Financial Services Alert: NY Cybersecurity Regulation in Effect – Covered Entities Have Initial 180 Day Transition Period to Comply

Related Professionals

Marcel C. Duhamel

Related Services

Litigation and Appeals

Related Industries

Financial Institutions

CLIENT ALERT | 3.3.2017

On March 1, the New York State Department of Financial Services' (DFS) Cybersecurity Requirements for Financial Services Companies (the regulations) went into effect. Initially proposed in September of 2016, the DFS considered comments submitted during the initial comment period as well as those submitted during an additional comment period following the publication of an updated proposed regulation in December 2016, and incorporated many of those comments into the final regulations. However, the regulations may continue to present compliance challenges for covered entities.

Covered Entities: The regulations apply to any entity or organization "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization" under New York banking law, insurance law, or financial services laws. This may include New York-licensed lenders, mortgage banks, life insurance companies, savings and loans, charitable foundations and other financial services firms. Certain covered entities are exempt – those with less than 10 employees or independent contractors, less than $5 million in gross annual revenue in each of the last three fiscal years, or less than $10 million in year-end total assets. These regulations do not apply to national banks. Covered entities will also need to consider the application of any federal cybersecurity guidance in addition to the Regulations.

Risk Assessment and Cybersecurity Policy: Covered entities must conduct a risk assessment to evaluate and identify cybersecurity risks to the organization, and develop a cybersecurity program and policy designed to address those identified risks and protect the entity's systems and nonpublic information stored on those systems. "Nonpublic information" is defined broadly to include not only personal information covered under other laws, such as social security numbers, drivers' licenses and financial account information, but also includes business-related information, the tampering with which would cause materially adverse impact on an entity's business.

The cybersecurity policy must include policies for functions or risks that in many organizations may fall outside the Chief Information Security Officer's (CISO) or information security's domain. The cybersecurity policy must address the following areas, to the extent applicable to the business: (1) information security; (2) data governance and classification; (3) asset inventory and device management; (4) access controls and identity management; (5) business continuity and disaster recovery planning; (6) systems operation and availability concerns; (7) systems and network security; (8) systems and network monitoring; (9) systems and application developments and quality assurance; (10) physical security and environmental controls; (11) customer data privacy; (12) vendor and third party service provider management; (13) risk assessment; and (14) incident response.

The written cybersecurity policy or policies that address these areas must be approved by a senior officer or the board of directors, or equivalent governing body.

Designation of CISO: The regulations also require covered entities to employ a CISO to design and oversee the cybersecurity program and policy, although the final regulations allow this function to be handled by a third party service provider. The CISO's responsibilities under the regulations include filing an annual report to the board of directors or equivalent governing body, which must assess the integrity and security of systems, policies and procedures, material risks, system effectiveness, and material cybersecurity events that occurred during the reporting period.

Mandated Controls: Certain controls and testing are mandated under the regulations, including annual penetration testing, bi-annual vulnerability assessments, audit trails, limiting system access as well as periodic review of access privileges. The regulations also require use of multi-factor authentication or equivalent standard approved by the CISO, and encryption of data both in transit and at rest.

Reporting to DFS: A covered entity must provide notice of a "cybersecurity event" to the DFS where notice is required under applicable law or regulation, or where there is a reasonable likelihood of material harm to the normal operations of the entity. "Cybersecurity event" is defined broadly to include any act or attempt to gain unauthorized access to an entity's systems, including unsuccessful attempts. This notice must be given as soon as reasonably possible but in any event no later than 72 hours after the event to DFS.

The regulations contain several other notable requirements including:

- **Periodic Review:** Covered entities must periodically conduct risk assessments and update policies and procedures accordingly.
- **Trained cybersecurity personnel and employee training:** Covered entities must employ sufficient personnel or use third party service providers that are properly trained in cybersecurity and maintain current knowledge of changing threats and countermeasures; must also conduct regular cybersecurity awareness training to employees and monitor employees for unauthorized access or use of nonpublic information.
- **Vendor management:** Policies and procedures must be designed and implemented to address cybersecurity responsibilities of vendors, specifically those that have access to systems. The regulations also require due diligence procedures; establishment of minimum cybersecurity practices to do business with the entity; and periodic assessment of vendors. Due diligence on access controls and use of encryption, and notice to the covered entity of event impacting the entity's systems or nonpublic

information held by the vendor is also required.

- **Incident Response Plan:** Covered entities must maintain an incident response plan that clearly define roles, responsibilities and levels of decision-making authority, closely coordinates internal and external communications, documents and reports cybersecurity events, and processes that seek to improve the incident response place after a cybersecurity event. The plan must also ensure that all required reports are filed with appropriate regulatory agencies.

Although the regulations are now in effect, covered entities have an initial 180 day transition period to comply with many of the regulations' requirements, and up to two years for certain requirements. Additionally, the regulations will likely begin impacting other organizations as covered entities seek to push the regulations' requirements on to their service providers and business partners. The regulations will also, as a practical matter, have an impact beyond New York's borders as covered entities who do business not only in that state but others take steps to comply. For questions about the regulations and how it may affect your organization, please contact Heather Enlow-Novitsky, Marcel Duhamel or your Vorys attorney.