Simpson Thacher

Memorandum

New York State Department of Financial Services Revises Proposed Cybersecurity Regulations

January 4, 2017

On December 28, 2016, the New York State Department of Financial Services ("DFS") released a revised version of proposed regulations that would create new cybersecurity standards and reporting guidelines for DFS-regulated banks, insurance companies, and other financial services institutions (*e.g.*, licensed nonbank lenders, mortgage companies, money transmitters). These revisions follow the conclusion of a public comment period on the DFS's initial proposal from September, which was characterized by some commenters as "one-size-fits-all" in nature and too prescriptive. DFS invites comments on this version by January 27, 2017.

According to Governor Andrew M. Cuomo, the "first-in-the-nation" regulations will help protect New York from the "ever-growing threat of cyber-attacks."[1] The revised proposal requires, among other things, that DFS-regulated banking, financial, and insurance institutions:

- establish a cybersecurity program;
- adopt a written cybersecurity policy;
- designate a head of information security and utilize cybersecurity personnel;
- create and implement policies and procedures for dealing with third party service providers;
- report designated cybersecurity events to DFS within 72 hours;
- conduct penetration testing and vulnerability assessments; and
- file annual reports with DFS.

[1] Press Release, New York State Department of Financial Services, DFS Issues Updated Proposed Cybersecurity Regulation Protecting Consumers and Financial Institutions (Dec. 28, 2016), *available* here.

The proposed regulations, which are subject to a new 30-day comment period, would take effect on March 1, 2017.

Background

The proposed regulations follow research by DFS into the state of cybersecurity measures in the financial sector and related industries.[2] In 2013, DFS conducted a financial services industry survey on cybersecurity as a response to what it saw as an increasing number of cybersecurity-related attacks from a variety of sources, such as "unfriendly nation states," hackers, and organized crime groups.[3] While the report it published following the survey noted that many institutions had taken significant steps to create appropriate cybersecurity policies and procedures, there were many remaining concerns, and DFS observed that "when competition surrounding new product development is fierce, security can lag behind."[4] DFS also published reports on the cybersecurity challenges facing the insurance sector, as well as an update on the banking sector focused specifically on third party service providers; these reports made similar observations. DFS concluded that cybersecurity events cause significant financial losses for the entities it regulates and for New York consumers.[5] Accordingly, DFS deemed it necessary to create minimum standards across the financial services industry to "ensure that Department-regulated entities are effectively addressing ever-growing cybersecurity risks in order to protect consumers and continue operating in a safe and sound manner."[6]

The Proposed Regulations

A. Who Would Be Impacted?

The proposed regulations would apply to "Covered Entities," which are defined as individuals and entities "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law" in New York State.[7] However, a "limited" small business exemption would apply for Covered Entities with (1) fewer than 10 employees (including independent contractors), (2) less than $5 million in gross annual revenue in each of the last three fiscal years, or (3) less than $10 million in year-

[2] *See* New York State Department of Financial Services, Update on Cyber Security in the Banking Sector: Third Party Service Providers (April 2015); New York State Department of Financial Services, Report on Cyber Security in the Insurance Sector (February 2015); New York State Department of Financial Services, Report on Cyber Security in the Banking Sector (May 2014), *available* here.

[3] *See* New York State Department of Financial Services, Report on Cyber Security in the Banking Sector (May 2014).

[4] *Id.*

[5] *See* N.Y. Reg., Sept. 28, 2016 at 68 (regulatory impact statement), *available* here.

[6] *Id.*

[7] *See* Cybersecurity Requirements for Financial Services Companies (Dec. 28, 2016) (to be codified at 23 NYCRR 500) (proposed regulation).

end total assets.[8] The updated proposal changed the requirements for these exceptions after feedback received during the comment period to exempt more small businesses. Nevertheless, since the proposal includes requirements for Covered Entities' interactions with third parties who have access to sensitive data, the impact of the proposal will likely have far reaching implications beyond the financial sector by impacting those who work with Covered Entities.[9]

B. What Would Be Required

DFS acknowledges in the proposal that many firms have already been proactive in creating and updating their cybersecurity programs, and often with great success, but also states that given the seriousness of the threat, "certain regulatory minimum standards are warranted." DFS regards the proposed regulations as not "overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances."[10] The proposed regulations are intended to set a baseline for where institutions should begin, as well as to serve as a tool to bring cybersecurity issues front and center to boards of directors and senior management.

1. Establish a Cybersecurity Program

The proposed regulations would require that all Covered Entities design a cybersecurity program that focuses on six key functions:

1) identifying and assessing internal and external cyber risks;

2) creating a defensive infrastructure to protect their information systems;

3) detecting "cybersecurity events" (which are defined as any acts or attempts, successful or unsuccessful, to gain unauthorized access to, disrupt, or misuse an information system or information stored on such information system);

4) responding to those events and mitigate any negative effects;

5) recovery following a cybersecurity event and restoring normal operations and services; and

6) fulfilling DFS regulatory reporting obligations.

[8] *See id.* The proposed regulations go into more detail about what specific portions of the regulations would still apply, as well as what to do in the event a Covered Entity ceases to meet the requirements for the exemption.

[9] *See id.*

[10] *See id.*

Furthermore, the proposed regulations require that as part of their cybersecurity program, Covered Entities limit user access privileges to information systems that provide access to nonpublic information.

2. *Adopt a Written Cybersecurity Policy*

Under the proposal, in addition to creating a program as outlined above, Covered Entities would also be required to have a written cybersecurity policy approved by a senior officer (defined as the senior individual or individuals responsible for the management, operations, security, information systems, compliance, and/or risk of a Covered Entity) that sets forth the company's policies and procedures for dealing with nonpublic information stored on their information systems.

The proposal sets out 14 minimum areas that would need to be addressed in the policy, including:

- access controls and identity management;
- business continuity and disaster recovery planning and resources;
- physical security and environmental controls;
- customer data privacy; and
- vendor and third party service provider management.

Additionally, the proposed regulations would require Covered Entities to implement multi-factor authentication (*i.e.*, verification of at least two different types of authentication factors) for anyone accessing their internal systems or data from an external network. Other major proposed requirements include limitations on data retention for all nonpublic information institutions are not required to retain by law or regulation and encryption of all nonpublic information held by them "both in transit and at rest."[11]

3. *Designate Head of Information Security and Utilize Cybersecurity Personnel*

The proposal would require Covered Entities to have sufficient staff to deal with cybersecurity issues and to designate a qualified individual to oversee and implement the cybersecurity program and enforce the institution's cybersecurity policies. Under the proposal, the individual may be employed directly by the company, by an affiliate of the company, or by a third party service provider. This individual would be responsible for developing an annual report to present to the Covered Entity's board of directors. Furthermore, internal or contracted cybersecurity personnel would need to be regularly updated and trained on changing cybersecurity threats and countermeasures. Under DFS's earlier proposal, Covered Entities would have been required to designate a single individual within

[11] *See id.*

the company to serve as Chief Information Security Officer and hire internal cybersecurity personnel, but the revisions make it clear that these requirements could be met using a third party service provider.

4. *Create and Implement Policies and Procedures for Working with Third Party Service Providers*

Some of the most noticeable updates to the proposed regulations deal with third party service providers. One of the reports prepared by DFS before the release of the initial proposal focused exclusively on the cybersecurity issues the banking sector faces as a result of the use of third party service providers and found that the procedures and policies in place for dealing with these third parties varied depending on the size and type of both the Covered Entity and the level of risk involved in the relationship with the third parties. The proposed regulations would require the downstream implementation of certain cybersecurity policies and procedures to be met by all third parties doing business with Covered Entities with access to their information systems and any nonpublic information they have. The proposed regulations would also require periodic assessments of third party service providers to ensure continued adequacy of their cybersecurity programs. In addition, Covered Entities' policies and procedures with respect to third party service providers would be required to include relevant guidelines addressing due diligence matters and/or contractual protections. Notably, the proposal no longer requires that third parties provide identity protection services for the customers of the Covered Entity who are "materially impacted" by any form of cybersecurity event caused by the third parties either negligent or willful misconduct.[12]

Because these requirements would apply to all third parties who have access to the information systems and nonpublic information of all Covered Entities, DFS's proposed regulations could have major impacts beyond the financial sector, to all those organizations who work with them, even those who are exempted themselves from complying with the rest of the regulations.

5. *Report Designated Cybersecurity Events to DFS within 72 Hours*

The proposed regulations would require Covered Entities to notify DFS as promptly as possible but in no event later than 72 hours after a determination that one of the following types of cybersecurity events has occurred:

- a cybersecurity event of which notice is required to be provided to any governmental body, self-regulatory agency, or any other supervisory body; and
- a cybersecurity event that has a reasonable likelihood of materially harming any material part of the normal operation of the Covered Entity.

[12] 38 N.Y. Reg. 67 (Sept. 28, 2016) (proposed regulations).

6. Penetration Testing and Vulnerability Assessments

DFS's proposed regulations would require Covered Entities to conduct at least annual penetration testing and bi-annual vulnerability assessments of their information systems, including any systematic scans or reviews of information systems reasonably designed to identify publicly known cybersecurity vulnerabilities.

7. File Annual Reports with DFS

The proposed regulations would require each Covered Entity to submit a written statement certifying compliance with all the regulations by February 15 of each year, starting in February of 2018.

C. What Is the Timeline for Compliance?

If adopted, the proposed regulations would take effect starting March 1, 2017. Following that date, Covered Entities would have 180 days to comply with the regulations' requirements (including the requirement to report cybersecurity events within 72 hours), and annual reporting obligations to DFS would commence February 15, 2018. By February 15, each Covered Entity would also be required to submit yearly statements to DFS, signed by the chairperson of the board of directors or a senior officer, certifying that it is in compliance with the requirements of the regulations.

Conclusion

The proposed regulations are another sign that cybersecurity is evolving from an area governed largely by "best practices" to one subject to heightened regulatory requirements. The proposed regulations exceed the current minimum federal standards set nearly 20 years ago under the Gramm-Leach-Bliley Act.[13] For some Covered Entities, DFS's proposed regulations may not require many changes beyond the new reporting requirements; other Covered Entities, however, may have to take significant steps to ensure their compliance with the regulations.

For those who are interested in submitting comments to DFS on the revised proposal, all comments are due by January 27, 2017.

[13] 38 N.Y. Reg. 69 (Sept. 28, 2016) (regulatory impact statement).

For more information regarding the proposed regulations, please contact any member of the Firm's Privacy and Cybersecurity Practice and Financial Institutions Practice.

The contents of this publication are for informational purposes only. Neither this publication nor the lawyers who authored it are rendering legal or other professional advice or opinions on specific facts or matters, nor does the distribution of this publication to any person constitute the establishment of an attorney-client relationship. Simpson Thacher & Bartlett LLP assumes no liability in connection with the use of this publication. Please contact your relationship partner if we can be of assistance regarding these important developments. The names and office locations of all of our partners, as well as our recent memoranda, can be obtained from our website, www.simpsonthacher.com.

Simpson Thacher Worldwide

UNITED STATES

New York
425 Lexington Avenue
New York, NY 10017
+1-212-455-2000

Houston
600 Travis Street, Suite 5400
Houston, TX 77002
+1-713-821-5650

Los Angeles
1999 Avenue of the Stars
Los Angeles, CA 90067
+1-310-407-7500

Palo Alto
2475 Hanover Street
Palo Alto, CA 94304
+1-650-251-5000

Washington, D.C.
900 G Street, NW
Washington, D.C. 20001
+1-202-636-5500

EUROPE

London
CityPoint
One Ropemaker Street
London EC2Y 9HU
England
+44-(0)20-7275-6500

ASIA

Beijing
3901 China World Tower
1 Jian Guo Men Wai Avenue
Beijing 100004
China
+86-10-5965-2999

Hong Kong
ICBC Tower
3 Garden Road, Central
Hong Kong
+852-2514-7600

Seoul
25th Floor, West Tower
Mirae Asset Center 1
26 Eulji-ro 5-Gil, Jung-Gu
Seoul 100-210
Korea
+82-2-6030-3800

Tokyo
Ark Hills Sengokuyama Mori Tower
9-10, Roppongi 1-Chome
Minato-Ku, Tokyo 106-0032
Japan
+81-3-5562-6200

SOUTH AMERICA

São Paulo
Av. Presidente Juscelino
Kubitschek, 1455
São Paulo, SP 04543-011
Brazil
+55-11-3546-1000