LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Financial Institutions Industry Group January 5, 2017 | Number 2061

NYSDFS Revises Cybersecurity Rules to Accommodate Industry Concerns

The revised regulations eliminate many of the categorical requirements in the original proposal and instead adopt a more risk-based approach.

On December 28, 2016, the New York State Department of Financial Services (NYSDFS) released a revised version of its "Cybersecurity Requirements for Financial Services Companies" (the Revised Proposed Rules).[1] A prior version of the proposal (the Original Proposed Rules) was subject to a public notice-and-comment period ending on November 14, 2016.[2] As summarized in a previous Latham *Client Alert*, many of the commenters expressed strong concerns that the Original Proposed Rules imposed sweeping, unworkable mandates and urged NYSDFS to adopt a more flexible, less prescriptive approach instead.

Those waiting to see whether NYSDFS would heed the commenters' concerns can now breathe a bit easier. The mandates in the Original Proposed Rules have generally been eliminated or softened in the Revised Proposed Rules, which provide much more discretion to covered entities to develop their cybersecurity policies and practices based on their own individualized risk assessments. The Revised Proposed Rules are now subject to a renewed 30-day public notice-and-comment period,[3] during which financial institutions can voice any additional concerns they have regarding the revised proposal, after which a final rule will likely be issued. In the meantime, the effective date of the proposal, which the NYSDFS originally proposed to be January 1, 2017, has been delayed until March 1, 2017.[4]

Revised Proposed Rules

Adoption of "Risk-Based Approach"

The Original Proposed Rules faced extensive industry criticism for being overly broad and categorical. Commenters called on NYSDFS to adopt a more risk-based approach — one that would allow "Covered Entities" (as defined in the Revised Proposed Rules) to assess for themselves what specific safeguards are needed to protect against the risks associated with their particular systems and data sets.

In apparent acknowledgment of these concerns, the Revised Proposed Rules now clarify that a cybersecurity program is to be "based on the Covered Entity's Risk Assessment."[5] The Risk Assessment "shall consider the particular risks of the Covered Entity's business operations related to cybersecurity" and the "availability and effectiveness" of its current controls, while also "allow[ing] for revision of controls to respond to technological developments and evolving threats."[6] Thus, at a general level, the Revised Proposed Rules recognize that each Covered Entity should have the flexibility to design a cybersecurity program that is tailored to its individual risk profile and adapted to current best practices.

Elimination of Categorical Mandates

At a more specific level, as well, the Revised Proposed Rules largely do away with the static, one-size-fits-all requirements that were the focus of commenters' criticism. In particular, many commenters had protested the requirement in the Original Proposed Rules that all "Nonpublic Information" be encrypted, both in transit and at rest.[7] This provision has now been downgraded from a categorical requirement to a default best practice, from which Covered Entities may deviate where appropriate. That is, while the Revised Proposed Rules still provide that a Covered Entity shall implement encryption to protect Nonpublic Information, the Revised Proposed Rules also provide that, to the extent a Covered Entity deems encryption to be "infeasible," it may use "effective alternative compensating controls" instead, so long as they are reviewed and approved by the Covered Entity's Chief Information Security Officer (CISO).[8]

Likewise, the Revised Proposed Rules narrow and relax the requirement in the Original Proposed Rules that Covered Entities use multi-factor and risk-based authentication[9] to protect Nonpublic Information. Whereas the Original Proposed Rules provided that each Covered Entity "shall require" multi-factor authentication for privileged access to systems containing Nonpublic Information, and risk-based authentication for any web applications that capture, display, or interface with Nonpublic Information,[10] the Revised Proposed Rules require only that Covered Entities "use effective controls, which *may* include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information."[11] Further, although the Revised Proposed Rules still provide that multi-factor authentication must be used to control any external access to a Covered Entity's internal networks, this provision, like the encryption provision, has been modified from a requirement into a default practice. The Revised Proposed Rules now allow the substitution of "reasonably equivalent or more secure access controls," so long as the Covered Entity's CISO has approved them in writing.[12]

The Revised Proposed Rules make comparable changes to other mandates contained in the Original Proposed Rules, including:

- Requirements for penetration testing and vulnerability assessments (now only required absent other effective means of detecting intrusion activity and vulnerabilities)[13]
- Requirements for maintaining audit trails and event logs (now only required "to the extent applicable and based on [the Covered Entity's] Risk Assessment")[14]
- Requirements for timely and secure disposal of Nonpublic Data (now no longer required "where targeted disposal is not reasonably feasible due to the manner in which the information is maintained")[15]

In conjunction with these changes, the Revised Proposed Rules also significantly narrow the term Nonpublic Information, which drove the scope of many of the requirements in the Original Proposed Rules, and still drives the scope of the modified requirements in the Revised Proposed Rules. Now, instead of broadly encompassing any information "linked or linkable to an individual,"[16] the term is defined much more narrowly with respect to personal information. Now, Nonpublic Information includes only information that, because of a name, number or other identifier, "can be used to identify" an individual "in combination with" certain other types of identity data (namely, social security number, driver's license number or non-driver identification card number, financial account number, security credential allowing access to the individual's financial account, or biometric records).[17] Notably, this language tracks the definition of "private information" in New York's breach notification law.[18]

Paring Back of Breach Notification Requirement

Commenters previously voiced concern that the Original Proposed Rules required Covered Entities to report any "Cybersecurity Event" to NYSDFS[19] — if Cybersecurity Event is defined to include any attempted intrusion, disruption, or misuse of a Covered Entity's information systems, regardless of how successful or how sensitive the affected data.[20] By contrast, under the Revised Proposed Rules, a Covered Entity is required to notify NYSDFS of a Cybersecurity Event only in either of the following two circumstances:

- If any other regulator or supervisory body is required to be notified
- If the Cybersecurity Event has "a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity"[21]

Additionally, whereas the Original Proposed Rules required a Covered Entity to report a Cybersecurity Event to NYSDFS within 72 hours of "becoming aware" of the event,[22] the Revised Proposed Rules clarify that the Covered Entity has 72 hours to report from the time it determines that a *qualifying* Cybersecurity Event has occurred.[23] By permitting Covered Entities to make this determination prior to reporting, the Revised Proposed Rules provide Covered Entities with time to assess the nature and significance of an event before the reporting obligation attaches.

More Clarity for Foreign Banking Organizations

The comments on the Original Proposed Rules included concerns foreign banking organizations (FBOs) expressed that the rules did not sufficiently address how FBOs are expected to comply with the requirements of the proposed rules (both original and revised). Specifically, commenters noted that the definition of Covered Entity applies to any "Person" required to operate under a New York license[24] — which could, as some commenters noted, be construed to imply that the Original Proposed Rules would apply extraterritorially to an FBO in its entirety, as opposed to merely the FBO's New York branch, since the FBO is the entity that obtains a license from the NYSDFS in order to operate a branch in New York.

The Revised Proposed Rules appear to address this issue in two ways. First, the Revised Proposed Rules include a revised definition of Person that clarifies that a branch itself can be a Covered Entity.[25] Additionally, the Revised Proposed Rules clarify that a Covered Entity can achieve compliance by "adopting a cybersecurity program maintained by an Affiliate," provided that the "Affiliate's" program complies with NYSDFS requirements.[26] The term Affiliate is defined in turn to include any Person that controls a Covered Entity,[27] which could by definition include an FBO that maintains a New York branch. Thus, the Revised Proposed Rules appear to distinguish between the New York branch of an FBO and the FBO itself, and would allow the New York branch to comply with NYSDFS requirements either by developing its own compliant program or by adopting the compliant program of the FBO itself.

No Change to Certification Requirement

The annual certification requirement in the Original Proposed Rules — requiring the board or a senior officer of a Covered Entity to annually certify compliance with the rules — has not been changed in the Revised Proposed Rules.[28] However, given the more flexible nature of the regulations as to which compliance must now be certified, this requirement arguably has become substantially less burdensome. Moreover, while the Original Proposed Rules required Covered Entities to submit their first compliance certification by February 15, 2018,[29] the Revised Proposed Rules provide for additional time beyond that for Covered Entities to come into compliance with certain provisions. Specifically, Covered Entities will have:

- One year from March 1, 2017 to comply with provisions concerning penetration testing and vulnerability assessments, risk assessment, multi-factor authentication and employee training[30]

- 18 months from March 1, 2017 to comply with provisions concerning audit trails and event logging, application security, data disposal, user monitoring and encryption[31]

- Two years from March 1, 2017 to comply with provisions concerning security assessments of third-party providers[32]

Conclusion

The modifications in the Revised Proposed Rules were clearly influenced by the substantial criticism various financial institutions, trade associations and other market participants lodged during the previous public notice-and-comment period. The Revised Proposed Rules still impose a number of significant new requirements and compliance obligations on Covered Entities. But, relative to where the NYSDFS started, regulators have stepped back from imposing broad, categorical mandates in favor of a more risk-based approach, as the commenters advocated.

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

You Might Also Be Interested In

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

5 Preventative Steps to Manage Legal Risk Following a Cybersecurity Breach

FCC Institutes New Privacy Regime for Broadband Providers and Other Telecommunications Carriers

Behind the Headlines of Evolving Cyberthreats (video)

Endnotes

[1] Cybersecurity Requirements for Financial Services Companies (proposed Dec. 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 *Revised Proposed Rules*].

[2] Cybersecurity Requirements for Financial Services Companies (proposed Sep. 28, 2016), [hereinafter *Original Proposed Rules*].

[3] Press Release, New York State Department of Financial Services, DFS Issues Updated Proposed Cybersecurity Regulation Protecting Consumers and Financial Institutions (Dec. 28, 2016).

[4] Revised Proposed Rules § 500.21.

[5] Revised Proposed Rules § 500.02(b).

[6] Revised Proposed Rules § 500.09(a).

[7] Original Proposed Rules § 500.15(a).

[8] Revised Proposed Rules § 500.15(b).The Revised Proposed Rules further clarify that encryption in transit is only required for Nonpublic Information "over external networks," whereas the encryption-in-transit requirement in the Original Proposed Rules did not distinguish between external and internal transmission.

[9] "Multi-factor authentication" is defined to mean "authentication through verification of at least two of the following types of authentication factors: (1) Knowledge factors, such as a password; or (2) Possession factors, such as a token or text message on a mobile phone; or (3) Inherence factors, such as a biometric characteristic." Revised Proposed Rules § 500.01(f). "Risk-based authentication" is defined to mean "any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions." (An example would be the use of challenge questions when a customer logs in to his financial account from an unfamiliar IP address or device.) Revised Proposed Rules § 500.01(l).

[10] Original Proposed Rules § 500.12.

[11] Revised Proposed Rules § 500.12(a).

[12] Revised Proposed Rules § 500.12(b).

[13] Revised Proposed Rules § 500.05.

[14] Revised Proposed Rules § 500.06.

[15] Revised Proposed Rules § 500.13.

[16] Original Proposed Rules § 500.01(g)(4).

[17] Revised Proposed Rules § 500.01(g)(2).

[18] *See* N.Y.G.B.S. § 899-aa(1)(B). The definition of "Nonpublic Information" in the Revised Proposed Rules also encompasses types of information other than personal identifying information, including any "business related information of a Covered Entity 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 Entity," as well as any health care-related information concerning any individual. Revised Proposed Rules § 500.01(g).

[19] Original Proposed Rules § 500.17(a).

[20] Original Proposed Rules § 500.01(d).

[21] Revised Proposed Rules § 500.17(a)(1)-(2).

[22] Original Proposed Rules § 500.17(a).

[23] Revised Proposed Rules § 500.17(a).

[24] Original Proposed Rules § 500.01(c).
[25] Revised Proposed Rules § 500.01(h).
[26] Revised Proposed Rules § 500.02(c).
[27] Revised Proposed Rules § 500.01(a).
[28] Revised Proposed Rules § 50017(b).
[29] Revised Proposed Rules § 500.21.
[30] Revised Proposed Rules § 500.22(b)(1).
[31] Revised Proposed Rules § 500.22(b)(2).
[32] Revised Proposed Rules § 500.22(b)(3).