DAVIS MALM & D'AGOSTINE P.C.

ATTORNEYS AT LAW

REGULATORY LAW ALERT
JUNE 2017

NEW CYBER RULES FOR NEW YORK-BASED BANKING, INSURANCE AND FINANCIAL SERVICE FIRMS HAVE FAR-REACHING EFFECTS

OVERVIEW

In potentially the most significant state-level expansion of data security obligations since the 2010 promulgation of Massachusetts state-wide rules for protecting personal information of individual state residents, the New York State Department of Financial Services (NY DFS) finalized new Cybersecurity Regulations effective as of March 1, 2017 (NY Cyber Rules), with some additional time afforded to achieve full compliance.

The NY Cyber Rules impose detailed data protection requirements on virtually all New York banking, insurance and financial services firms. These obligations operate in parallel with, and in addition to, federal Gramm Leach Bliley data security protections applicable to financial institutions and other federal data security laws.

Once implemented, the NY Cyber Rules will have a significant impact on all companies covered by the Rules, as they will be subject to what are potentially the most rigorous data security requirements applicable to any entity anywhere in the United States. The NY Cyber Rules will also reach beyond New York to add regulatory requirements for the many service providers to the covered entities. They also provide the most potent example yet of the recent trend favoring state-level regulation of data security that began with Massachusetts seven years ago and has continued since then in a half-dozen additional states, including Connecticut and Rhode Island.

SCOPE OF RULES

The NY Cyber Rules will apply to a business if it (i) is a "covered entity," and (ii) maintains "nonpublic information" requiring protection.

A "covered entity" is defined to include any business operating under "a certificate, permit, accreditation or similar authorization under [the New York State] Banking Law, the Insurance Law, or the Financial Services Laws...". Given New York's massive banking, insurance, and financial services industries, the number of "covered entities" is likely to be both substantial and significantly in excess of the "financial institutions" operating in New York that are subject to federal regulatory requirements pursuant to Gramm Leach Bliley.

"Nonpublic Information" includes:

- individual information (name or identifying number plus a confidential social security or financial information number and expressly including individual biometric information);
- health information (data on the health or condition of any individual or family member); and
- certain business-related information (any information that, if tampered with or disclosed without authorization, would materially harm the covered entity's business, operations or security).

This broad hodgepodge creates an expansive set of information that covered entities must protect that goes beyond the protections afforded by existing federal or state laws.

KEY OBLIGATIONS APPLICABLE TO NONPUBLIC INFORMATION OF COVERED ENTITIES

Each covered entity must establish a cybersecurity program, based on a risk assessment, performing the following six "core" functions:

1. identify and assess cybersecurity risks that may threaten the security or integrity of nonpublic information stored on the covered entity's information systems (i.e., the "risk assessment");
2. use defensive infrastructure and implement policies and procedures to protect information systems and nonpublic information from unauthorized access, disruption, and misuse;
3. detect attempts at unauthorized access, disruption, or misuse;
4. respond to such attempts to mitigate any negative effects;
5. recover from such events and restore normal operations and service; and
6. fulfill regulatory reporting obligations.

Such program must include a written cybersecurity policy, also based on the risk assessment, which includes the following elements:

- information security;
- data governance and classification;
- asset inventory and device management;
- access controls and identity management;
- business continuity and disaster recovery planning and resources;
- systems operations and availability concerns;
- systems and network security;
- systems and network monitoring;
- systems and application development and quality assurance;
- physical security and environmental controls;
- customer data privacy;
- vendor and third-party service provider management;
- risk assessment; and
- incident response.

Each covered entity must conduct penetration testing to seek weaknesses in infrastructure on an annual basis. Vulnerability testing to "identify publicly-known cybersecurity vulnerabilities" must be conducted bi-annually.

The risk assessment also must consider use of two-factor or multi-factor authentication technologies to minimize opportunities for unauthorized access and must be used for accessing the entities' networks from external locations unless an equivalent alternative is used.

Written policies documenting the cybersecurity program must include addressing security concerns with third parties having access to the entity's nonpublic information, including any risk assessments undertaken relative to third-party provisions, minimum security practices required of them, due diligence processes, and periodic reassessment of protections, as well as specifically addressing access controls, encryption, notices of breaches/attempted breaches, and security-related representations and warranties.

Each covered entity must designate a chief information security officer (CISO) responsible for reporting to the covered entity's board of directors each year on the firm's cybersecurity program and material cybersecurity risks. The CISO can be an employee or a third-party consultant.

Beginning February 15, 2018, the chair of the covered entity's board of directors must submit to NY DFS a signed certification that the entity's program complies with the NY Cyber Rules to the best of the entity's knowledge.

The covered entity must notify the NY DFS of any breaches or attempted breaches (i.e., that trigger a governmental or self-regulating body notice requirement or has a reasonable likelihood of materially harming operations) within 72 hours after the determination that such event has occurred.

Finally, the covered entity must develop and maintain available for provision to NY DFS on request all relevant documents, including:

- a written cybersecurity policy;
- the annual CISO report to the board of directors;
- documentation of cyber monitoring and testing results;
- records sufficient to reconstruct key transactions and maintain audit trails;
- guidelines applicable to third-party vendor security;
- a written incident response plan;
- the annual certificate of compliance and back up support; and
- documentation of all areas that require improvement and the efforts planned to address such deficiencies.

IMPLEMENTATION DEADLINES

The following are some key compliance periods to keep in mind:

- 180 days from March 1, 2017 (late August 2017) unless additional time for specific action items is provided below;
- one year from March 1, 2017 (March 2018) for the first CISO written report, completion of initial penetration testing and vulnerability assessments, and completion of the initial risk assessment, implement multi-factor authentication, and conduct initial personnel training;
- 18 months from March 1, 2017 (late August 2018) to complete requirements relating to audit trails, application security, limiting data retention, ability to monitor users and encryption; and
- two years from March 1, 2017 (March 2019) to complete requirements relating to third-party vendors.

EXEMPTIONS FROM SOME OR ALL OBLIGATIONS OF COVERED ENTITY STATUS

Reinsurers of covered entities are exempt unless they separately qualify as covered entities themselves.

Covered entities are exempted from certain obligations if:

- the entity and its affiliates located in New York have fewer than 10 employees or independent contractors;
- the entity has fewer than $5 million in New York gross annual revenues in each of last three years; or
- the entity and affiliates have less than $10 million in year-end total assets.

Such partially exempted entities must still establish a cybersecurity program and written policy, limit access privileges, conduct a risk assessment, and report breaches and attempted breaches within 72 hours.

Covered entities also are partially exempted if they are insurance companies who have no nonpublic information, other than employee/affiliate information, or do not use information systems and do not possess nonpublic information. These categories of exempted entities must still conduct periodic risk assessments, implement third-party service provider security policies, and limit the sensitive data that they do retain.

In both cases, partially exempted entities are required to file a notice of exemption to NY DFS within 30 days after determining they are exempt.

CONCLUDING THOUGHTS

The NY Cyber Rules reflect a growing realization among industry participants, legislators and regulators that critically important data should be protected by robust data security measures and, if voluntary compliance proves insufficient, state governments will step in and require them as a legal matter.

Given the critical importance of financial, banking and insurance information, the NY Cyber Rules understandably rival, and appear to exceed in many cases, federal statutes such as Gramm Leach Bliley and HIPAA-HITECH as imposing the most rigorous and detailed data security requirements in the United States. They also exceed in important respects the groundbreaking Massachusetts rules enacted a half-dozen years ago which apply to all holders of sensitive personal information of Massachusetts individual residents. The NY Cyber Rules include the same mandatory written security plan, encryption and third-party vendor provisions as seen in Massachusetts, but also mandate appointment of a CISO, development of an annual report to the board of directors, submission by the Board chairperson to the NY DFS of a formal affidavit of compliance, mandatory record keeping and audit trail requirements, a required written incident response plan, and mandatory use of multi-factor authentication or equivalent technologies.

The requirement that the board chairperson must personally certify to the completeness of the plan – and presumably be personally liable if requirements are found not to be met – will make data security a "C" suite level issue that will trigger additional attention and resources at the highest levels of the covered entity, in a way similar to the Sarbanes-Oxley certifications required for public corporations several years ago. The NY Cyber Rules do not have any express penalty provisions, but one can expect that the Superintendent of NY DFS will enforce the regulations to the greatest extent practicable under applicable law.

Firm clients should promptly determine whether they qualify as a covered entity and, if not, whether they are vendors to a covered entity. The NY Cyber Rules require a tremendous amount of specific work to come into full compliance and work should commence as soon as possible. Even if a firm client is outside the scope of the NY Cyber Rules, all should realize that they likely will influence the "state of the art" for protection of sensitive information and that regulators and courts in other states may well expect that the provisions in the NY Cyber Rules should be part of a strong cyber plan by any company protecting financial or other data. At a minimum, all companies should consider a written security plan, a third party vendor policy, a written incident response plan, laptop and email encryption, annual program review, and consideration of multi-factor authentication technologies to be important components in a strong cybersecurity program.

A special note of thanks to Ethan Severance, legal intern, for his research assistance in preparing this alert.

CONTACT

If you have questions, please contact Robert J. Munnelly, Jr., in our Regulatory and Administrative Law Practice.

One Boston Place, Boston, Massachusetts 02108 | phone 617.367.2500 | fax 617.523.6215 | info@davismalm.com.