Client Alert

February 22, 2017

One of a Kind: NYDFS Cyber Rule Finalized, Effective March 1, 2017

By Nathan D. Taylor and Adam J. Fleisher

The closely watched New York State Department of Financial Services (NYDFS) cybersecurity standards for covered financial institutions are now final and take effect March 1, 2017 in less than a week. The final rule largely tracks the second proposed rule issued in December 2016, which we discussed in our client alert. As a result, the final rule is narrower and less prescriptive than the original proposal, but will still present challenges, especially for financial institutions that do not have mature cybersecurity processes and controls in place.

It was not clear what the steps the NYDFS would take following its December 2016 proposal (*e.g.*, whether the NYDFS would issue another proposal for comment). The announcement last week by Governor Andrew Cuomo and the NYDFS affirms that NYDFS is moving full steam ahead, with limited substantive revisions and without providing covered entities much time to comply. Critically, the *timing* of the final rule is unchanged; its effective date is March 1, 2017, with the first annual certification of compliance due February 15, 2018. The phased compliance periods for specific requirements are also unchanged as well. The final rule generally will apply to all entities subject to the authority of NYDFS under New York banking, insurance and financial services law, including commercial banks, foreign banks with New York State-licensed offices, mortgage brokers and servicers, small-loan lenders and money transmitters doing business in New York.

In light of the final rule's impending effective date, covered financial institutions will need to: (1) promptly assess the current state of their information security programs and what modifications may be required based on the specific controls required by the rule; and (2) consider the policies, procedures and mechanisms that may need to be created to meet the rule's reporting, recordkeeping and certification requirements. Potential implementation challenges that we previously identified remain, and may be exacerbated by the rapidly approaching effective date. In particular, covered entities need to understand the following:

- **Ambiguities in the Final Rule.** In finalizing the rule, the NYDFS did not provide any additional clarity regarding the nature and scope of certain of the prescriptive requirements, such as encryption and multifactor authentication. For example, while covered entities are required, based on their risk assessments, to "implement controls, including encryption," to protect "nonpublic information" in transit and at rest, 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." In addition, it should be noted that the definition of "nonpublic information," while narrowed to include only sensitive personal information, such as Social Security numbers and biometric data, still includes certain "business-related information," which needs to be incorporated into any analysis of the appropriate use of encryption by each covered entity.

  The multifactor authentication requirement also remains unchanged from the second proposed rule. As a result, it is not clear if the NYDFS expects the requirement for multifactor authentication for access to

"internal networks from an external network" to apply to employee remote access, customer access to online accounts or both. The final rule does include minor modifications to the penetration testing requirements (including revising the definition of "penetration testing" to eliminate the apparent requirement that such testing be done without authorization), but the rule does not offer further clarity on why covered entities are required to *either* engage in continuous monitoring and testing of the effectiveness of their cybersecurity programs *or* to conduct an annual penetration test and bi-annual vulnerability assessments—in other words, what the NYDFS contemplates would make these two discrete sets of controls interchangeable.

- **Reporting.** Covered entities will have significant reporting obligations, including: (1) an annual report by a covered entity's CISO to the covered entity's board of directors or equivalent governing body on the entity's cybersecurity program and "material" cybersecurity risks (with such report, along with other documents relating to the cybersecurity program, made available to the NYDFS upon request); and (2) notices to the NYDFS no later than 72 hours "from a determination" that a cybersecurity event has occurred that either: (A) impacts the covered entity 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 covered entity. Covered entities will have to determine what types of events will require notice to the NYDFS under these provisions and incorporate these considerations into their incident response plans.

- **Certification.** The requirement for annual certifications of compliance remains unchanged and is likely to cause significant challenges for many covered entities. Specifically, each covered entity must certify its compliance with the cybersecurity regulations (as opposed to, for example, that the covered entity has implemented policies and procedures designed to meet the requirements of the regulation). Covered entities also are required to maintain "all records, schedules and data supporting" the certification for up to five years. Perhaps further complicating this certification requirement, the final rule maintains the requirement that covered entities document remedial efforts to address "areas, systems or processes that require material improvement." By requiring covered entities to both certify their full compliance and document areas requiring improvement, the NYDFS risks giving covered entities a Hobson's Choice: either document for inspection by the NYDFS what could be deemed indicia of noncompliance or forego efforts to continually improve and update the enterprise's information security program.

- **Timing.** Covered entities do not have much time to plan their approach to compliance with the final rule. Although the effective date is imminent, the final rule includes different phased timing requirements for when certain standards must be met. In general, compliance will be required 180 days from the rule's effective date. Compliance with certain specific requirements will be required within one year (*e.g.*, the penetration testing and multifactor authentication requirements), eighteen months (*e.g.*, the audit trail requirement) and two years (the third-party service provider security policy requirements) from the effective date.

  Although there are phased compliance periods for specific controls, the time periods are not consistent. For example, the compliance date for the risk assessment is one year from the effective date of the regulation (*i.e.*, March 1, 2018), which would in its own right give covered entities time to appropriately plan, scope and conduct a risk assessment. But, the risk assessment must inform the cybersecurity

policies and procedures that are required to be in place within 180 days of the effective date, as well as other controls, such as penetration testing and the use of multifactor authentication that must be in place within one year of the effective date. Moreover, the first certification of compliance will occur before the phased compliance periods expire. As a result, a covered entity's first two certifications may only be able to address those aspects of the final rule that are required at the time of the certification.

Now that the regulations are finalized, covered entities will need to consider their compliance position and their approach to demonstrating their compliance with the requirements of these cybersecurity standards. As Governor Cuomo stated in the press release issued with the NYDFS, the final rule represents "first-in-the-nation cybersecurity regulation" issued by a state financial regulator. Among other things, being first means that this rule is untested and unprecedented, and that may leave covered entities grappling with an uncertain regulatory future for some time.

Contact:

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

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

Client Alert

Financial Services Team

California

Michael J. Agoglia	(415) 268-6057
Alexis A. Amezcua	(415) 268-6557
Elizabeth Balassone	(415) 268-7585
Roland E. Brandel	(415) 268-7093
Sarah Nicole Davis	(415) 268-7478
Henry M. Fields	(213) 892-5275
Joseph Gabai	(213) 892-5284
Angela E. Kleine	(415) 268-6214
Jim McCabe	(415) 268-7011
James R. McGuire	(415) 268-7013
Mark David McPherson	(212) 468-8263
Ben Patterson	(415) 268-6818
Sylvia Rivera	(213) 892-5734
Nicholas Alan Roethlisberger	(415) 268-7534
Grant C. Schrader	(415) 268-6635
William L. Stern	(415) 268-7637
Nancy R. Thomas	(213) 892-5561
Lauren Lynn Wroblewski	(415) 268-6458

New York

James M. Bergin	(212) 468-8033
Meghan E. Dwyer	(212) 336-4067
Tiffani B. Figueroa	(212) 336-4360
David J. Fioccola	(212) 336-4069
Marc-Alain Galeazzi	(212) 336-4153
Adam J. Hunt	(212) 336-4341
Jessica Kaufman	(212) 336-4257
Mark P. Ladner	(212) 468-8035
Jiang Liu	(212) 468-8008
David H. Medlar	(212) 336-4302
Barbara R. Mendelson	(212) 468-8118
Michael B. Miller	(212) 468-8009
Judy Man Ni Mok	(212) 336-4073
Jeffrey K. Rosenberg	(212) 336-4130
Mark R. Sobin	(212) 336-4222
Joan P. Warrington	(212) 506-7307

Washington, D.C.

Leonard N. Chanin	(202) 887-8790
Rick Fischer	(202) 887-1566
Adam J. Fleisher	(202) 887-8781
Natalie A. Fleming Nolen	(202) 887-1551
Calvin D. Funk	(202) 887-6930
Julian E. Hammar	(202) 887-1679
Oliver I. Ireland	(202) 778-1614
Crystal N. Kaldjob	(202) 887-1687
Steven M. Kaufmann	(202) 887-8794

Washington, D.C. (continued)

Donald C. Lampe	(202) 887-1524
Jeremy R. Mandell	(202) 887-1505
Amanda J. Mollo	(202) 778-1609
Obrea O. Poindexter	(202) 887-8741
Ryan J. Richardson	(202) 887-8761
Sean Ruff	(202) 887-1530
Trevor R. Salter	(202) 887-1527
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.