalez
202-223-7316
rgonzalez@paulweiss.com

Michele Hirshman
212-373-3747
mhirshman@paulweiss.com

Brad S. Karp
212-373-3316
bkarp@paulweiss.com

Lorin L. Reisner
212-373-3250
lreisner@paulweiss.com

Elizabeth M. Sacksteder
212-373-3505
esacksteder@paulweiss.com

Theodore V. Wells Jr.
212-373-3089
twells@paulweiss.com

Richard C. Tarlowe
212-373-3035
rtarlowe@paulweiss.com

Associate Andrew D. Reich contributed to this client memorandum.

[1] *Cybersecurity Requirements for Financial Services Companies* at 2, September 13, 2016, to be codified at 23 NYCRR Part 500 (not yet published in New York Register), available at http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.
[2] *Id.*
[3] *Id.* at 6 (Section 500.02).
[4] *Id.* at 14 (Section 500.15).
[5] *Id.* at 14 (Section 500.13).
[6] *Id.* at 14 (Section 500.14).
[7] *Id.* at 7 (Section 500.03).
[8] *Id.* at 8 (Section 500.04).
[9] *Id.* at 11 (Sections 500.10 & 500.11).

[10] *Id.* at 9–10 (Sections 500.05 & 500.06).
[11] *Id.* at 11 (Section 500.09).
[12] *Id.* at 4 & 13 (Sections 500.01(f) & 500.12).
[13] *Id.* at 16 (Section 500.17).
[14] For a guide to CISA, please see the Paul, Weiss client memorandum located here.
[15] *Cybersecurity Requirements for Financial Services Companies* at 16 (Section 500.17).
[16] *Id.* at 17 (Section 500.18).
[17] *Id.* at 17 & 18 (Sections 500.2o & 500.21).