Hogan Lovells

The "Final Final" Is Here: NYDFS Cybersecurity Regulations

23 February 2017

As Hogan Lovells previously reported, the New York State Department of Financial Services (NYDFS) has launched a significant initiative to impose detailed cybersecurity requirements on covered financial institutions. NYDFS announced initial proposed rules in 13 September 2016; after industry complaints and a public hearing, NYDFS revised the rules in a second iteration on 28 December 2016, with a planned effective date of 1 March 2017. The revised rules were subject to another public comment period which closed in late January 2017.

Last week, NYDFS announced the final form of these rules including a handful of changes made after the latest public comment period. The Final Rules, published here, come into effect on 1 March 2017. As with the December proposal, the regulations impose staggered requirements for covered institutions (also referred to as Covered Entities); that timeline—which imposes obligations as early as 28 August 2017—has not changed.

What Do You Need to Know Now?

As a first step, determine whether your financial institution is covered. The scope of the regulations is quite broad, but there are exemptions (some of which are limited exemptions only). And even those Covered Entities that enjoy an exemption must still file a certificate of exemption with NYDFS within 30 days of that determination. As a corollary to this, if a Covered Entity ceases to qualify for an exemption as of its most recent fiscal year end, the Covered Entity has 180 days to come into compliance.

Second, assemble your team. The staggered implementation timeline requires that a Chief Information Security Officer (CISO) be designated no later than 28 August 2017. For most financial institutions, the reality is that this likely is more than a one-person job. And, importantly, the cybersecurity requirements apply enterprise-wide, so whether designated as "cybersecurity personnel" or otherwise, the NYDFS obligations will affect everyone in the institution.

Next, understand (and update) your risk profile. The staggered implementation schedule provides that the mandated Risk Assessment is due by 1 March 2018 (within one year of the effective date). But other items that depend upon the Risk Assessment—such as the cybersecurity program, the cybersecurity policy, and access privilege limitations—must be in place by 28 August 2017.

The full set of initial compliance requirement dates for the Final Rules are as follows:

Date	Compliance Requirement(s)
August 28, 2017	Cybersecurity Program; Cybersecurity Policy; CISO; Access Privileges; Cybersecurity Personnel and Intelligence; Incident Response Plan; Notice of Cybersecurity Event; Exemptions
February 15, 2018	Initial Certification of Compliance
March 1, 2018	Initial CISO Report; Penetration Testing and Vulnerability Assessments; Risk Assessment; Multi-Factor Authentication; Cybersecurity Awareness Training
September 1, 2018*	Audit Trail; Application Security; Limitations on Data Retention; Monitoring of Authorized Users; Encryption of Nonpublic Information
March 1, 2019	Third-Party Service Provider Security Policy

* September 1, 2018 is a Saturday. New York law provides that when a compliance date falls on a weekend or holiday, the due date is the next business day – in this case, Tuesday, September 4, 2018 (as Monday the 3rd is Labor Day).

What Has Changed Since the December Announcement?

As we had predicted in our 30 December alert, NYDFS adopted only modest revisions from the December version into the Final Rules. Other than a few minor clarifications and renumberings, the 28 December NYDFS proposal is mostly intact. For the records retention requirements, covered institutions must still maintain records designed to reconstruct material financial transactions to support the institution's operations and obligations for five years. But the finalized regulations have relaxed the audit trail rules; Covered Entities must now keep them for three years instead of five. (Section 500.6(b)). As a practical matter, however, Covered Entities may wish to keep them for five years, given that many other records relating to compliance with these rules are subject to a five-year retention requirement.

There are other helpful clarifications. For instance, as we noted in our previous alert, the rules require that covered institutions must report, within 72 hours of determining that the cybersecurity event is reportable, the following types of events: (1) 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. (Section 500.17(a)). The Final Rules now clarify that this first category of reportable incidents—those reported to other agencies—are limited to events "impacting the Covered Entity." Another notable clarification in the finalized regulations provides that the annual certification of compliance due to the Superintendent each 15 February shall cover the prior calendar year.

The most notable changes appear in the Exemptions section of the Final Rules. Previously, the December iteration of the rules allowed a limited exemption for Covered Entities with fewer than 10 employees, including independent contractors. As revised, that provision now applies the exemption to those with "fewer than 10 employees, including any independent contractors of the Covered Entity or its Affiliates located in New York or responsible for business of the Covered Entity." (Section 500.19(a)(1)). Similarly, the limited exemption applicable to those with less than US$5M in gross revenue for each of the last three fiscal years is further expanded: now, Covered Entities with less than US$5M in gross revenue from its New York business operations (or its affiliates' operations) meet the exemption. In other words, certain larger financial institutions with a smaller New York "footprint" may qualify for

either (or both) of these new limited exemptions. The Final Rules also added another limited exemption for certain captive insurance companies that do not control, use, or possess Nonpublic Information beyond that information relating to its parent and affiliate companies.

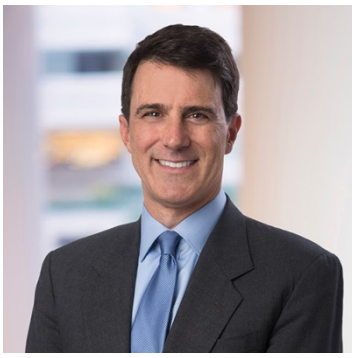
Importantly, the types of entities listed above receive only limited exemptions under the regulations. For instance, those institutions with less than US$5M in gross annual revenue, or those with fewer than 10 employees located in New York (or responsible for the Covered Entity's business) are exempt from several provisions, but subject to others: such institutions must still have a cybersecurity program; a cybersecurity policy; limitations on access privileges; a risk assessment; third-party service provider security policies; and policies and procedures for data retention and disposal. The Final Rules also provide new exemptions for certain charitable annuity societies, risk retention groups, and accredited or certified reinsurers.

What Should You Expect Next?

Other regulatory and law enforcement agencies likely will be coming out with their own cybersecurity rules, regulations, best practices principles, and compliance expectations. Some of these will have the force of law, and others may be less defined, but will nonetheless place important demands on financial institutions. Financial institutions and those who serve them should make sure to stay abreast of these developments.

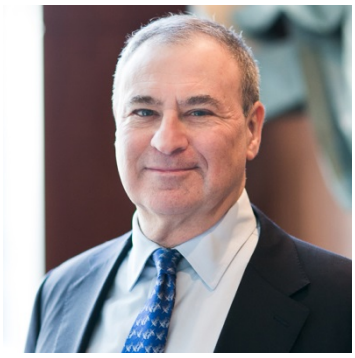
Hogan Lovells' market-leading team of cybersecurity and financial regulatory legal and technical professionals brings deep experience in the financial services and other industry sectors. We provide clients a wide range of regulatory compliance and other advisory services, as well as incident response and enforcement representation. We have significant experience in dealing with the New York Department of Financial Services, banking regulators, the Federal Trade Commission, the Consumer Financial Protection Bureau, other regulatory agencies, and federal and New York state criminal law enforcement authorities. Please let us know if you have any questions, or if we can be of assistance in these matters.

Contacts



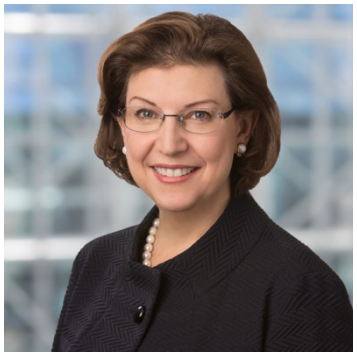
Gregory Lisa
Partner, Washington, D.C.
Tel +1 202 637 3647
gregory.lisa@hoganlovells.com

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

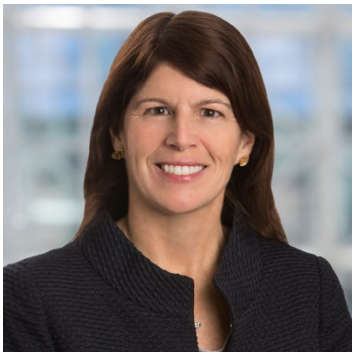


Marc Gottridge
Partner, New York
Tel +1 212 909 0643
marc.gottridge@hoganlovells.com

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



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

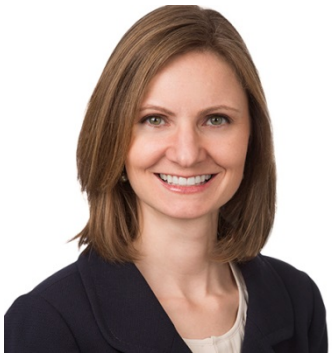


Beth Peters
Partner, Washington, D.C.
Tel +1 202 637 5837
beth.peters@hoganlovells.com

Richard Schaberg
Partner, Washington, D.C.,
New York
Tel +1 202 637 5671
Tel +1 212 918 3000
richard.schaberg@hoganlovells.com

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

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



Stephenie Gosnell Handler
Senior 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