SQUIRE PATTON BOGGS

New York Proposes Cybersecurity Regulations for Financial Services Companies

On the heels of the National Association of Insurance Commissioner's (NAIC) release of the second draft of its Data Security Model Law, the New York Department of Financial Services (DFS) has promulgated a proposed regulation governing Cybersecurity Requirements for Financial Services Companies.

The proposed regulation is subject to a 45-day notice and comment period before it is finally issued as an active regulation. The plan is to have the regulation effective January 1, 2017, with a 180-day transitional period for compliance with the regulation.

Information about the regulation can be found in the DFS press release here and in a short explanation of the new regulation here. The full text of the regulation, which will be found at 23 NYCRR Part 500 (Financial Services Law) may be found here.

While there are some similarities with the NAIC's Data Security Model Law, the DFS Cybersecurity Regulation charts its own course. It requires each regulated financial institution to establish a cybersecurity program with the following five core functions:

(1) identification of cyber risks

(2) implementation of policies and procedures to protect unauthorized access/use or other malicious acts

(3) detection of cybersecurity events

(4) responsiveness to identified cybersecurity events to mitigate negative events

(5) recovery from cybersecurity events and restoration of services.

A written cybersecurity policy must be adopted that addresses the following minimum requirements:

- Information security
- Data governance and classification
- Access controls and identity management
- Business continuity and disaster recovery
- Capacity and performance planning
- System operations and availability
- 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
- Incident response

Additionally, each cybersecurity program must include the following:

- Annual penetration testing and vulnerability assessments
- Implementation and maintenance of audit trails
- Limitations and periodic reviews of access privileges
- Annual updates of written application security procedures
- Annual risk assessments
- Hiring and training of skilled cybersecurity personnel
- Multi-factor authentication
- Timely destruction of nonpublic information
- Monitoring of authorized users
- Encryption of nonpublic information held or transmitted
- Written incident response plan

The regulation will apply to any person (individual, partnership, corporation, association or any other entity) operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the banking law, the insurance law or the financial services law. The cybersecurity policy of each person must be reviewed by the entity's board of directors or governing body and approved by a senior officer. A Chief Information Security Officer (CISO) must be designated. If a third-party is used to meet this requirement, the regulation nevertheless puts responsibility for compliance on a senior member of the entity's personnel responsible for third-party providers. The CISO must prepare a report every six months to the governing body of the entity on the cybersecurity program.

The proposed regulation has requirements for cybersecurity personnel, sets forth the third-party information security requirements and requires multi-factor authentication to access systems and databases. Nonpublic information held or transmitted must be encrypted, but alternatives are provided if encryption is not possible.

Each entity also has to create an incident response plan as part of its cybersecurity policy. An outline of minimum requirements is provided by the proposed regulation. Additionally, and similar to the NAIC model act, the superintendent must be notified of any cybersecurity event. The regulation also has limited exceptions for smaller entities.

Unlike the NAIC model act, which has to be released and then passed by each individual state, the proposed regulation will go into effect in New York unless, during the public notice and comment period, the DFS makes any changes or seeks an extension. Accordingly, compliance and development of a cybersecurity policy consistent with the proposed regulation must start now.

Should your organization need assistance in providing comments to the proposed regulation or with creating a compliant cybersecurity policy, please let us know and our Data Privacy & Cybersecurity team will be pleased to assist you.