Client Alert

March 23, 2017

New York Cybersecurity Regulations: What Do They Mean and When Do They Mean it By?

By Nathan D. Taylor and Adam Fleisher

The New York State Department of Financial Services (NYDFS) has released guidance for covered financial institutions regarding its cybersecurity rule (the "Cybersecurity Rule" or "Rule") that took effect on March 1, 2017. The guidance comes in the form of frequently asked questions (FAQs) and a summary of key compliance dates. Although the guidance is apparently intended to assist covered financial institutions as the clock ticks towards the first of the Rule's phased compliance deadlines less than six months away, the guidance is unlikely to make the implementation challenges many financial institutions will face any less daunting.

The Cybersecurity Rule requires that covered financial institutions, among other things, adopt detailed programs, policies and procedures to protect Information Systems[1] and certain sensitive business and consumer information ("Nonpublic Information")[2] from cybersecurity threats. As we have noted, the Rule is narrower and less prescriptive than the original proposal from September 2016 (and largely the same as the second proposal from December 2016). Nonetheless, covered financial institutions now have less than six months to establish compliance with the first of the Cybersecurity Rule's requirements. This means covered financial institutions will quickly need to: (1) assess the current state of their information security programs and what modifications may be required based on the specific policies and controls required by the Rule; and (2) consider the new processes that may need to be created to meet the Rule's reporting, recordkeeping and certification requirements.

The following provides a summary of key obligations and issues under the Cybersecurity Rule. We also note, where applicable, how the new FAQs and other information from NYDFS may inform the requirements of the Rule, in particular with respect to certain ambiguities and potential implementation challenges that remained when the rule was finalized in mid-February.

OVERVIEW

The Cybersecurity Rule applies to "covered entities"—generally, entities subject to NYDFS authority under New York banking, insurance and financial services law, including, for example, commercial banks, foreign banks with

[1] An "Information System" is defined to include essentially any computer or networked electronic system: "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."

[2] "Nonpublic Information" is defined to include: (1) certain sensitive personal information, such as Social Security numbers, drivers' license numbers, and biometric data; (2) "business-related information," the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the covered financial institution; and (3) certain information created by, or derived from, a healthcare provider or an individual relating to medical conditions, the provision of health care to an individual or payment for the provision of health care.

New York State-licensed offices, mortgage brokers and servicers, small-loan lenders and money transmitters doing business in New York.

As noted above, the Rule is focused on the protection of Information Systems and Nonpublic Information. In this regard, the requirements imposed by the Rule can be divided into three categories of requirements and controls: (1) administrative requirements, such as written policies and procedures; (2) technical controls, such as encryption and multifactor authentication; and (3) notice, recordkeeping and reporting requirements. We address highlights of each below.

ADMINISTRATIVE REQUIREMENTS

Cybersecurity Program. The Cybersecurity Rule requires each covered financial institution to maintain a "cybersecurity program" designed to protect the confidentiality, integrity and availability of its Information Systems. This "core" requirement of the Rule is generally consistent with other standards (*e.g.*, the Gramm-Leach-Bliley Act) and best practices,[3] in that it requires that the cybersecurity program be designed to perform the core cybersecurity functions of identifying and assessing threats and risks, protecting Information Systems and Nonpublic Information from malicious use and unauthorized access and detecting, responding to and recovering from "Cybersecurity Events."[4] In a slight twist, the program must also be designed to fulfill applicable reporting obligations imposed by the Rule.

Of note, NYDFS confirmed in the FAQs that a covered financial institution may adopt the cybersecurity program of an affiliate "in whole or in part," but the covered financial institution's overall cybersecurity program must meet the requirements of the Cybersecurity Rule. In this regard, the covered financial institution itself (not the affiliate) must certify to compliance with the Rule. Nonetheless, NYDFS also notes that where a covered financial institution adopts an affiliate's program, the affiliate's program must be available to NYDFS for examination. This fact may complicate business decisions for some covered financial institutions, particularly where the affiliate is not already subject to NYDFS jurisdiction.

Written Cybersecurity Policy. As part of its cybersecurity program, a covered financial institution must have written cybersecurity policies, approved by a senior officer or its board of directors, that address a wide variety of security concepts, including data classification, asset inventory and device management, access controls and identity management, business continuity, network security, physical security, third-party service provider requirements and incident response procedures. As a result, a critical first step for covered financial institutions is to map their existing written information security policies to the Cybersecurity Rule to determine what if any additional policies and procedures may be necessary.

[3] Indeed, in the publication of the final rule in the State Register, NYDFS noted that it "continues to believe that the regulation is consistent with other standards," which was why NYDFS did not feel the need to further "harmonize" its rules with existing cybersecurity regimes. *See* N.Y. Stat. Reg. Vol. XXXIX, Issue 9 (Mar. 1, 2017), *available at* https://docs.dos.ny.gov/info/register/2017/march1/pdf/Rule%20Making%20Activities.pdf.

[4] "Cybersecurity Events" are 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."

Risk Assessment. A covered financial institution is also required to conduct periodic risk assessments that must inform the design of its cybersecurity program. In this regard, a covered financial institution must have a written policy and procedure for conducting risk assessments that must include, among other things, establishing criteria for evaluating and categorizing identified cybersecurity risks or threats and assessing the adequacy of existing controls in light of these identified risks. As discussed further below, the Rule provides covered financial institutions with one year to come into compliance with the risk assessment requirements (i.e., by March 1, 2018), which is six months after the required cybersecurity program and written policies must be in place. The FAQs, however, affirm that covered financial institutions "are generally not required to comply with, or incorporate into their cybersecurity programs, provisions of the regulation for which the applicable transitional period has not yet ended." With regard to the risk assessment specifically, NYDFS indicated that it "recognizes that in some cases there may be updates and revisions" to the program and policies incorporating the results of a future risk assessment.

Additional Policies and Procedures. The Cybersecurity Rule identifies a wide range of specific policies and procedures that a covered financial institution must have in place. These include:

- Written procedures, guidelines and standards related to *application security* to ensure the use of secure development practices for internally developed applications and to evaluate, assess and test the security of third-party applications;
- Risk-based policies, procedures and controls to *monitor* user activity and detect unauthorized access to, or use of, Nonpublic Information by such users;
- Policies and procedures for the *secure disposal* of Nonpublic Information, consistent with retention requirements under existing laws and regulations; and
- Written policies and procedures relating to *third-party service providers* that address, for example, risk assessments of, and minimum cybersecurity standards for, these third parties. Covered financial institutions must also have policies and procedures that address "due diligence and/or contractual protections" relating to service providers, including a service provider's use of multifactor authentication, and encryption and notice to the financial institution in the event of certain Cybersecurity Events. In the FAQs, NYDFS affirms that not all service providers are *required* to implement multifactor authentication and encryption when dealing with a covered financial institution. Instead, NYDFS notes that there is no "one-size-fits-all solution" created by the Cybersecurity Rule, and each covered financial institution must make a risk assessment regarding the appropriate controls "based on the individual facts and circumstances presented."

Incident Response Plan. A covered financial institution must also have a written incident response plan for material Cybersecurity Events. The plan must address a number of aspects of incident response, including, for example, roles, responsibilities and decision-making authority and processes for documenting and reporting Cybersecurity Events.

Chief Information Security Officer/Responsible Individual. The Cybersecurity Rule requires that a covered financial institution have a qualified individual (defined in the Rule as the "CISO") responsible for overseeing and implementing its cybersecurity program and enforcing its cybersecurity policy. (The Rule does not require that an individual actually hold the title CISO, but rather that an identified individual be designated responsible for the program.) The FAQs clarify that the CISO can be an employee of an affiliate, but the covered financial institution remains responsible for all requirements of the Rule, including ensuring that the CISO performs her obligations under the Rule. For example, the CISO must report at least annually to the board of directors on the cybersecurity program.

The covered financial institution must also have sufficient *cybersecurity personnel* in place to oversee the core functions of the cybersecurity program (i.e., identify risks, and prevent, detect, respond and recover from cybersecurity threats, as applicable). The covered financial institution must provide these personnel with appropriate training and verify that they take steps to maintain current knowledge of changing cybersecurity threats and countermeasures. More broadly, the covered financial institution must provide all personnel with regular *cybersecurity awareness training*.

TECHNICAL CONTROLS

While the Cybersecurity Rule is clearly focused on administrative controls and processes and there are far fewer technical controls mandated by the Rule, the Rule's technical controls may in practice be far more prescriptive. As we noted previously, NYDFS did not provide additional clarity regarding the nature and scope of certain of these requirements, such as the encryption and multifactor authentication requirements, in the final revisions to the Cybersecurity Rule. NYDFS has provided no further guidance in the FAQs either.

Penetration Testing and Vulnerability Assessments. A covered financial institution's cybersecurity program must include monitoring and testing to assess the effectiveness of the program. This monitoring and testing can be *either*: (1) continuous monitoring, or using other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities; or (2) annual penetration testing, based on relevant identified risks in accordance with the risk assessment, *and* bi-annual vulnerability assessments. In the FAQs, NYDFS elaborates that "continuous monitoring" entails "the ability to continuously, on an ongoing basis, detect changes or activities . . . that may create or indicate the existence of cybersecurity vulnerabilities or malicious activity." The FAQs also illustrate these requirements by contrast. For example, the FAQs indicate that manual review of logs and firewall configurations would not be considered "effective continuous monitoring." Nonetheless, it appears that that NYDFS believes that "continuous system monitoring" is an appropriate alternative to periodic penetration testing and vulnerability assessments.

Multi-factor Authentication. The Cybersecurity Rule appears to push beyond some industry standard expectations for the use of multifactor authentication, although the actual requirements are to be ostensibly based on a covered institution's risk assessment. Specifically, a covered financial institution is required to use "effective" controls, which may include multifactor authentication or risk-based authentication, to protect against unauthorized access to Nonpublic Information or Information Systems. Nonetheless, multifactor authentication is specifically required for access to the covered financial institution's internal networks from external networks, unless the CISO "has approved in writing the use of reasonably equivalent or more secure access controls."

This provision was not clarified in the final rule, and there is no discussion of it in the FAQs. As a result, it remains unclear if NYDFS expects the requirement for multifactor authentication to apply to employee remote access, customer access to online accounts or both.

Encryption of Nonpublic Information. One of the most significant requirements of the Cybersecurity Rule is the requirement that covered entities must implement controls, including encryption, to protect Nonpublic Information held or transmitted by the covered financial institution both in transit over external networks and at rest. Under the Rule, *if* a covered financial institution determines that encryption is infeasible, the covered financial institution is permitted to secure such information using compensating controls reviewed and approved by the CISO. As we noted previously, the Rule is not clear as to whether encryption is a mandate and whether compensating controls can only be adopted as an alternative when encryption is "infeasible."

The FAQs offer no further insight on this point, although NYDFS did state in its State Register notice accompanying the final rule that it did not further modify the encryption requirement because it believes in "the importance of encryption as a key cybersecurity control." NYDFS also noted, however, that it believes the final rule also provides "flexibility for Covered Entities to evaluate, in light of their Risk Assessment, the scope and means of feasibly implementing encryption controls." Notably, NYDFS also stated that it considers leased lines (i.e., dedicated connections between a covered financial institution and some other party) to constitute "external networks" for purposes of this requirement.

Audit Trails. A covered financial institution is also required to securely maintain systems, based on its risk assessment, in order to reconstruct material financial transactions sufficient to support normal operations and obligations (and maintain such records for five years). Covered entities are also required to maintain "audit trails" to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the covered financial institution (and maintain such records for three years).

Access Privileges. A covered financial institution must limit user access privileges to systems that provide access to Nonpublic Information and periodically review those access privileges.

NOTIFICATIONS AND REPORTING

Covered financial institutions have significant reporting obligations under the Rule, including: (1) an annual report by a covered financial institution's CISO to its board of directors or equivalent governing body on the financial institution's cybersecurity program and "material" cybersecurity risks (with such report, along with other documents relating to the cybersecurity program, being made available to NYDFS upon request); and (2) notices to NYDFS no later than 72 hours "from a determination" that a Cybersecurity Event has occurred that either: (A) impacts the covered financial institution and requires notice to a "government body, self-regulatory agency or any other supervisory body"; or (B) has a "reasonable likelihood of materially harming any material part of the normal operation(s)" of the financial institution.

The FAQs largely repeat these requirements without any commentary, although NYDFS notes that "even if [an] attack is not successful," it may constitute a reportable event. This statement appears to significantly broaden the scope of the notification requirement, as NYDFS apparently believes that unsuccessful attacks could have a

reasonable likelihood of materially harming a covered financial institution. As a result, covered financial institutions will have to determine what types of events will require notice to NYDFS and incorporate these considerations into their incident response plans.

NYDFS also notes in the FAQs that it will "at a later date" provide a secure reporting tool for notices of Cybersecurity Events required to be provided to NYDFS, but that for now covered entities are required to send such notices to the supervisory staff to which the covered financial institution typically reports.

Certification and Documentation of Remedial Efforts. The requirement for annual certifications of compliance is likely to cause significant challenges for many covered financial institutions. Specifically, each covered financial institution must certify its compliance with the Cybersecurity Rule (as opposed to, for example, certifying that the covered financial institution has implemented policies and procedures designed to meet the requirements of the Rule). Covered financial institution are also required to maintain "all records, schedules and data supporting" the certification for up to five years. Perhaps further complicating this certification requirement, the Cybersecurity Rule requires that covered financial institutions document remedial efforts to address "areas, systems or processes that require material improvement."

In the FAQs, NYDFS states that it "expects full compliance" with the Rule while also stating that a covered financial institution "*may not* submit a certification . . . unless [it] is in compliance with all applicable requirements" of the Cybersecurity Rule at the time of certification (emphasis added). By requiring covered financial institutions to both certify their full compliance and document areas requiring improvement, NYDFS risks giving covered entities a Hobson's choice: either document for inspection by NYDFS what could be deemed indicia of noncompliance or forego efforts to continually improve and update the enterprise's information security program.

OTHER CONSIDERATIONS AND TIMING

As noted, the Cybersecurity Rule takes effect in phases, with the first set of requirements coming into force on August 28, 2017 and then additional requirements one year, 18 months, and two years following the March 1, 2017 effective date. NYDFS summarizes these transition periods at http://dfs.ny.gov/about/cybersecurity.htm. The FAQs helpfully confirm that at the first annual certification (due February 15, 2018), a covered financial institution is only required to certify to the requirements for which the transitional period has terminated prior to that date. **Appendix A** below provides a more detailed summary of the phased compliance periods.

Now that NYDFS has provided guidance in the form of the FAQs, covered financial institutions should not expect much additional clarification from NYDFS in the short term on its precise expectations under the Cybersecurity Rule. As we have noted before, implementation is likely to continue to be challenging, including because this is a "first-in-the-nation cybersecurity regulation" issued by a state financial regulator.

Contacts:

Nathan D. Taylor
(202) 778-1644
ndtaylor@mofo.com

Adam J. Fleisher
(202) 887-8781
afleisher@mofo.com

Appendix A
Key Compliance Dates

By **August 28, 2017**, covered financial institutions must be in compliance with the following:

- The requirement to have a cybersecurity program and cybersecurity policies and procedures;
- The designation of a CISO;
- The access privileges requirement;
- The requirements relating to cybersecurity personnel and cybersecurity intelligence;
- The requirement for an incident response plan; and
- The requirement to provide notice of certain cybersecurity events to NYDFS and to document remedial efforts.

The first certification to compliance with the Rule is required by **February 15, 2018**.

By **March 1, 2018**, covered financial institutions must be in compliance with the following:

- The requirement that the CISO report to the board of directors on the cybersecurity program;
- The penetration testing and vulnerability assessment requirements;
- The risk assessment requirement (i.e., the covered financial institution must have completed its first risk assessment under the Cybersecurity Rule);
- The multifactor authentication requirements; and
- The cybersecurity awareness training requirement.

By **September 3, 2018**, covered financial institutions must be in compliance with the following:

- The audit trail requirements;
- The application security requirements;
- The data retention requirements;
- The monitoring requirements; and
- The encryption requirements.

Finally, by **March 1, 2019**, covered financial institutions must be in compliance with the third-party service provider provisions.

Client Alert

Financial Services Team

California		New York	
Alexis A. Amezcua	(415) 268-6557	James M. Bergin	(212) 468-8033
Elizabeth Balassone	(415) 268-7585	Meghan E. Dwyer	(212) 336-4067
Roland E. Brandel	(415) 268-7093	David J. Fioccola	(212) 336-4069
Sarah Nicole Davis	(415) 268-7478	Marc-Alain Galeazzi	(212) 336-4153
Henry M. Fields	(213) 892-5275	Adam J. Hunt	(212) 336-4341
Joseph Gabai	(213) 892-5284	Jessica Kaufman	(212) 336-4257
Angela E. Kleine	(415) 268-6214	Mark P. Ladner	(212) 468-8035
Jim McCabe	(415) 268-7011	Jiang Liu	(212) 468-8008
James R. McGuire	(415) 268-7013	David H. Medlar	(212) 336-4302
Mark David McPherson	(212) 468-8263	Barbara R. Mendelson	(212) 468-8118
Ben Patterson	(415) 268-6818	Michael B. Miller	(212) 468-8009
Sylvia Rivera	(213) 892-5734	Judy Man Ni Mok	(212) 336-4073
Nicholas Alan Roethlisberger	(415) 268-7534	Jeffrey K. Rosenberg	(212) 336-4130
Grant C. Schrader	(415) 268-6635	Mark R. Sobin	(212) 336-4222
William L. Stern	(415) 268-7637	Joan P. Warrington	(212) 506-7307
Nancy R. Thomas	(213) 892-5561		
Lauren Lynn Wroblewski	(415) 268-6458		

Washington, D.C.		Washington, D.C. (continued)	
Rick Fischer	(202) 887-1566	Donald C. Lampe	(202) 887-1524
Adam J. Fleisher	(202) 887-8781	Jeremy R. Mandell	(202) 887-1505
Natalie A. Fleming Nolen	(202) 887-1551	Amanda J. Mollo	(202) 778-1609
Calvin D. Funk	(202) 887-6930	Obrea O. Poindexter	(202) 887-8741
Julian E. Hammar	(202) 887-1679	Ryan J. Richardson	(202) 887-8761
Oliver I. Ireland	(202) 778-1614	Sean Ruff	(202) 887-1530
Crystal N. Kaldjob	(202) 887-1687	Trevor R. Salter	(202) 887-1527
Steven M. Kaufmann	(202) 887-8794	Nathan D. Taylor	(202) 778-1644

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for 13 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.