New York's New Cybersecurity Requirements For Financial Services Companies

March 6, 2017 | **CLIENT ALERTS**

On September 13, 2016, New York State proposed new cybersecurity requirements for banks, insurance companies, and financial service businesses regulated by the New York State Department of Financial Services ("DFS"). The regulations were amended based on public comments and went into effect on March 1, 2017. The regulations are a response to threats posed to information and financial systems by nation-states, terrorist organizations, and independent criminal actors. In 2013, New York's regulators imposed a similar security policy, breach notification, and encryption requirements on the healthcare industry through the enactment of New York General Business Law § 899-aa, which complements the federal healthcare privacy laws. Despite the early focus or cybersecurity in the healthcare industry, many financial sector companies have only recently adopted policies to prevent cyber-crime. This is troubling because the financial impact of losses suffered by financial institutions and their consumers can be significant. For example, in 2015 Target agreed to pay $39,400,000 to settle claims by the financial industry (banks, credit unions, and MasterCard) related to a 2013 data breach. To date, the data breach has cost Target over $290,000,000. Both state and federal regulators are now paying close attention to this issue, including Thomas Curry, Comptroller of the Currency who stated that "cyber threats [are] perhaps the foremost risk facing banks today . . . [and] represents one of the major, if not the major risk facing banks today."[1]

In drafting the proposed regulations, DFS did extensive surveying of cyber security protocols and incidents in the banking and insurance sectors and third party service providers in the banking sector (i.e., check/payment processors, trading and settlement operations, and data processing companies). Through the surveying, DFS learned that a vast majority of banking, insurance, and third party service providers already use encryption, have access controls, and have general security standards and protocols as part of their day-to-day operations. DFS did not indicate whether small businesses were in the majority or if they may be disproportionately impacted by the new regulations.

The new regulations apply to all businesses regulated by DFS pursuant to a license, charter, certificate, permit, or those authorized under New York's Banking Law, Insurance Law, or Financial Services Law. The regulations also apply to affiliates of regulated entities, much like healthcare privacy laws apply to affiliates or business associates. The regulations protect nonpublic information, which is defined as "electronic information that is not publicly available and is business related information that if disclosed in an unauthorized manner will cause a material adverse impact to business, operations, or security of the regulated entity." The regulations also protect information obtained from healthcare providers or individuals that relates to "past, present, or future physical, mental, or behavioral health or condition of any individual or any member of their family or household." The regulations further protect passwords or other authentication factors or information that can be used to trace an individual's identity, including a name, social security number, date and place of birth, mother's maiden name, biometric information, medical, educational, financial, occupational, or marketing information about a person.

Pursuant to the regulations, each regulated entity must establish and maintain a cybersecurity program that ensures confidentiality, integrity, and the availability of its electronic information as described in the regulations. There are six (6) specific functions that the programs must address including, 1) identifying external and internal cyber risks, identifying nonpublic information and how it can be accessed; 2) employing defensive infrastructure and policies/procedures to protect the nonpublic information; 3) detect any attempt (successful or otherwise) to gain unauthorized access to, disrupt or misuse electronic information resources; 4) respond to any attempt to gain unauthorized access and mitigate any negative effects; 5) recover and restore normal operations after any attempt to gain unauthorized access; and 6) fulfill specific regulatory reporting obligations. Pursuant to the regulations, entities are required to encrypt all nonpublic information held or transmitted by an entity both while in transit and at rest. Except as specifically stated in the regulations, companies have 180 days to comply with the new regulations and will be required to file an annual certification attesting to compliance beginning on February 15, 2018. Third-party service providers will have two years to comply with the new rules.

Each regulated entity must have a written cybersecurity policy that addresses fourteen (14) separate and distinct concerns ranging from general information security, data classification, physical security and environmental controls, encryption of nonpublic information, customer data privacy, risk assessment, and incident response. The written cybersecurity policy must be approved annually by a board of directors or senior officer of the company. Entities must provide training on the policy and procedures to all employees. Annual assessments of risk and penetration testing of the vulnerability of the system are required. The regulated entities must also have access controls with appropriate limitations and must track and maintain data logs of all access to critical systems. Moreover, the entities must keep a record of access and alterations made to the data log. The cybersecurity policy must address multi-factor identification (i.e., a password and security token or biometric information) for accessing nonpublic information or accessing internal systems from an external network. Third party service providers are also obligated to implement written policies and procedures designed to ensure the security of certain information held by those providers. The third party provider's policies must be based on the risk assessments made by the DFS regulated entity.

Entities must designate a Chief Information Security Officer ("CISO") to oversee and implement the cybersecurity program and enforce its cybersecurity policy. The CISO is also responsible for implementing cybersecurity incident response plans. Incident response plans guide a company's response to a breach. The primary objective of a plan is to manage a cybersecurity event to limit damage, increase the confidence of shareholders, regulators, and the public, and reduce recovery time and costs. A proactive incident response plan can save a company hundreds of hours and mitigate financial exposure. Drafting an incident response and building an incident response program should be a high level priority for regulated entities. The incident response plans generally outline the events which trigger a response, the team assigned to handle any breach or incident, identify the investigation to be completed, and detail key actions to be taken and notifications to be made in the event of a cybersecurity incident. The plan should also outline post-incident procedures and should be updated to improve future responses. Having a thorough plan is imperative when legal counsel has to report the breach to regulators. Counsel's ability to communicate that a company is following its incident response plan and taking specified measures to mitigate exposure will significantly decrease further questioning or intervention by a regulator.

Data retention is another area impacted by the regulations. Each entity must timely destroy nonpublic information unless retention of the information is necessary for the business or is required by law. This could provide significant cost savings for entities that maintain large amounts of data, but can also be hard to administer given

the existence of regulation litigation holds that are routinely imposed during the pendency of lawsuits and may prohibit any destruction of relevant records.

Finally, the proposed regulations require that all regulated entities provide notice to the Superintendent of DFS if there is a cybersecurity event that has a "reasonable likelihood of materially affecting the normal operations or nonpublic information." The regulated entity must provide that notice as "promptly as possible but in no event later than 72 hours after becoming aware of such a cybersecurity event." A cybersecurity event under the regulations includes the actual or potential unauthorized tampering with, or access to or use of nonpublic information or any event that involves cybersecurity issues and is reported to any government or self-regulatory agency. Annual compliance reporting is also required and all entities must maintain records, schedules, and data that support each certification of compliance made to DFS for at least five (5) years.

There is a limited exemption offered to smaller regulated entities

- with fewer than 10 employees
- that have less than $5,000,000 in gross annual revenue in each of the last three fiscal years, or
- that have less than $10,000,000 in year-end total assets, including assets of all affiliates.

Entities that qualify for the exemptions are not required to, among other things, designate a CISO, perform certain tests or maintain an audit trail, provide training, encrypt data, or have a written incident response plan. The precise exemptions are detailed in the new regulation and any entity that ceases to qualify for an exemption has 180 days from the end of the current fiscal year to become compliant.

The adoption of the cybersecurity requirements outlined above will be burdensome for smaller businesses, but for many of the large sophisticated bank and insurance companies, these rules will only require slight modifications to current practices, policies, and procedures. The most immediate challenge will be in managing third party vendors, implementing new or revised documentation retention policies, and providing oversight and direction to employees on the new cybersecurity regulations to ensure that the new policies are administered and implemented in a manner that is compliant with the regulations.

The cybersecurity group at Lippes Mathias Wexler Friedman LLP is always available to answer questions on the proposed regulations, provide assistance in drafting a compliant policy, or reviewing and revising preexisting policies to ensure compliance with the regulations.

Please contact Stacey I. Moar to learn more.