Hogan Lovells

# New York Department of Financial Services Cybersecurity Rules Revised and Delayed

30 December 2016

There is significant interest in the New York Department of Financial Services' (NYDFS or the Department) proposed cybersecurity regulations (the Initial Rules) that were due to become effective January 1, 2017. NYDFS issued an update to the Rules (the Updated Rules) on December 28, 2016, and extended the effective date until March 1, 2017. The Updated Rules will apply to over 3,000 financial institutions—banks, insurance companies, and other institutions operating under a license or authorization of New York state law (the Covered Entities), with certain exemptions.

The Initial Rules, announced on September 13, 2016, would have required Covered Entities to, among other things:

- establish a cybersecurity program;
- adopt a written cybersecurity policy;
- designate a Chief Information Security Officer (CISO) responsible for overseeing the policy and program, and reporting to the Board (or the institution's equivalent body or person) at least bi-annually;
- establish and maintain policies, controls, and due diligence designed to ensure the security and integrity of systems and nonpublic information held or accessed by third-party providers;
- conduct periodic penetration testing, vulnerability assessments, and risk assessments of the institution's information systems;
- encrypt all Nonpublic Information in transit and at rest, with time-limited exceptions for use of compensating controls;
- limit retention of Nonpublic Information;
- report 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") that meet certain broad criteria;
- establish an incident response plan to respond to and recover from a Cybersecurity Event;
- ensure that the Board (or its equivalent) will review annually the cybersecurity policy; and
- certify—either by the Chair of the Board or a Senior Officer, annually and in writing—that the cybersecurity program complies with the regulation.

## Major Changes in the Revised Regulations

Following a hearing in late December and after several written complaints from covered banks and insurance companies, NYDFS advised that it would update the Initial Rules. The Updated Rules were announced on December 28, 2016. To allow affected institutions sufficient time to implement the new requirements, the effective date is now March 1, 2017, instead of January 1, 2017, and the Updated Rules provide a series of staggered implementation dates beyond the effective date.

In addition to several minor changes to the Initial Rules—including, for instance, the newly added definition of "Third Party Service Provider"—the Updated Rules provide a number of notable changes and clarifications:

- **Risk-Based Approach.** Rather than a "one-size-fits-all" approach, many requirements for both the cybersecurity program and the cybersecurity policy (or policies) are now explicitly tied to the institution's Risk Assessment. For example, requirements related to an institution's vulnerability and penetration testing, audit trail capabilities, and use of encryption, and certain multi-factor authentication rules are also now explicitly based on the risks and other issues identified in the Risk Assessment, which is more fully described below.
- **The Risk Assessment**. The Initial Rules provided that the Risk Assessment would be conducted "at least annually" and must, among other things, "justify" how identified risks would be mitigated or accepted, and "assign[] accountability for the identified risks." The Initial Rules also appeared to encompass all of a Covered Entity's information systems, regardless of whether those systems contained or utilized Nonpublic Information. Pursuant to the Updated Rules, Covered Entities must conduct a "periodic Risk Assessment" that is "sufficient to inform the design of the cybersecurity program" (as opposed to "at least annually") which must be "updated as reasonably necessary to address changes" to the institution's systems, Nonpublic Information, and operations, and must be able to respond to changing technological developments, evolving threats, and the particular risks facing the entity. In a likely cause for relief among compliance officers and information security officers, there is no explicit "justification" requirement or rule to assign specific accountability for cybersecurity issues. Nevertheless, the Risk Assessment must still describe how the risks will be mitigated or accepted, and how those risks will be addressed.
- **Board-Level Expectations.** The Initial Rules called for Board (or its equivalent) review of the cybersecurity policy at least annually, with approval by a Senior Officer. In the Updated Rules, this requirement has been replaced by only the requirement that the policy be approved by the Board (or its equivalent) *or* an appropriate Board committee *or* a Senior Officer.
- **The CISO and Cybersecurity Personnel.** Many financial institutions had expressed concern regarding the Initial Rule's requirement that institutions expressly designate an individual as a Chief Information Security Officer, or CISO. Under the Updated Rule, which still uses the CISO terminology, the role is defined by function, rather than title. The CISO's report is also now required at least annually, rather than bi-annually. The revisions also clarify an ambiguity in the initial iteration of the Rules, which had provided that Covered Entities must "employ" cybersecurity personnel, but that they may also use qualified third-parties "to assist in complying" with the regulatory requirements. The Updated Rules make

clear that Covered Entities must "utilize qualified cybersecurity personnel of the Covered Entity, an affiliate, or a Third Party Service Provider."

- **Encryption.** The Initial Rules had a sunset provision for use of compensating controls and made encryption a de facto default requirement for data in motion and at rest. The Updated Rules make encryption dependent on the risk assessment, and allows use of compensating controls more generally (subject to initial CISO review and approval, with annual review thereafter).
- **Materiality**. Many financial institutions are subject to cyber-events on a daily basis–- scans, "cyber-sniffing," and other unwelcome events—though most are easily screened and prevented. Reporting and otherwise accounting for such routine events would be incredibly burdensome, and likely would divert precious resources from addressing other more serious cyber-related risks. Apparently recognizing this, the Update Rules include a "materiality" threshold for certain provisions. For instance, as part of its cybersecurity program, an institution must have an incident response plan to respond to and recover from cybersecurity events. As originally drafted in the Initial Rules, the incident response plan was required to cover "any Cybersecurity Event affecting the confidentiality, integrity, or availability" of the institution's systems or operations, which arguably might include forgotten passwords, isolated (and unsuccessful) email scams, and the like. As revised, the Updated Rules provide that the incident response plan must be designed to respond to and recover from "any Cybersecurity Event *materially* affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations." Similarly, the CISO now reports on "material" cybersecurity risks.
- **The 72-Hour Notice Rule**. Along the same principles, several financial institutions had raised objections to the requirement to provide notice to NYDFS within 72 hours of certain types of cybersecurity events. While the Department decided to retain the 72 hour time frame in the Updated Rules, it limited the requirement to (1) those events for which the Covered Entity is required to provide notice to other regulators, self-regulatory agencies, or supervisory bodies; and (2) events that have "a reasonable likelihood of materially harming any material part of the normal operations" of the institution. And importantly, the 72-hour clock now runs from the time that the Covered Entity determines that the event meets one of these two criteria, not from when the Covered Entity first becomes aware of the event. NYDFS removed the provision mandating reports of events involving "actual or potential unauthorized tampering with, or access to, or use of, Nonpublic Information," which would cast an incredibly large net but would be unlikely to yield additional useful information to law enforcement or regulators.
- **Nonpublic Information definition**. The Updated Rules narrow key aspects of the definition of Nonpublic Information relating to "individuals" (certain business related information covered under the definition is largely unchanged). In the Initial Rules, the definition included "any information that could be used to distinguish or trace an individual's identify including, but not limited to, any information that is linked or linkable to an individual." That aspect of the definition has been modified to follow approaches more typically seen in other state and federal laws, focusing on various identifiers "in combination with" more traditional sensitive information categories such as Social Security numbers, driver license numbers, account information and biometric records. On the other hand, the Updated Rules expand the definition of healthcare information to include such

information "in any form or medium." This expansion is in tension with the introduction to the definition, which states that Nonpublic Information means "all electronic information."

- **Reliance on Affiliates.** The Updated Rules include a new provision that allows Covered Entities to meet cybersecurity program requirements by adopting those of an affiliate, so long as the affiliate's program meets the requirements of the NYDFS Updated Rule. A Covered Entity may also use the CISO of an affiliate.
- **Confidentiality and Transparency Provisions**. The Updated Rules provide for a completely new section, titled "Confidentiality," set forth at Section 500.18 (subsequent sections were renumbered), which provides: "Information provided by a Covered Entity pursuant to this Part is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law." This provision may have a number of implications—some of which may be yet unresolved and the subject of later disputes—but the primary aim appears to be insulating these required reports, assessments, and policies from being available for discovery in civil litigation. In other words, this Confidentiality provision offers Covered Entities the protection that, while these incident reports, assessments, and other mandatory documents will be required for regulatory purposes, they will not be available for use by plaintiffs' attorneys seeking to use these materials in lawsuits against the institutions. This new provision may also insulate those materials from disclosure under New York's Freedom of Information Law. The new Confidentiality provision is accompanied by an explicit and broad transparency requirement: the Updated Rules include new language in Section 500.02 requiring Covered Entities to make available to NYDFS "upon request" all documentation and information "relevant" to a Covered Entity's cybersecurity program.
- **New Exemptions.** The Updated Rules provide additional exemptions from several of the Rule's requirements. Several requirements, including the CISO, penetration testing, audit trail, encryption, and incident response plan rules will not apply to Covered Entities with fewer than 10 employees (including contractors), or with less than $5M in gross annual revenue for each of the last three fiscal years, or with less than $10M in year-end assets. Importantly, the Updated Rules provide that employees, agents, designees, and other representatives of Covered Entities, who are themselves Covered Entities, need not develop their own cybersecurity programs if they are covered by the program of the Covered Entity whom they represent. Finally, Covered Entities that do not directly or indirectly use, operate, maintain, or control an information system, and that does not directly or indirectly control, own, access, generate, receive or possess Nonpublic Information, are exempt from several requirements, although they are still required to perform a Risk Assessment, have policies regarding their third-party service providers, and have limits on data retention. All Covered Entities claiming an exemption must submit a Notice of Exemption Form to the Department of Financial Services.

This is not an exhaustive list of updates, many of which are particular to specific provisions. For instance, the Covered Entity must provide for regular cybersecurity awareness training for all personnel, but there is no longer an explicit requirement that all of its personnel attend the training. And while Section 500.13 of the Updated Rules still require a Covered Entity to have policies and procedures for periodically and securely destroying Nonpublic Information, these data retention limitations have been substantially revised to broaden the permitted uses for which such data can be retained and to exempt Covered Entities from these requirements when targeted destruction of such data is impractical.

We provide a comparison of the Initial Rules and the Updated Rules here.

## Timing and Implementation

As noted above, NYDFS has moved back the planned Effective Date of the regulations to March 1, 2017. And Covered Entities will have 180 days from this date—that is, by August 28, 2017—to comply with most of the requirements. The rule also allows for certain other compliance dates:

- **By February 15, 2018:** Initial Certification of Compliance submissions must be filed
- **By March 1, 2018 (1 year after the Effective Date):** Initial CISO Report; Penetration Testing and Vulnerability Assessments; Risk Assessment; Multi-Factor Authentication; and Training
- **By September 1, 2018 (18 months after the Effective Date):** Audit Trail; Application Security; Limitations on Data Retention; Monitoring of Authorized Users; and Encryption of Nonpublic Information
- **By March 1, 2019:** Third-Party Service Provider Security Policy

Importantly, the Updated Rules are subject to another 30-day public review and comment period. It is highly likely that the NYDFS final review will focus on comments not raised during the original comment period and on the changes to the Rules provided in the Updated Rule. As a result, while there might still be modifications to this December 28 proposal, we anticipate that any additional changes will be minor, if any.

## Key Takeaways

The NYDFS's action moves it closer to the fruition of the objectives it announced over a year ago. However, given the serious obligations that the NYDFS cybersecurity regulations will impose upon covered financial institutions, and the burdens and costs stemming from those obligations, NYDFS's decision to revisit the regulations and delay implementation is a welcome development. That said, covered institutions should keep a few things in mind.

**Winter is (Still) Coming.** The Updated Rules will be followed by a 30-day period of public comment and review, and its effective date is now March 1, 2017, instead of January 1, 2017. Even with the staggered compliance implementation/transition dates, this is a short implementation period in which to confirm compliance with such far-reaching rules.

**Know Your Risk.** Many of the provisions of the Updated Rules are now explicitly tied to the institution's Risk Assessment. For Covered Entities, this is a sliver of good news: the rules are not "one-size-fits-all" and instead are calibrated to the risks from, among other things, the institution's products and services; its market; its geographic footprint; industry-specific threats; its business model and structure; and, of course, the technology and information that it collects, stores, and uses. This should enable a Covered Entity's cybersecurity program and policy to maintain its focus on real risks, and will therefore serve necessary operational as well as regulatory compliance needs. But this also likely comes with the expectation that institutions will invest significant attention to their Risk Assessments, and ensuring that their programs, internal controls, and other policies hug the shoreline of what is detailed in those Risk Assessments. Curiously, under the

implementation/compliance schedule, Covered Entities must develop their Risk Assessments no later than March 1, 2018 (one year after the effective date), but certain other rules, for instance, the cybersecurity program, the cybersecurity policy, and the access privilege limitations—all of which are predicated on the issues and concerns identified in the Risk Assessment—must be in place by August 28, 2017. This may warrant a comment or request for clarification during the comment period.

**Other Rules Are in Play, and More Are on Their Way.** While New York is the first state to attempt to regulate cybersecurity itself with a broad-based regulatory regime, there are other legal obligations and regulatory expectations surrounding cybersecurity that are likely applicable to many the Updated Rule's Covered Entities.

For instance, in October 2016 the U.S. federal banking agencies issued an advance notice of proposed rulemaking regarding cyber risk management standards, and such regulations are presumably forthcoming after the comment period, which closes on January 17, 2017. In addition, as we have previously reported, the Financial Crimes Enforcement Network (FinCEN) announced its expectation that financial institutions report several types of cyber events in Suspicious Activities Reports (SARs). The Federal Trade Commission has taken several enforcement actions regarding data security measures, even where no actual breach has occurred. The Financial Industry Regulatory Authority (FINRA) has publicly stated that cybersecurity will be one of its enforcement priorities in 2017. In March 2016, the Consumer Financial Protection Bureau took action against an online payments platform relating to the company's public statements regarding its security policies. In certain circumstances, shareholders or customers may allege that a company's failures to maintain proper cybersecurity measures should render them liable in a civil suit. Further, for Covered Entities engaged in multiple jurisdictions, other states may follow the NYDFS example and implement their own cybersecurity rules. And for insurers, the National Association of Insurance Commissioners (NAIC) is working on an Insurance Data Security Model Law.

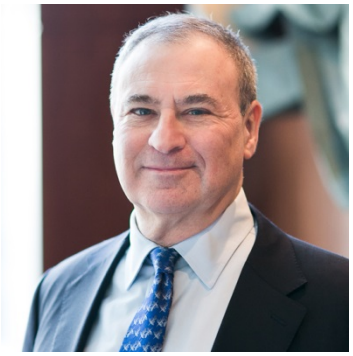
In short, although NYDFS has relaxed and clarified some aspects of its proposed regime, institutions should still be aware of and should begin to prepare for their obligations under the Updated Rules, other regulatory and legal expectations, and potential liabilities. If further revisions occur, or if there are other developments from other regulatory agencies, state or federal, we will let you know.

* * * * * * *

Please let us know if you have any questions, or if we can be of assistance on these matters.

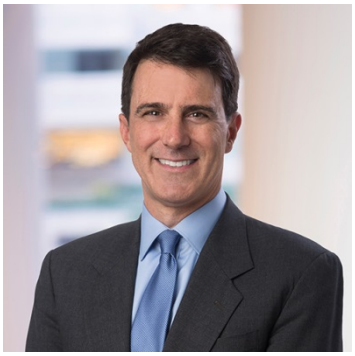
## Contacts


**Aleksandar Dukic**
Partner, Washington, D.C.
Tel +1 202 637 5466
aleksandar.dukic@hoganlovells.com

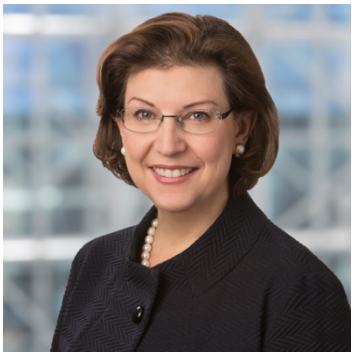


**Marc Gottridge**
Partner, New York
Tel +1 212 909 0643
marc.gottridge@hoganlovells.com

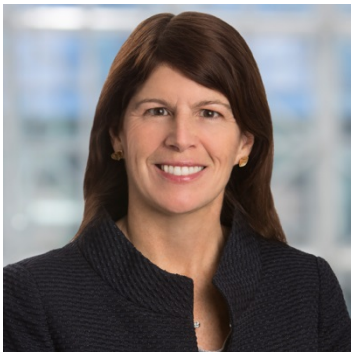
**Deen Kaplan**
Partner, Washington, D.C.
Tel +1 202 637 5799
deen.kaplan@hoganlovells.com



**Gregory Lisa**
Partner, Washington, D.C.
Tel +1 202 637 3647
gregory.lisa@hoganlovells.com



**Harriet Pearson**
Partner, Washington, D.C. and New York
Tel +1 202 637 5477
+1 212 918 5548
harriet.pearson@hoganlovells.com



**Beth Peters**
Partner, Washington, D.C.
Tel +1 202 637 5837
beth.peters@hoganlovells.com

**Richard Schaberg**
Partner, Washington, D.C.
Tel +1 202 637 5671
richard.schaberg@hoganlovells.com

**Timothy Tobin**
Partner, Washington, D.C.
Tel +1 202 637 6833
timothy.tobin@hoganlovells.com

**Laura Biddle**
Counsel, Washington, D.C.
Tel +1 202 637 5419
laura.biddle@hoganlovells.com

**Stephenie Gosnell Handler**
Associate, Washington, D.C.
Tel +1 202 637 5540
stephenie.handler@hoganlovells.com

**Paul Otto**
Senior Associate, Washington, D.C.
Tel +1 202 637 5887
paul.otto@hoganlovells.com