LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Financial Institutions Industry Group December 22, 2016 | Number 2058

Financial Institutions Await Response to Concerns Over NYSDFS' Proposed Cybersecurity Rules

Comments submitted on the proposed regulations criticize the lack of a risk-based approach, overbroad definitions, potential extraterritorial implications, an excessive breach notification threshold and a daunting annual certification requirement.

Dozens of financial institutions and trade associations have lodged emphatic objections with the New York State Department of Financial Services (NYSDFS) in response to the Department's September 28, 2016 Notice of Proposed Rulemaking entitled "Cybersecurity Requirements for Financial Services Companies" (the Proposed Rules).[1] As published for comment in the New York State Register, the Proposed Rules would impose expansive new cybersecurity requirements on entities under NYSDFS' jurisdiction (and, through contract, would likely also impact service providers that process or store non-public information on their behalf). The Proposed Rules are considerably more prescriptive than cybersecurity guidance and standards promulgated by other financial regulators and, if adopted in their current form, would significantly ratchet up cybersecurity compliance obligations for affected institutions.

Interested parties were given the opportunity to provide feedback to NYSDFS on the Proposed Rules in a public notice-and-comment period that ended on November 14, 2016. The selected comments reviewed in this Client Alert cover a wide range of topics, but are animated by an overarching criticism that the Proposed Rules impose sweeping, categorical mandates as opposed to flexible, risk-based standards. The contemplated approach, the commenters warn, is at odds with well accepted principles of cybersecurity governance and would result in significant costs on financial institutions that are not justified by the cybersecurity benefits.

Recent reports indicate that, in light of the comments, the NYSDFS intends to modify the Proposed Rules and delay the effective date, which had initially been designated as January 1, 2017. How far NYSDFS goes toward modifying the Proposed Rules may signal where regulatory trends are headed in this area and how aggressively regulators may seek to exert pressure on businesses to incorporate specific policies and practices into their cybersecurity programs.

Background on the Proposed Rules

NYSDFS announced the Proposed Rules as a "groundbreaking" effort to combat cybersecurity attacks on the financial sector. "New York, the financial capital of the world, is leading the nation in taking decisive action to protect consumers and our financial system," the NYSDFS stated in a press release.[2] The Proposed Rules, it explained, were based on an extensive survey of best practices followed by financial institutions and recommended by cybersecurity experts.

While the prefatory language pays lip service to not being "overly proscriptive,"[3] a close reading of the substance of the Proposed Rules reveals a strict regulatory scheme that effectively hardens various (current) best practices into categorical mandates. By contrast, other government agencies, across the regulatory landscape — from the National Institute of Standards & Technology (NIST), to the Department of Health & Human Services, to the Federal Trade Commission, to the Securities & Exchange Commission — have consciously avoided hard-wiring specific practices directly into regulatory requirements. Rather, these agencies have followed a "risk-based" approach, by directing businesses to assess their vulnerability to various cybersecurity risks and to adopt safeguards reasonably designed to protect against those risks — without prescribing in regulation precisely what those measures should be. In this way, each business retains the flexibility to tailor its cybersecurity policies to its particular risk profile and to modify its policies over time to reflect changes in best practices.

Some of the specific mandates included in the Proposed Rules are uncontroversial, but others have astonishing reach, given the expansive way in which key underlying terms are defined. Among the mandatory program elements are requirements that each "Covered Entity":

- Designate a Chief Information Security Officer (CISO) responsible for overseeing and implementing the Covered Entity's cybersecurity program[4]
- Conduct annual penetration testing and quarterly vulnerability assessments of the Covered Entity's "Information Systems"[5]
- Require multi-factor authentication for any external access to the Covered Entity's network and for any privileged access to databases containing "Nonpublic Information"[6]
- Encrypt all Nonpublic Information held or transmitted by the Covered Entity, both in transit and at rest (with a one-year grace period for encrypting data in transit, and a five-year grace period for encrypting data at rest, so long as compensating controls are used in the interim)[7]
- Maintain audit trails of all financial transactions and data logging of all privileged access to critical systems, for a minimum of six years[8]
- Ensure that Nonpublic Information is retained no longer than necessary for the business purpose for which it was collected, absent any legal or regulatory retention requirement[9]
- Periodically (at least annually) assess the adequacy of the cybersecurity practices of any third parties with access to the Covered Entity's Information Systems or Nonpublic Information[10]
- Notify NYSDFS as promptly as possible, and in any event no less than 72 hours, of any "Cybersecurity Event" affecting Nonpublic Information or posing a reasonable likelihood of materially affecting the normal operation of the Covered Entity[11]

The key terms used in these requirements are defined quite broadly:

- Nonpublic Information is defined to include any information that is not publicly available and is either (1) business-related information whose disclosure could cause a material adverse impact to the Covered Entity or (2) information that "can be used to distinguish or trace an individual's identity," including name, date of birth, and social security number, or any other information "that is linked or linkable to an individual."[12]

- Information System is defined to include any "electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information," including specialized systems such as industrial control systems, environmental control systems, and telephone exchange systems.[13]

- Cybersecurity Event is defined to include "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."[14]

The Proposed Rules require the Board of Directors or a "Senior Officer" of a Covered Entity to certify, on annual basis, that it is in compliance with the Proposed Rules.[15] The certification is to be made to the best of the knowledge of the individual(s) providing the certification, following a review of relevant documents, reports, certifications and opinions of officers and employees of the Covered Entity, as well as outside vendors or other individuals as may be necessary.[16]

The Covered Entities subject to the Proposed Rules include any entities "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization" under the New York banking law, insurance law, or financial services law —essentially any institution subject to NYSDFS' supervision.[17] An exemption for smaller banks is narrowly limited to banks with fewer than 1,000 customers, less than US$5 million in gross annual revenue, and less than US$10 million in year-end total assets.[18]

The Proposed Rules originally stated that they would become effective as of January 1, 2017.[19] Covered Entities would have 180 days after that to come into compliance and would be required to submit their first annual compliance certification to NYSDFS by January 15, 2018.[20] However, according to recent reports, NYSDFS now intends to delay the effective date by two months, until March 1, 2017, to allow for publication and public consideration of a modified version of the Proposed Rules. Procedurally, before a final set of rules is promulgated, NYSDFS would be expected to file an assessment of the public comments received, including a summary of commenters' questions and requested changes, together with NYSDFS' response and an explanation of any final changes made.

Public Comments

Our review of the comments which the NYSDFS received focused on letters submitted by a variety of financial and insurance industry trade associations.[21] The more salient themes of these letters are summarized below.

Lack of Risk-Based Approach

Commenters expressed universal alarm that the Proposed Rules are overbroad and inflexible, due to their lack of a risk-based approach, and would impose requirements that are unworkable or unsuited to many systems, applications, and datasets, within all classes of financial institutions. According to one commenter, "[t]he one-size-fits-all nature of these requirements does not account for different financial services companies' unique business models, differences in their IT systems and their widely varying risk profiles."[22] The categorical nature of the Proposed Rules, the commenters contend, will force Covered Entities to implement the required measures regardless of the resulting costs and benefits, and thereby prevent firms from allocating their limited cybersecurity resources efficiently. As another commenter stated: "In addition to creating a tremendous amount of work for Covered Entities — the burden and costs of which should not be underestimated — the provisions as currently drafted would require dedication of resources to protect systems that pose no real risk to customer information or the financial stability of Covered Entities, in addition to adding extra layers of protection where none are needed."[23]

Commenters further argued that the prescriptive nature of the Proposed Rules is out of step with prevailing federal and industry cybersecurity standards, which financial entities have relied on for years as the foundation for their cybersecurity compliance programs. For example, commenters cited the NIST Cybersecurity Framework, which gives firms ample elbow room to match their cybersecurity practices to the actual risks associated with their particular systems and data. Likewise, several commenters pointed to the Federal Financial Institutions Examination Council's Cybersecurity Assessment Tool, and cybersecurity regulations promulgated by various financial agencies under the Gramm-Leach-Bliley Act, which follow a similar approach. As one commenter summarized: "[W]e are not aware of any authoritative guidance on cybersecurity that is not risk based and technology agnostic."[24] By deviating from this norm, another commenter added, the Proposed Rules create conflicts that could impede Covered Entities' current compliance efforts and "potentially place them at a competitive disadvantage" vis-à-vis financial institutions outside NYSDFS supervision, "without a compensating improvement in the effectiveness of their cybersecurity."[25]

Commenters offered various proposals for softening the Proposed Rules to provide firms with greater flexibility on how to achieve compliance. One commenter, for example, proposed adding a section providing that a Covered Entity "may comply with any provision" of the Proposed Rules "by doing so in a manner satisfying the requirements of a Risk-based approach."[26] The commenter proposed defining "Risk-based approach" to mean "implementing the applicable measures or other superseding or compensating controls ... as appropriate in accordance with the level of risk," and maintaining supportive documentation of the underlying risk assessment that may be shown to NYSDFS upon request.[27] In this way, the mandates in the Proposed Rules would be transformed into default practices, from which Covered Entities would be free to depart so long as they reasonably justified the departure in written documentation.

Unworkable Mandates

As to the specific technical requirements in the Proposed Rules that the commenters found overly prescriptive, the comments focus particular criticism on the encryption and multi-factor authentication requirements.[28]

The Proposed Rules require encryption of all Nonpublic Information, whether at rest or in transit (and whether in transit inside or outside the Covered Entity's network). The effective scope of the requirement is driven by the term Nonpublic Information, which, as noted above, is defined broadly, to include, among other things, any information "linkable to an individual." One commenter characterized the definition as "so broad that it could cover nearly all information obtained by a firm."[29] "[A]s a practical matter," another commenter opined, "Covered Entities would default to treating virtually all information as Nonpublic Information," regardless of its actual sensitivity.[30] Thus, the comment letters presume that the encryption requirement will lead Covered Entities to deploy encryption across-the-board to virtually all of their systems.

Such indiscriminate implementation of encryption would, the letters argue, be both impractical and counterproductive. For example, one comment letter explains, many firms rely on legacy, proprietary, or commingled systems that do not support modern encryption protocols. Even if those systems could — at massive expense — be upgraded to support the NYSDFS encryption requirement, "there would be enormous delays in data processing" entailed by the widespread use of encryption across the network, causing firms to "be unable to satisfy timely requests for information."[31] In other words, the encryption requirement would privilege the confidentiality of data over the integrity and availability of the data — which can be just as critical to business operations, as well as the safety and soundness of a financial institution. Moreover, the letter continues, requiring encryption would deter firms from exploring other

ways of protecting data — such as tokenization — that are potentially simpler, faster, and even more secure. Finally, the letter notes, encrypting all data in transit within a network may undermine a firm's ability to monitor its network traffic for suspicious activity — thereby sacrificing one (potentially more important) form of security control for another.

Commenters similarly criticized the multi-factor authentication requirement as overkill. The Proposed Rules require using this control for any external access to a Covered Entity's network or for any privileged access (internal or external) to a database containing Nonpublic Information. A number of commenters acknowledged the benefits of multi-factor authentication, but argued that it should not be required "regardless of any risk related to accessing the system and data, and regardless of other and potentially better controls that may be in place."[32] Another commenter added that, like overuse of encryption, overuse of multi-factor authentication "may ultimately be self-defeating, likely resulting in the creation of ad hoc workarounds and noncompliance."[33]

In line with their general recommendations to bring the Proposed Rules in line with a more "risk-based" approach, the commenters argued that, to the extent the encryption and multi-factor authentication provisions are retained in the final rules, the provisions should not be mandatory in nature. Instead, as one commenter recommended, the provisions should require firms to implement these practices only "based on a risk-based analysis to the extent technically feasible and in light of compensating controls."[34]

Extraterritorial Effects

In addition to the technical ramifications of the Proposed Rules, some commenters expressed concerns about their territorial scope as well. Comments from foreign banking organizations (FBOs), highlighted in a comment letter submitted by the Institute of International Bankers (the IIB Letter), point out a problem with the definition of a "Covered Entity" under the Proposed Rules. The definition includes any person required to operate under a New York license, but fails to distinguish between an FBO and its New York branch. Since an FBO is required to obtain a license in order to operate a New York branch, the definition might be read to imply that the Proposed Rules apply to the FBO itself — in its entirety — as opposed to only its New York operations. Unless the definition is appropriately clarified, the IIB Letter states, the Proposed Rules would result in the "unwarranted extraterritorial application of New York law."[35]

Moreover, the IIB Letter stresses that a cybersecurity program implemented by a New York branch of an FBO typically is subsumed within the larger cybersecurity program of the FBO as a whole. Yet, the IIB Letter argues, the Proposed Rules fail to distinguish between these two operational levels or address how responsibility for compliance with the Proposed Rules is to be allocated between them. For example, the Proposed Rules require each Covered Entity to designate a CISO to head its cybersecurity program; but a New York branch of an FBO will typically not have its own CISO. The person responsible for overseeing the branch's network operations is likely to be a lower-level employee of the FBO, if not an employee of a US affiliate of the FBO or even a third-party service provider. With respect to this and similar inflexibly worded governance requirements contained in the Proposed Rules, the IIB Letter urges that the requirements be modified to clarify that they only apply to the operations of a New York branch of an FBO, and that the FBO is entitled to administrative flexibility as to how it internally assigns responsibility for meeting the governance requirements.

Excessive Breach Notification Requirement

The comment letters also critique the breach notification requirement contained in the Proposed Rules, arguing that the threshold for notification is far too low. The Proposed Rules require Covered Entities to report to NYSDFS, within 72 hours, any Cybersecurity Event affecting Nonpublic Information. The letters argue that, because a Cybersecurity Event is defined to include any attempted intrusion — regardless of how successful, or how sensitive the Nonpublic Information affected — the disclosure requirement would generate an incessant flood of notifications. As one commenter stated:

Would every firewall packet drop — every automatically blocked attempt to breach a firewall — be included? For larger institutions, those attempts may number in the hundreds of thousands per day. It is difficult for us to see what the purpose for the [NYSDFS] collecting such vast amounts of information would be or how collecting the information would help Covered Entities reduce their cybersecurity risk.[36]

Commenters particularly questioned the value of such a broad disclosure requirement given that financial institutions are already subject to a variety of federal and state breach notification requirements concerning breaches of sensitive customer data (*i.e.*, data elements associated with financial risk or harm to consumers). Moreover, many firms voluntarily share information about breaches with peer firms through the Financial Sector Information Sharing and Analysis Center, which in itself is a best practice. Accordingly, several commenters suggested that the definition of Cybersecurity Event be narrowed to include only a cybersecurity attack that is both successful and significant, or, as one commenter expressed, that has "a reasonable likelihood of materially affecting the normal operation of" a Covered Entity.[37]

Beyond the reporting threshold, commenters also criticized the 72-hour deadline for reporting as impractical. As one commenter stated, this tight timeline "may often compel Covered Entities to report to the NYSDFS before they have had a reasonable opportunity to assess the significance of the triggering Cybersecurity Event."[38] The commenter suggested making the disclosure requirement more flexible, so as to require notification "without unreasonable delay," but without any fixed deadline — in accordance with typical breach notification requirements.[39]

Onerous Certification Requirement

Finally, several commenters expressed concern regarding the Proposed Rules' annual certification requirement. The requirement calls for the board or a senior official of a Covered Entity to certify each year that the entity's cybersecurity program "complies" with the NYSDFS regulations. Given the sweeping mandates contained in the Proposed Regulations, the commenters argue, a firm's leadership cannot reasonably be expected to certify that the firm is fully in compliance — "especially," as one commenter articulated, "in an environment that is inherently uncertain and fraught with unknown risks."[40] The practical result of the compliance requirement, the commenters contend, will be to drive Covered Entities to focus inordinately on proving compliance with the specific practices that happen to be mandated in NYSDFS regulations, rather than addressing their actual risks in a strategic, holistic fashion.[41] As one commenter put the point, Covered Entities will be driven to "expend resources ensuring that controls are applied across-the-board regardless of risk and documenting [those] compliance efforts, possibly diverting resources away from addressing companies' real vulnerabilities as they change over time."[42]

Additionally, commenters expressed confusion regarding the apparent contradiction between the certification requirement — which seems to require a Covered Entity to certify that its cybersecurity program is fully compliant with all of the NYSDFS regulations — and other language in the Proposed Rules requiring Covered Entities to identify any gaps in their cybersecurity program where improvement is needed.[43] As one commenter stated, the certification requirement "does not recognize that cybersecurity

is an iterative process, and it leaves no room for instances where complete compliance has not been achieved but remediation plans have been duly put in place."[44]

To remedy these issues, the commenters suggest that NYSDFS remove the annual certification requirement altogether, or else temper its language to only "require confirmation that processes reasonably designed to achieve compliance are in place."[45] As with the regulations as a whole, the commenters stress that any certification requirement should allow firms to implement, and attest to, a risk-based approach to cybersecurity.

Conclusion

Any modifications by NYSDFS to the Proposed Rules will be informed by substantial feedback based on the extensive and strongly asserted views reflected in the many commenters' submissions. How NYSDFS will respond is difficult to predict. As reflected in its announcement of the Proposed Rules, NYSDFS apparently seeks to establish itself as a leading regulator of cybersecurity in the financial sector. Yet, in pursuing this mantle, NYSDFS has proposed a regulatory regime that is conspicuously more prescriptive than the approach taken by its regulatory counterparts at the federal, state, and international level. Even in the post-breach or post-audit enforcement context, most regulators have avoided dictating particular means to achieving an effective and comprehensive cybersecurity program. Judging by the comment letters, the industry reaction to NYSDFS' proposed approach is unequivocal: the Proposed Rules fail to provide firms with sufficient flexibility to scale and tailor their cybersecurity practices to fit their operational risk profiles. With potential modifications to the Proposed Rules apparently in the works, all eyes are on the NYSDFS to see whether the agency will largely stand by its original approach or whether, in response to the comments received, it will adopt a set of final rules reflecting an approach that is more risk-based and consistent with prevailing regulatory and industry standards.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Jennifer Archie
jennifer.archie@lw.com
+1.202.637.2205
Washington, D.C.

Alan W. Avery
alan.avery@lw.com
+1.202.906.1301
New York

Serrin Turner
serrin.turner@lw.com
+1.202.906.1330
New York

Pia Naib
pia.naib@lw.com
+1.212.906.1208
New York

The authors would like to thank Will Clark and Ryan Schachne for their contributions to this *Client Alert*.

You Might Also Be Interested In

OCC to Make Available Special Purpose National Bank Charters to Fintech Companies

China Issues Its First Network Security Law

Bitcoin Again Held to Be "Funds" for Federal Money Transmitting Purposes

New York State Department of Financial Services Releases Final Regulations to Enhance Anti-Money Laundering and Sanctions Compliance for Financial Institutions

---

Endnotes

[1] Cybersecurity Requirements for Financial Services Companies (proposed Sep. 28, 2016), *available at* http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf (to be codified at 23 N.Y.C.R.R. pt. 500) [hereinafter *Proposed Rules*].

[2] Press Release, New York State Department of Financial Services, Governor Cuomo Announces Proposal of First-in-the-Nation Cybersecurity Regulation to Protect Consumers and Financial Institutions (Sept. 13, 2016).

[3] Proposed Rules § 500.0.

[4] Proposed Rules § 500.4.

[5] Proposed Rules § 500.5.

[6] Proposed Rules § 500.12

[7] Proposed Rules § 500.15.

[8] Proposed Rules § 500.06.

[9] Proposed Rules § 500.13.

[10] Proposed Rules § 500.11.

[11] Proposed Rules § 500.17.

[12] Proposed Rules § 500.01(g).

[13] Proposed Rules § 500.01(e).

[14] Proposed Rules § 500.01(d).

[15] Proposed Rules § 500.17(b).

[16] Proposed Rules App. A.

[17] Proposed Rules § 500.01(c).

[18] Proposed Rules § 500.18.

[19] Proposed Rules § 500.20.

[20] Proposed Rules § 500.20, 500.21.

[21] Letter from Securities Industry and Financial Markets Association (SIFMA), American Bankers Association, Financial Services Roundtable, Financial Services Sector Coordinating Council, Mortgage Bankers Association, American Financial Services Association, American Land Title Association, and New York Mortgage Bankers Association to Cassandra Lentchner, Deputy Superintendent for Compliance (Nov. 14, 2016) [hereinafter *SIFMA Letter*]; Letter from Trade Associations to Cassandra Lentchner, Deputy Superintendent for Compliance (Nov. 14, 2016) [hereinafter *ABA Letter*]; Letter from the Clearing House Association L.L.C. to Cassandra Lentchner, Deputy Superintendent for Compliance (Nov. 14, 2016) [hereinafter *Clearing House*

Letter]; Letter from Institute of International Bankers (IIB) to Cassandra Lentchner, Deputy Superintendent for Compliance (Nov. 14, 2016) [hereinafter *IIB Letter*].

[22] ABA Letter at 1.

[23] IIB Letter at 9.

[24] SIFMA Letter at 5.

[25] IIB Letter at 12. The IIB stressed that this issue was particularly important for foreign banking organizations, which may be supervised not only by federal and state regulators, but also by multiple countries.

[26] Clearing House Letter at 4.

[27] *Id*. at 5.

[28] Commenters also expressed concerns regarding the lack of a risk-based approach with respect to additional technical requirements in the Proposed Rules, including the logging and audit trail requirements and the vetting requirements for third-party service providers.

[29] Clearing House Letter at 5.

[30] IIB Letter at 17.

[31] SIFMA Letter at 14.

[32] IIB Letter at 21.

[33] SIFMA Letter at 14.

[34] *Id*.

[35] IIB Letter at 3.

[36] Clearing House Letter at 7.

[37] *Id.* at 8; *see also* IIB Letter at 16; SIFMA Letter at 8.

[38] Clearing House Letter at 8.

[39] Notably, however, while still not the majority practice, there are other regulators that have imposed similarly strict timing requirements for breach notifications. For example, the European Union's General Data Protection Regulation, when it goes into effect in 2018, will require regulated entities to notify their data protection authorities of a data breach within 72 hours or to supply a "reasoned justification" where that window cannot be met. Some notification deadlines are even tighter; for instance, the Monetary Authority of Singapore has instructed financial institutions to report security breaches within *one hour* of discovery.

[40] SIFMA Letter at 15.

[41] *Id*.

[42] Clearing House Letter at 11.

[43] *See* Proposed Rules § 500.17(b)(1) ("To the extent a Covered Entity has identified areas, systems, or processes that require material improvement, updating or redesign, the Covered Entity shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the superintendent.")

[44] SIFMA Letter at 15.

[45] Clearing House Letter at 11; *see also* SIFMA Letter at 15.