# What's New in the Revised NY State Proposed Cybersecurity Regulation?

As reported in our December 2016 article entitled, "*Proposed NYS DFS Cybersecurity Regulations to Significantly Impact FS Companies*", the New York State Department of Financial Services ("DFS") issued an initial version of a proposed cybersecurity regulation (the "Initial Regulation") that would require banks, insurance companies and other institutions regulated by the DFS ("Covered Entities") to establish and maintain a rigorous cybersecurity program.

On December 28, 2016, the DFS published an updated version of the regulation (the "Updated Regulation") after the comment period for the Initial Regulation ended, making significant changes to its security requirements[1]. The DFS will finalize the regulation after the expiration of a new 30-day comment period, and the new effective date of the regulation is expected to be **March 1, 2017**. Covered Entities will have 180 days from the effective date (until late August 2017) to comply with most of the regulation's provisions, but they will have up to two years to comply with certain other provisions. *Below is a summary of some of the key revisions contained in the Updated Regulation:*

## SCOPE OF "NONPUBLIC INFORMATION"

As noted in our December 2016 article, the regulation is designed to protect the security of "Nonpublic Information," which the Initial Regulation defined very broadly, going well beyond typical personally identifiable information. While the Updated Regulation narrows the scope of "Nonpublic Information" somewhat, the term is still defined quite broadly.

In the Updated Regulation, "Nonpublic Information" means:

- 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 Covered Entity's business, operations or security;
- Any information concerning an individual which because of name, number, personal mark or other identifier can be used to identify such individual, together with any one or more of the following: (i) social security number, (ii) driver's license number or identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records; and
- Any information (except age or gender) created by or derived from a health care provider or an individual and that relates to (i) the physical, mental or behavioral health or condition of any individual or family member, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

The Updated Regulation continues to provide that the information above would not be deemed Nonpublic Information if it is "Publicly Available Information." However, this exception will still require a Covered Entity to have a "reasonable basis to believe" that the otherwise Nonpublic Information was "lawfully made available to the general public" via certain specified sources. Therefore, it appears that Covered Entities would still need to perform some due diligence to "reasonably" satisfy themselves that the

[1] The Updated Regulation can be found at http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.

dissemination of publicly-available information was "lawful."

## Cybersecurity Policy Requirements

Covered Entities must implement and maintain a written cybersecurity policy. While the Initial Regulation required all Covered Entities' cybersecurity policies to address each of fourteen issues, the Updated Regulation provides that each Covered Entity's policy should be based on that particular Covered Entity's own risk assessment and should address the fourteen issues "to the extent applicable to the Covered Entity's operations." Thus, the Updated Regulation provides some flexibility as to which issues each Covered Entity's cybersecurity policy must address.

## Third Party Service Providers' Cybersecurity Obligations

As we noted in our December 2016 article, some organizations that are not regulated by the DFS would still be affected by this regulation because Covered Entities must identify and assess the cybersecurity risks of doing business with third party service providers that have access to Covered Entities' Information Systems and Nonpublic Information. The Updated Regulation offers Covered Entities more flexibility in identifying and addressing their service providers' cybersecurity risks. Now, Covered Entities' obligation to conduct cybersecurity assessments of their service providers will be based on the risks those service providers present. Additionally, Covered Entities are no longer expressly required to include in their contracts certain types of cybersecurity-related requirements for those service providers. Of course, Covered Entities may always require their service providers to comply with cybersecurity requirements that such Covered Entities choose to impose.

## Encryption of Nonpublic Information

The Initial Regulation required Covered Entities to encrypt all Nonpublic Information that they hold or transmit. An exception to that encryption requirement applied only if encryption was infeasible, and that exception applied for a limited time. Under the Updated Regulation, Covered Entities are required to implement "controls" (which may include encryption) that are appropriate based on their risk assessments. Therefore, encryption is not strictly required under the Updated Regulation. However, Covered Entities that use controls other than encryption must review the effectiveness of those controls (and review the feasibility of encryption) at least annually.

## Notices to the Superintendent of the DFS

The Initial Regulation required Covered Entities to notify the Superintendent of the DFS within 72 hours after becoming aware of any "Cybersecurity Event" that has a reasonable likelihood of materially affecting the normal operation of the Covered Entity, or that affects Nonpublic Information[2]. The Updated Regulation reduces the scope of Cybersecurity Events that require notification to the Superintendent. Under the Updated Regulation, Cybersecurity Events that require notice to the Superintendent are:

a) those in which notice must be provided to any supervisory body, and

b) those that "have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity."

In addition, the Updated Regulation eliminates the notification requirement for Covered Entities to notify the Superintendent of the DFS within 72 hours after identifying "any material risk of imminent harm relating to its cybersecurity

[2] Notably, the term "Cybersecurity Event" is broadly defined as "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" (emphasis added). Thus, even an unsuccessful attempt to gain unauthorized access will be considered a "Cybersecurity Event" for purposes of the regulation. The term "Information System" is also broadly defined, and could be interpreted to include any information system within the Covered Entity.

program," even if no cybersecurity event had actually occurred. Under the Updated Regulation, if a Covered Entity identifies areas that require material improvement, update or design, the Covered Entity must document its identification of the problem and its remedial efforts. The Superintendent may inspect the Covered Entity's documentation.

## Penetration Testing and Vulnerability Assessments

The Initial Regulation required Covered Entities to conduct penetration testing at least once a year, and vulnerability assessments at least quarterly. The Updated Regulation is less prescriptive in its requirements. Under the Updated Regulation, the cybersecurity program for each Covered Entity must include monitoring and testing that is designed to assess the effectiveness of the program. Covered Entities would be required to conduct annual penetration testing and bi-annual vulnerability assessments only in absence of effective continuous monitoring or other systems to detect changes that may indicate vulnerabilities.

## Additional Exemptions

The Updated Regulation exempts from certain requirements Covered Entities that have fewer than ten employees and those that are not required to access, receive or possess Nonpublic Information.

## What is Next?

As noted above, the effective date of the proposed regulation is expected to be March 1, 2017. All organizations covered by the regulation should design (or re-design) their cybersecurity programs and procedures to comply with the regulation once it becomes effective. This applies to Covered Entities, as well as to third party service providers that have access to Covered Entities' Nonpublic Information.

For more information on the topic discussed, contact Andre R. Jaglom at jaglom@thsh.com, David R. Lallouz at lallouz@thsh.com, Michael J. Riela at riela@thsh.com, or any other member of the Firm's Cybersecurity and Data Privacy Practice Group.