Proposed NY State DFS Cybersecurity Regulation to Significantly Impact Financial Services Companies and Businesses That Serve Them

This September, the New York State Department of Financial Services ("DFS") issued a proposed cybersecurity regulation, which is expected to become effective on January 1, 2017 and will require banks, insurance companies and other institutions regulated by the DFS ("Covered Entities") to establish and maintain a rigorous cybersecurity program[1]. Unless the regulation is dramatically altered before it becomes final, it will be one of the broadest and most demanding cybersecurity regulations in the country. The existing cybersecurity programs of many affected companies will likely not comply with the new proposed regulation.

What Information Is the Proposed Regulation Designed to Protect?

The purpose of the DFS's proposed regulation is to protect the security of Covered Entities' "Information Systems" and both their and their clients' "Nonpublic Information." While other data privacy and cybersecurity regulations focus on protecting personally identifiable information, the DFS's proposed regulation defines "Nonpublic Information" much more broadly. Under the proposed regulation, "Nonpublic Information" includes:

a) any business-related information, the tampering with which would cause a "material adverse impact to the business, operations or security of the Covered Entity";

b) "any information" that a client or customer provides to a Covered Entity in connection with the seeking or obtaining of any financial product or service; and

c) information that can be used to identify any individual, including an individual's name, Social Security number, date and place of birth, mother's maiden name and biometric records.

This information will not be deemed Nonpublic Information if it is "Publicly Available Information." However, this exception is narrow, as it requires a Covered Entity to have a "reasonable basis to believe" that the information was "lawfully made available to the general public" via certain specified sources. Therefore, Covered Entities will need to perform some due diligence to "reasonably" satisfy themselves that the dissemination of publicly-available information was "lawful."

Who Will Be Subject to the Regulation?

The proposed regulation applies to any "Covered Entity," which includes an individual or organization that operates under a license, registration or other authorization under New York State's banking, insurance or financial services laws. This includes banks and trust companies, insurance companies, licensed consumer lenders, check cashers, licensed mortgage lenders and brokers, and other institutions that are regulated by the DFS.

Moreover, organizations that are not regulated by the DFS will be impacted as Covered Entities will be required to identify and assess the cybersecurity risks of doing business with business partners that have access to Information Systems and Nonpublic Information. Business partners who do not maintain

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

adequate cybersecurity practices ultimately may end up being unable to do business with Covered Entities.

What Does the Proposed Regulation Require?

Based on the proposed regulation, Covered Entities will need to abide by the following requirements, among others[2]:

A. *Cybersecurity Program.* Covered Entities will be required to establish and maintain a cybersecurity program to perform core cybersecurity functions, such as (a) identifying internal and external cyber risks; (b) using defensive infrastructure and implementing policies and procedures to protect Information Systems and the Nonpublic Information stored on the Information Systems; and (c) detecting and responding to cybersecurity events.

B. *Written Cybersecurity Policy*. Covered Entities will be required to implement and maintain a written cybersecurity policy to address the protection of their Information Systems and the Nonpublic Information that is stored on those systems. The written cybersecurity policy must be reviewed by the Board of Directors or equivalent governing body, and approved by a senior officer of the Covered Entity.

C. *Chief Information Security Officer.* Each Covered Entity will need to designate a qualified individual to serve as its Chief Information Security Officer (known as a "CISO"), who would be responsible for overseeing and implementing the cybersecurity program and enforcing the cybersecurity policy. This requirement may be met by using third-party service providers, but each Covered Entity must have a senior member of the organization oversee the service provider and retain responsibility for compliance with the regulation. Each Covered Entity will also need to employ sufficiently trained and competent cybersecurity personnel to manage its cybersecurity risks and implement security measures.

D. *Encryption of Nonpublic Information.* Each Covered Entity will be required to encrypt all Nonpublic Information held or transmitted by the Covered Entity. There are limited exemptions where encryption is infeasible for a Covered Entity and the risks can be mitigated.

E. *Incident Response Plan.* Each Covered Entity would be required to establish a written incident response plan that is designed to promptly respond to, and recover from, a cybersecurity event. All breaches must be reported to the DFS within 72 hours of detection.

Some smaller Covered Entities will be exempt from some of the requirements of the proposed regulation, but they are still required to comply with most of the general requirements such as adopting a cybersecurity program and naming a CISO. To qualify for the exemption, Covered Entities must have fewer than 1,000 customers, less than $5 million in gross annual revenue and less than $10 million in assets.

When Will the Regulation Take Effect?

The proposed regulation is expected to become effective on January 1, 2017, and Covered Entities will have 180 days from the regulation's effective date to comply with its requirements. Thus, Covered Entities should expect to be required to comply with the final regulation by the end of June 2017 and will be required to submit annual certifications of compliance to the DFS beginning on January 15, 2018.

What Should You Do Now?

With now less than a month before the final regulation comes into effect, all organizations covered by the proposed regulation will need to carefully review the regulation and design their

[2] This article summarizes the most significant requirements under the proposed regulation, but does not summarize all of the requirements.

cybersecurity programs and procedures to comply with the regulation once it becomes effective. This applies to organizations directly covered by the regulation and their partners, whose business relationships may be impacted if their cybersecurity practices are not adequate. The requirements of the regulation are complex and technical, and will require the involvement of management, specialized IT personnel and counsel to interpret and assist in complying with this regulation.

For more information on the topic discussed, contact **Michael J. Riela** at **riela@thsh.com** or **David R. Lallouz** at **lallouz@thsh.com**.

For more information on Tannenbaum Helpern's Cybersecurity and Data Security practice, visit **http://bit.ly/2gmly7N**.