MORRISON
FOERSTER

# NY Department of Financial Services Issues Significant Cybersecurity Proposal

Nathan D. Taylor and Adam J. Fleisher

09/26/2016

Privacy + Data Security

Client Alert

On September 13, 2016, the New York State Department of Financial Services (NYDFS) proposed cybersecurity rules that, if finalized in their current form, would create one of the most comprehensive, detailed and onerous cybersecurity standards in the country. While the proposed rules would apply only to financial institutions subject to the NYDFS's authority under New York law, this proposal is important for all companies. It highlights a trend that legislatures and regulators are revisiting decades-old approaches to cybersecurity and considering alternatives that would shift from a risk-based paradigm to a prescriptive approach. The NYDFS in particular has made great efforts to "spark additional dialogue, collaboration and, ultimately, regulatory convergence among" federal and state financial regulators on comprehensive cybersecurity standards for all financial institutions. In light of the significant role that New York plays in this country's financial markets and NYDFS's role as regulator for many financial institutions based in New York, this proposal comes with a level of credibility that could influence the broader, national dialogue and consideration of what cybersecurity standards are appropriate, even if NYDFS does not have unique expertise with respect to cybersecurity. If it does, consideration and monitoring of this proposal is important for all companies.

At the highest level, the proposed rules would require covered financial institutions to put in place controls designed to protect "nonpublic information" and the information systems that handle "nonpublic information." While NYDFS believes that its proposal would establish "minimum" regulatory standards that are not "overly prescriptive," the proposal is so prescriptive in some respects that it would be unworkable.

One critical issue with the proposal is the breadth of the definition of "nonpublic information" and the controls that would apply to that information. Instead of focusing on the types of information that, if misused, could harm a financial institution's customers, the proposed rules include a four-part definition of "nonpublic information" that includes virtually any information about a customer. For example, the definition incorporates the federal Gramm-Leach-Bliley Act (GLBA) definition of customer information that applies for purposes of the GLBA privacy standards. As a result, the proposed rules would cover, among other things, any information that an individual provides to a financial institution in obtaining a product or service, any information about the individual that results from a transaction and any information that the financial institution obtains about the individual in connection with providing a financial product or service to the individual. This would include basic information, such as a customer's name or the fact that the individual is a customer. While the definition makes sense in the context of the GLBA privacy rules that are focused on limiting disclosures of customer information to nonaffiliated third parties, it can lead to extreme results when tied to detailed cybersecurity controls, such as encryption, as is the case here.

The proposed rules include a number of "standard" data security controls that are required under existing federal and state law or have become best practices for regulated financial institutions. In fact, the NYDFS has incorporated into its proposal many of the controls required of federally chartered banks under the GLBA, as well as the federal banking agencies' expectations on security communicated in the FFIEC examination handbook. For example, the proposed rules would

require that a covered financial institution implement a cybersecurity program designed to protect nonpublic information, identify risks to that information and detect and respond to security incidents involving that information, and ensure that a qualified individual is responsible for overseeing the program and reporting to the institution's Board of Directors regarding security. From a technical standpoint, a covered financial institution's written policies would be required to address, "at a minimum," fourteen security concepts and controls, including, for example, access controls, network monitoring and security, physical controls and vendor management.

The proposed rules, however, become far more prescriptive (and less process-based) when requiring the implementation of specific controls.

- The proposed rules would require the **encryption** of all "nonpublic information," both in transit and at rest. This is dramatic in light of the broad definition of "nonpublic information," and would far exceed a sensible standard, let alone encryption requirements under existing law. For example, the proposal would require the encryption of a customer's name on any system where that name is stored and in any electronic communication in which the customer's name would be transmitted. As a practical matter, this would likely mean that a covered financial institution would have to encrypt every system and device that handles any customer information. It would also mean that a financial institution would have to encrypt every e-mail sent to a customer. While the proposed rules would account for scenarios where there are technological feasibility issues associated with implementing encryption, technological feasibility is not the issue. The issue is the burden, operational complexities, impacts to availability/access and the costs that would flow from a requirement to encrypt systems that do not include sensitive information.
- The proposed rules would require that a covered financial institution implement **multifactor authentication** in several contexts, including for all remote access from an external network and for "privileged access" to database servers that provide access to "nonpublic information." The exact contours of these requirements are not clear. For example, does "privileged access" mean any access to "nonpublic information" that the proposal would treat as sensitive? Would "privileged access" include non-user access, such as machine use of service accounts? The proposed rules also would require "risk-based authentication" for access to web applications that handle "nonpublic information" and "support[ing]" multifactor authentication for "any individual accessing" such web applications. The proposal is not clear if its focus is internal access, customer access or both. Regardless, existing federal standards for banks on multifactor authentication provide far greater flexibility to implement multifactor authentication or other layered security for customer access to, for example, online banking.
- The proposed rules would also impose significant **logging/audit trail** requirements. Again, however, the exact contours of the requirements are not clear. For example, a covered financial institution would be required to "track and maintain data that allows for the complete and accurate reconstruction of all financial transactions and accounting necessary to enable" the covered entity to detect and respond to a security incident. A covered financial institution also would be required to "log system events . . . and all system administrator functions performed on the systems." While it is not clear what exactly would need to be logged, the intent of the requirement is very clear-to require broad and comprehensive logging. Moreover, the proposed regulations would require "records produced as part of [this] audit trail" to be retained for a minimum of six years. This would be an extreme log-retention period that, in light of the detail and breadth of the logs, would impose significant storage costs on covered financial institutions.
- The proposed rules would require a covered financial institution to implement policies relating to the security of "nonpublic information" accessible to, or held by, " **third parties** doing business with the" financial institution. Among other things, the covered financial institution would be required to have in place policies and procedures for such third parties that address due diligence practices to assess the adequacy of cybersecurity practices of those third parties, "periodic assessment, at least annually, of such third parties and the continued adequacy of their cybersecurity

practices" and contractual provisions addressing the use of multifactor authentication, encryption for data in transit and at rest, and prompt notice of a cybersecurity event. In light of the breadth of the proposed encryption and multifactor authentication requirements, the obligation to flow down to "third parties" these requirements will present significant challenges in the vendor procurement process, particularly for a covered financial institution to feel comfortable that it has met its obligations under the regulations.

- Despite the sweeping requirements of the proposed rule, a covered financial institution would only be provided with 180 days to put in place policies, procedures, controls and systems that comply with the requirements. Moreover, a covered financial institution's Board of Directors would be required to provide an **annual certification of compliance** to NYDFS, which would be due for the first time on January 15, 2018. While requiring Board certifications would clearly create a compliance incentive for covered financial institutions, the Board certification will present a significant challenge in light of the fact that the proposal is not process-based and would impose broad standards, many of which are vague or potentially unworkable.

While the proposed rules would apply only to financial institutions subject to the NYDFS's authority under New York law, it is worth noting that there will be compliance challenges in the context of bank and financial holding companies that include federally chartered or other federally regulated entities, in addition to one or more affiliate or subsidiary that is subject to the NYDFS's authority. In this regard, holding companies often create holding company level security policies and standards that apply to all financial institutions within the family of companies. There will undoubtedly be practical questions as to how to address the fact that the subsidiaries subject to the NYDFS's authority are subject to less flexible standards and whether to establish stand-alone processes to address this fact.

The proposed rules are now subject to a 45-day notice and public comment period following the September 28, 2016 publication in the New York State register before their final issuance.