Bloomberg BNA

Privacy and Security Law Report®

New York Cybersecurity Regulations

The New York Department of Financial Services has proposed ''first-in-the-nation'' sweeping cybersecurity regulations for banks, credit unions and insurers chartered or licensed in New York. If adopted as written, compliance with the proposed regulations could prove expensive and challenging because of their comprehensiveness, accountability demands, and subjectivity, the authors write.

New York Proposes Groundbreaking Cybersecurity Regulations for Financial Institutions and Insurers

BY KATE MCGRAIL AND ELIZABETH DEL CID

On Sept. 13, New York's Department of Financial Services (DFS) proposed ''first-in-the-nation'' broad and sweeping cybersecurity regulations for banks, credit unions and insurers that are chartered or licensed in New York. The proposed regulations have already begun to serve as a model for the federal government, and it is likely that other states and different industries will follow suit.

Kate McGrail is a litigation attorney at Murphy & McGonigle in Glen Allen, Va.. McGrail represents clients in the financial services and insurance industries on compliance, regulatory and litigation matters, including cybersecurity.

Elizabeth Del Cid is a litigation attorney at Murphy & McGonigle in New York.

If enacted, regulated entities will have 180 days from Jan. 1, 2017 (the effective date of the proposed regulations) to comply with the new requirements, except as otherwise specified. The proposed regulations are subject to a 45-day notice and public comment period which was open from Sept. 28 to Nov. 13.

If adopted as written, compliance with the proposed regulations could prove expensive and challenging because of their comprehensiveness, accountability demands, and subjectivity. And the stakes are high. Noncompliance could mean revocation or suspension of the regulated entities' license to do business in New York. Highlights of the proposed regulations and compliance challenges are set forth below.

Cybersecurity Program

The proposed regulations require the establishment of a cybersecurity program that is designed to perform various core functions, including:

- identifying internal and external cybersecurity risks;
- protecting non-public information from unauthorized access;
- detecting cybersecurity events;
- mitigating the negative effects of cybersecurity events;
- recovering from cybersecurity events and restoring normal operations and services;

- fulfilling all regulatory reporting obligations; and
- destroying data.

Cybersecurity Policy

The proposed regulations require the implementation of a written cybersecurity policy that shall be reviewed by the board of directors and approved by a senior officer on an annual basis. The cybersecurity policy shall address areas such as:

- information security;
- data governance and classification;
- access controls and identity management;
- business continuity and disaster recovery planning and resources;
- capacity and performance planning;
- systems operations and availability concerns;
- systems and network security and 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; and
- limitations on data retention.

Chief Information Security Officer. The proposed regulations require that regulated entities designate a Chief Information Security Officer (CISO) responsible for overseeing and implementing the cybersecurity program and policies, and presenting a cybersecurity report at least bi-annually to the board of directors. The report must assess the confidentiality, integrity and availability of the information system, detail exceptions to the cybersecurity policies and procedures, identify cybersecurity risks, assess the effectiveness of the cybersecurity program, propose steps to remediate any inadequacies of the cybersecurity program and summarize material cybersecurity events.

Non-compliance could mean revocation or suspension of the regulated entities' license to do business in New York.

Reporting Requirements. Commencing Jan. 15, 2018, regulated entities will be required to provide to DFS an annual certification, signed by the chairman of the board or a senior officer, certifying compliance with the cybersecurity regulations. In addition, the proposed regulations contain a requirement that regulated entities notify DFS of any cybersecurity event that has a reasonable likelihood of materially affecting the normal operation of the regulated entity or affects non-public information within 72 hours of becoming aware of the cybersecurity event. This requirement applies to (1) any cybersecurity event involving the actual or potential unauthorized tampering with, or access to or use of, nonpublic information and (2) any cybersecurity event of which notice is provided to any government or self-regulatory agency.

Third Party Information Security Policy. The proposed regulations require that regulated entities ensure that third-party servicers adopt similarly stringent cybersecurity policies that include multifactor authentication to gain access to its information systems, encryption of all non-public information, prompt notice of cybersecurity events, identity protection services for customers materially impacted by cybersecurity events, various representations and warranties from third-party service providers and the right of the regulated entity to perform cybersecurity audits.

Encryption, Authentication and Assessment Requirements. Under the proposed regulations, regulated entities must encrypt all non-public information in transit or at rest, require multifactor authentication to gain access to their information systems and perform vulnerability assessments and penetration testing, in which entities attempt to infiltrate their own systems to assess their integrity.

Personnel Requirements. The proposed regulations require the regulated entity to employ cybersecurity personnel sufficient to manage the cybersecurity risk and to perform the core functions of the cybersecurity program and the cybersecurity personnel to stay abreast of changing cybersecurity threats and countermeasures. All personnel of the regulated entity are required to attend regular cybersecurity awareness sessions.

Exemptions. The proposed regulations exempt smaller institutions, including those with fewer than 1,000 customers in each of the preceding three years, those with less than $5 million in gross annual revenue in each of the preceding three years, and those with less than $10 million in year-end total assets.

Compliance Challenges

The proposed regulations extend well beyond industry practices, and it could prove difficult to comply with them. For mid-sized and smaller institutions, compliance could prove expensive and challenging, especially with respect to the encryption, authentication and assessment requirements, because they likely do not already undertake these measures.

For large institutions that contract with hundreds of vendors, requiring third-party servicers to adopt similarly stringent cybersecurity policies could be a heavy burden. The significant ongoing reporting requirements will impact all institutions alike, and those submitting the certification could be held individually liable if the institution's cybersecurity program is found to be deficient. In addition, the proposed regulations are peppered with vague and ambiguous terms that could complicate compliance. For example, they mandate notifying DFS of the ''*potential* unauthorized tampering with, or access to or use of, Nonpublic Information.'' ''Poten-

  PVLR ISSN 1538-3423

tial'' and ''tampering'' are not defined terms. The proposed regulations also require ''all personnel to attend regular cybersecurity awareness sessions.'' But ''regular'' is not defined, nor is the extent or substance of a ''cybersecurity awareness session.''