Wall Street LAWYER
Securities in the Electronic Age

October 2016 ▪ Volume 19 ▪ Issue 10

NYDFS: "FIRST-IN-THE-NATION" CYBERSECURITY PROPOSAL

By Mark L. Krotoski, Charles Horn & Sarah V. Riddell

Mark L. Krotoski is a partner in the Silicon Valley office of Morgan, Lewis & Bockius. Mr. Krotoski represents and advises clients on antitrust cartel investigations; cybersecurity and privacy matters; trade secret, economic espionage, fraud, and foreign corrupt practices cases; and government investigations. Charles M. Horn is a partner in the Washington, D.C. office of Morgan Lewis. Mr. Horn counsels U.S. and international banks and other financial institutions on corporate, regulatory, supervisory, enforcement and compliance matters before all major federal and state financial regulatory agencies. Sarah V. Riddell is an associate in the firm's Chicago office. Ms. Riddell is a former lawyer with the U.S. Commodity Futures Trading Commission (CFTC), and she advises domestic and foreign exchanges, derivatives clearing organizations, swap execution facilities, and other financial institutions on a broad range of regulatory matters, including CFTC registration and compliance. Contact: mark.krotoski@morganlewis.com or charles.horn@morganlewis.com.

New "first-in-the-nation" cybersecurity rules in the pipeline for banks, insurers, and financial services companies regulated in New York could prove costly for companies, but will they improve cybersecurity?

The New York Department of Financial Services (NYDFS) has proposed cybersecurity rules that would require banks, insurers, and other NYDFS-regulated financial services companies to adhere to stringent cybersecurity requirements mandating firms to test their systems, establish plans to respond to cybersecurity events, and annually certify compliance with the cybersecurity requirements, among other mandates. Comments on the proposed rules are due in 45 days.

Do the proposed rules signal a new trend to regulate cybersecurity? Will other states and regulators consider similar mandatory cybersecurity requirements? This article will discuss the genesis of the proposed rules and offer observations on how the rules could impact companies and affect the regulatory landscape in this space.

Background

On September 13, the NYDFS issued what was described as "a new first-in-the-nation regulation" titled "Cybersecurity Requirements for Financial Services Companies" (Proposal).[1]

The Proposal had been foreshadowed by the agency's recent examination and focus on cybersecurity issues. Cybersecurity has been

IN THIS ISSUE:

THOMSON REUTERS

41852288

at the forefront of NYDFS's regulatory initiatives for some time. NYDFS issued its first report on cybersecurity in the banking sector in May 2014,[2] a second cybersecurity report on the insurance sector in February 2015,[3] and a third report on the use of third-party service providers in the banking sector in April 2015.[4] Over the past several years, NYDFS has surveyed close to 200 regulated banking institutions and insurance companies and has met with cybersecurity experts. Findings from its surveys and other due diligence informed the Proposal, which largely follows the areas identified in the NYDFS's November 2015 letter to federal financial services regulatory agencies (Letter to Regulators).[5] The Letter to Regulators invited comment on the NYDFS regulatory framework and noted the "demonstrated need for robust regulatory action in the cyber security space" and that "the Department is now considering a new cyber security regulation for financial institutions."

Overview of the NYDFS Cybersecurity Proposal

Important Dates

Comments on the Proposal are due by November 12, 2016. The Proposal, unless modified, would become effective on January 1, 2017, with a 180-day grace period for compliance. Thus, banking, insurance, and financial services firms subject to the Proposal (Covered Entities) would be required to have a cybersecurity program and other requirements in place by June 30, 2017, and Covered Entities would begin filing the annual compliance certification (described below) on January 15, 2018.

Core Functions of Cybersecurity Program

The Proposal would require each Covered Entity to establish a cybersecurity program that

- identifies internal and external cyber risks;
- uses defensive infrastructure to protect the Covered Entity's Information Systems[6] and Nonpublic Information stored on such systems from unauthorized access, use, or other malicious acts;
- detects "Cybersecurity Events," defined as "any act or attempt, *successful or unsuccessful*, to gain unauthorized access to, disrupt, or misuse an Information System or information stored on such Information System";
- responds to identified Cybersecurity Events to mitigate any adverse effects;

Wall Street Lawyer
West LegalEdcenter
610 Opperman Drive
Eagan, MN 55123

One Year Subscription ● 12 Issues ● $ 867.96
(ISSN#: 1095-2985)

- recovers from Cybersecurity Events (the Proposal does not mandate a specific recovery time objective); and
- fulfills all regulatory reporting obligations.[7]

As part of a Covered Entity's cybersecurity program, a Covered Entity would be required to establish a cybersecurity policy that addresses 14 areas,[8] including customer data privacy, vendor and third-party service provider management, risk assessment,[9] and incident response, among others. A Covered Entity's board of directors would need to review (and a senior officer approve) the cybersecurity policy at least annually and as frequently as necessary to address the cybersecurity risks posed to the Covered Entity.[10] The Proposal includes "minimum" requirements for quarterly vulnerability assessments and annual penetration testing,[11] among other requirements for incident response plans, encryption,[12]access permissions, and authentication methods typically found in cybersecurity best practices.

We have highlighted the more notable features of the Proposal below.

Chief Information Security Officer and Other Personnel

A Covered Entity would be responsible for designating a qualified individual to serve as a Chief Information Security Officer (CISO) to oversee and implement the cybersecurity program and enforce the cybersecurity policy. The Proposal would permit a Covered Entity to use a third-party service provider to comply with this requirement, but the Covered Entity would retain responsibility for compliance and would need to designate a senior member of its personnel to oversee the third-party service provider.

New regulatory obligations are imposed on the CISO.[13] The Proposal requires a bi-annual report to the Covered Entity's board of directors, which differs from the proposal in the Letter to the Regulators, which would have required a CISO to submit an annual report to NYDFS that assessed the Covered Entity's cybersecurity program and the cybersecurity risks to the Covered Entity, and that was reviewed by the board of directors before submission to NYDFS.

Under the Proposal, the CISO's bi-annual report to the Covered Entity's board of directors must

- assess the confidentiality, integrity, and availability of the Covered Entity's Information Systems;
- detail exceptions to the Covered Entity's cybersecurity policies and procedures;
- identify cyber risks to the Covered Entity;
- assess the effectiveness of the cybersecurity program;
- propose steps to remediate inadequacies identified in the cybersecurity program; and
- summarize all material Cybersecurity Events that affected the Covered Entity during the time period covered by the report.

In addition, the CISO would be required on an annual basis to review, assess, and update the Covered Entity's guidelines, procedures, and standards (requirements under the Proposal) for secure development practices of in-house applications.

Under the Proposal, all personnel would be subject to regular cybersecurity awareness training, updated to reflect the risks identified in a Covered Entity's annual risk assessment.[14] Cybersecurity personnel would be required to attend regular updates and training sessions and to take steps to stay current with regard to changing cybersecurity threats and countermeasures.

Third-Party Service Providers: Evaluation and "Preferred Provisions"

The Letter to Regulators discussed minimum "pre-

ferred provisions" that should be included in agreements with third-party service providers. Consistent with that observation, the Proposal requires that a Covered Entity's cybersecurity policy cover third parties. The cybersecurity policy would need to establish minimum preferred provisions to be included in contracts with third-party service providers. In addition, the Proposal would require a Covered Entity to identify third parties with access to Information Systems or Nonpublic Information, establish minimum cybersecurity practices each third party must satisfy, evaluate the adequacy of each third party's cybersecurity practices, and annually assess each third party's continued adequacy of its cybersecurity practices.

With one significant difference from the Letter to the Regulators, the Proposal would require a Covered Entity to establish preferred provisions for contracts with third-party service providers,[15] to the extent applicable, provisions regarding

- 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 to the Covered Entity in the event of a cybersecurity incident;
- identification of protection services provided to customers materially impacted by a Cybersecurity Event resulting from the third party's negligence or willful misconduct (this provision appears to replace the requirement in the Letter to Regulators that a third party indemnify the Covered Entity in the event of a cybersecurity incident that results in loss);
- the right of the Covered Entity or its agents to perform cybersecurity audits of the third-party vendor; and
- representations and warranties by the third party that the service or product provided to the Covered Entity is free of viruses, "trap doors," "time bombs," and other mechanisms that would impair the security of the Covered Entity's Information Systems or Nonpublic Information.

Annual Compliance Certification

As described above, the Proposal would require the board of directors to annually review the Covered Entity's cybersecurity program and provide a Certification of Compliance with the NYDFS Cybersecurity Regulations.[16] Specifically, the board of directors would need to review documents, reports, certifications, and opinions of officers, employees, representatives, outside vendors, and other individuals or entities, as necessary. The chairperson of the board or senior officer would be required to certify that the Covered Entity's cybersecurity program complies with NYDFS regulations. NYDFS provides a template certification in the Proposal.

Notification to NYDFS

A Covered Entity must notify the NYDFS Superintendent within 72 hours of becoming aware of a Cybersecurity Event that has a reasonable likelihood of materially affecting the normal operation of the Covered Entity or Nonpublic Information.[17] In addition, a Covered Entity must notify the NYDFS Superintendent when it notifies other government or self-regulatory organizations of a Cybersecurity Event and when a Cybersecurity Event involves "the actual or potential unauthorized tampering with, or access to or use of, Nonpublic Information."

Audit Trail

The Proposal subjects Covered Entities to strict audit trail requirements.[18] Under the Proposal, an Audit Trail must track and maintain data for complete and accurate reconstruction of all financial transactions and accounting necessary to enable the Covered Entity to detect and respond to a Cybersecurity Event,

as well as log all privileged access to "critical systems," which are not defined under the Proposal. The Audit Trail cannot be alterable or subject to tampering. Further, a Covered Entity would be required to maintain records of the Audit Trail for six years (note that the Proposal's standard record retention period is five years).[19]

Exclusion

Although the Proposal purports to exclude "small firms"[20] from some of the Proposal's mandates, such firms will still be subject to, among other things, the requirements for a cybersecurity program, cybersecurity policy, a third-party information security oversight program, and the NYDFS cybersecurity event notification requirements.

Initial Observations

The Proposal raises a number of important operational, compliance, and risk management concerns for New York financial firms. We discuss some of these concerns below.

Costs of Compliance

NYDFS's "minimum standards" under the Proposal will come at a high cost. The numerous mandatory requirements that are in the Proposal would, if adopted, materially increase operational and compliance costs for New York financial firms, even for small firms that in fact are not exempted from many of the Proposal's more substantial requirements. A central question, however, is whether the costs of meeting these new regulatory standards will necessarily result in stronger cybersecurity, or will they divert limited resources that would be better tailored and used to address specific cyber risks? Effective cybersecurity should be flexible and tailored to the risks and needs of the program. While the Proposal cautions against "being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances," it fails to recognize the burdens imposed by the new regulatory requirements. In turn, the mandatory regulations are likely to result in higher cybersecurity costs and not necessarily more effective cybersecurity programs.

Other Options to Foster Effective Cybersecurity

Another question concerns the mandatory nature of the new regulations. Since the Proposal recognizes the "great success" of many firms in developing cybersecurity programs, it seems that enforcement efforts could instead focus on those firms that lack effective cybersecurity practices. An "across the board" mandatory new cybersecurity regimen is inconsistent with the more flexible and tailored approach encouraged by other government agencies, including those at the federal level.

Certainly, promoting effective cybersecurity practices across firms with access to Nonpublic Information remains essential. The question is whether and why government should impose prescriptive mandatory requirements in stark contrast to more flexible standards and best practices that encourage companies to adopt strong cybersecurity programs.

As one example, currently, critical infrastructure sectors (16 including the financial services sector)[21] are subject to flexible cybersecurity measures pursuant to the National Institute of Standards and Technology (NIST) framework.[22] The NIST framework was established by an Executive Order with the goal that each critical infrastructure sector would "maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"[23]—calling for a voluntary, flexible framework to achieve this goal.

In contrast, NYDFS acknowledges that many firms have already increased their cybersecurity, but that some firms that have not done so should "move swiftly and urgently" so all Covered Entities are subject to "minimum" cybersecurity standards. Instead of adopt-

ing a flexible approach based on best practice standards that can be adapted as needed, NYDFS has introduced new rigid mandates. The stringent requirements beg the question: Are mandatory measures the best approach to preventing successful cybersecurity attacks and protecting customer information? Or, rather, should governments identify best practices and standards that firms can tailor to their unique information systems and cyber risks?

Expanding Concurrent Jurisdiction and Inconsistent Standards

Most of the Covered Entities are subject to oversight by multiple regulatory authorities. The Proposal would subject Covered Entities to multiple regulatory requirements (such as notification requirements) and, in some cases, diverging standards. For instance, New York banking organizations generally are subject to regulation and supervision by multiple federal bank regulatory authorities, which in turn have adopted their own guidance on information security practices, policies, and procedures.[24] Although the federal guidance in our view for the most part is not materially at odds with the substantive elements of the Proposal, New York banking organizations will be subject to more extensive prescriptive requirements than exist at the federal level, and will have to assess their compliance with the Proposal and assure that their cybersecurity programs, policies, and procedures also align with applicable federal guidance on the topic.

Notice Requirements

NYDFS broadly defines a Cybersecurity Event to include an unsuccessful attempt to gain unauthorized access to a Covered Entity's Information Systems.[25] Notification to the NYDFS Superintendent is required "no later than 72 hours after becoming aware" of a Cybersecurity Event that has a reasonable likelihood of materially affecting the normal operation of the Covered Entity or Nonpublic Information.[26]

In most cyber incidents, it is not possible to know the scope, nature, and manner of the intrusion for some time. For this reason, notification standards recognize that some time is normally required to determine the scope of the breach. Not much may be known about the incident within the first 72 hours of a cyber event. Most notification provisions also provide for delayed notification upon the request of law enforcement. Against other notification standards, the proposed NYDFS notification standard is unrealistically short, unnecessarily broad (including unsuccessful attempts), and imprecise on when it is triggered.

Also, are unsuccessful attempts, by definition, nonmaterial? At what point would NYDFS expect a Covered Entity to report an unsuccessful attempt to gain access to its Information Systems?

NYDFS would require a Covered Entity to report upon the "potential unauthorized tampering with, or access to or use of, Nonpublic Information." Thus, because of the 72-hour notice requirement, a Covered Entity may have to report about an attempt before it can determine whether the attempt potentially tampered with or accessed Nonpublic Information. The Proposal is unclear on the kind of response Covered Entities should expect NYDFS to have in this case or, more broadly, upon any notification of a Cybersecurity Event.

Notice requirements are growing in number across state and federal statutes or regulations. One of the challenges is that they apply different standards on when notice may be given, and under what circumstances. The Proposal adds new standards to the regulatory maze of notification requirements. For this reason, we previously have suggested that one federal notification should uniformly apply.[27]

Annual Compliance Certification

The annual compliance certification potentially opens the board of directors and senior officer to serious liability if the certification is later found to be inaccurate or inadequate. Not only would there be the

risk of direct liability to NYDFS, but a finding of an inaccurate certification could potentially expose the financial institution to private liability or collateral action by other state or federal regulatory authorities.[28] Moreover, NYDFS has not provided guidance on whether a Covered Entity could explain material noncompliance matters and remediation efforts taken in response to such matters. It would not be surprising, however, if directors and senior officers were reluctant to sign these certifications.

Regulatory Inflexibility?

In the introduction to the Proposal, NYDFS provides that "minimum standards" are necessary, but not such that they are "overly prescriptive" and thereby prevent cybersecurity programs to match evolving risks. What kind of flexibility does a Covered Entity have in establishing its cybersecurity program? Will a Covered Entity's designation of a CISO or determination to accept the risk of a deficiency found through testing rather than remediate be second-guessed? The Proposal does not mandate a recovery time objective in the event of a cybersecurity incident. Practically speaking, will NYDFS be concerned if a Covered Entity is not operating as normal by the business day following an event?[29]

Proposal's Impact on Other Regulators

The self-described "new first-in-the-nation" cybersecurity regulation contains new mandatory standards. It is likely that other state regulators may seek to emulate and adopt these new requirements, although it is less certain whether federal financial regulators would be encouraged to do the same. The mandatory regulations will increase the costs of cybersecurity. Because many companies have and are adopting strong cybersecurity policies, a key open question is whether more effective cybersecurity will result from the adoption of mandatory requirements such as these.

Next Steps

Covered Entities that fall within the scope of the Proposal should consider commenting on the proposal and continue to monitor actions that NYDFS takes in connection with the Proposal and other cybersecurity initiatives. After the Proposal is adopted, firms should stay abreast of cybersecurity guidance issued by NYDFS and enforcement actions NYDFS takes in relation to cybersecurity programs, and update their cybersecurity programs in light of guidance that NYDFS offers, including guidance made available in enforcement actions.

ENDNOTES:

[1]Cybersecurity Requirements for Financial Services Companies (Sept. 13, 2016), *available at* http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf; *see also* "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.

[2]Governor Andrew M. Cuomo & Superintendent Benjamin M. Lawsky, NYDFS, *Report on Cyber Security in the Banking Sector* (May 2014), *available at* http://www.dfs.ny.gov/reportpub/dfs_cyber_banking_report_052014.pdf.

[3]New York State Department of Financial Services Report on Cyber Security in the Insurance Sector (Feb. 2015); *available at* http://www.dfs.ny.gov/reportpub/dfs_cyber_insurance_report_022015.pdf.

[4]New York State Department of Financial Services Report Update on Cyber Security in Banking Sector: Third Party Service Providers (April 2015), *available at* http://www.dfs.ny.gov/reportpub/dfs_rpt_tpvendor_042015.pdf.

[5]Letter on file with the author.

[6]The Proposal defines "Information System" 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."

[7]Proposal, Section 500.02 (Cybersecurity Program).

[8]*Id.* Section 500.03(a) (Cybersecurity Policy).

[9]*Id.* Section 500.09 (Risk Assessment).

[10]*Id.* Section 500.03(b) (Cybersecurity Policy).

[11]*Id.* Section 500.05 (Penetration Testing and Vulnerability Assessments).

[12]*Id.* Section 500.15 (Encryption of Nonpublic Information).

[13]*Id.* Section 500.04 (Chief Information Security Officer).

[14]*Id.* Section 500.14 (Training and Monitoring).

[15]*Id.* Section 500.11 (Third Party Information Security Policy).

[16]*Id.* Section 500.17(b) (Notices to Superintendent).

[17]*Id.* Section 500.17 (Notices to Superintendent).

[18]*Id.* Section 500.06 (Audit Trail).

[19]*Id.* Section 500.17(b) (requiring retention of records "for examination" including "all records, schedules and data supporting th[e] certificate [of compliance] for a period of five years.").

[20]A "small firm" has fewer than 1000 customers in each of the last three calendar years, less than $5,000,000 in gross annual revenue in each of the last three fiscal years, and less than $10,000,000 in year-end total assets (including assets of all affiliates).

[21]Critical infrastructure sectors have been designated as critical because their assets, systems, and networks (whether physical or virtual) are considered so vital to the United States that their destruction or incapacity would have a debilitating effect on the nation's security, economic security, or public health or safety (or any combination thereof). The 16 critical infrastructure sectors include chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[22]Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology (Feb. 12, 2014), *available at* https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[23]Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (Feb. 12, 2013), *available at* https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[24]*See*, e.g., Federal Financial Institutions Examination Council, IT Examination HandBook InfoBase, *available at* http://ithandbook.ffiec.gov.

[25]Proposal, Section 500.01(d) (Cybersecurity Event Definition).

[26]*Id.* Section 500.17 (Notices to Superintendent).

[27]*See*, e.g., M. Krotoski, L. Wang, & J. Rosen,"The Need to Repair the Complex, Cumbersome, Costly Data Breach Notification Maze,"BNA's Privacy & Security Law Report, 15 PVLR 271 (Feb. 8, 2016), *available at* https://www.morganlewis.com/~~/media/files/publication/outside%20publication/article/bna-need-to-repair-data-breach-notification-maze-08feb16.ashx?la=en.

[28]See our prior *All Things FinReg Blog* posting on a CFPB enforcement action taken against a consumer payments provider involving inadequate data security practices, *available at* http://blogs.morganlewis.com/finreg/03/03/2016/cfpb-downloads-an-enforcement-action-on-a-payment-provider-for-data-security-issues.

[29]*See*, e.g., 17 C.F.R. § 39.18(e)(3) (requiring a derivatives clearing organization to resume daily processing, clearing, and settlement no later than the next business day following the disruption).