Bond

INFORMATION MEMO
CYBERSECURITY AND DATA PRIVACY

FEBRUARY 2017

New York State Department of Financial Services Issues Final Cybersecurity Regulations

On February 16, 2017, the New York State Department of Financial Services ("DFS") issued final cybersecurity regulations (the "Final Regulations"), with extensive requirements for cybersecurity programs by entities regulated by DFS, including banks, insurance companies and health plans ("Covered Entities"). The Final Regulations respond to criticism of the proposed regulations, issued first on September 13, 2016 and again on December 28, 2016, but retain many key elements of the regulations as initially proposed. With an effective date of March 1, 2017, the Final Regulations phase in certain obligations, over a time period ranging from six months to two years.

Changes in Final Regulations

While DFS made numerous changes to the regulations after the first public comment period, it made fewer amendments in issuing the Final Regulations. The most important changes created additional exemptions and redefined other exemptions. As we explained to clients in a prior Bond Memorandum, the proposed regulations would have obligated educational and charitable institutions that issue charitable gift annuities under Insurance Law § 1110 to comply with the new cybersecurity mandates.

On January 27, 2017, Tracy E. Miller, Co-Chair of the firm's Cybersecurity and Data Privacy Practice, submitted a letter in which she urged DFS to exempt institutions of higher education and other not-for-profit organizations covered by the proposed regulations solely due to the operation of a donor annuity program. We are pleased that the Final Regulations grant this exemption, which applies to hundreds of charitable organizations in the State, including universities, colleges, museums, social service providers and advocacy organizations.

The Final Regulations also exempt entities covered solely due to the application of Insurance Law § 5904 (risk retention groups not chartered or licensed as property/casualty insurers in New York), 11 NYCRR § 125 (reinsurers) and captive insurance companies regulated under Insurance Law Article 70 that do not control, own, access, generate, receive or possess nonpublic information ("NPI") other than information relating to a corporate parents. The Final Regulations also revised the exemptions for small entities so that the number of employees and revenue of affiliates located in New York State are considered when determining whether a Covered Entity meets one of the small entity definitions. Small entities and captive insurance companies are exempt from some, but not all, of the Final Regulations.

Summary of Final Regulations

The Final Regulations set forth cybersecurity standards that financial institutions, banks, insurance companies and health plans operating in New York must now satisfy. Entities covered by the Final Regulations must create a cybersecurity program based on a risk assessment that: (1) identifies risks to an entity's NPI stored on the Covered Entity's information systems; (2) uses defensive infrastructure and implements policies and procedures to protect information systems from unauthorized access and malicious acts; (3) detects successful and unsuccessful attempts to gain unauthorized access; (4) responds to identified cybersecurity events to mitigate negative effects; and (5) fulfills regulatory reporting requirements.

Covered Entities must also:

- Adopt policies and procedures for the security of information systems and NPI accessible to or held by third parties;
- Address data governance and classification, to the extent applicable;
- Address systems and application development and quality assurance;
- Conduct continuous monitoring or annual penetration testing and a bi-annual vulnerability assessment;
- Use multi-factor or risk-based authentication;
- Encrypt NPI at rest and in transmission; and
- Adopt an incident response plan with specified elements.

In response to public criticism, the Final Regulations qualified many of the specified elements of a cybersecurity program by stating that the required elements would apply based on the risk assessment conducted by the Covered Entity, rather than applying uniformly to all Covered Entities. Reflecting the increasing focus on board and senior management accountability for cybersecurity, the board of directors or the senior security officer of each Covered Entity must submit a certificate of compliance with the Final Regulations on an annual basis starting on February 15, 2018.

Under the Final Regulations, Covered Entities are required to implement written policies and procedures governing their practices with respect to third party service providers. Specifically, as set forth in the Final Regulations, Covered Entities must adopt policies that:

- Set minimum security practices that must be met by third party providers in order for them to do business with the Covered Entity;
- Establish procedures for due diligence to evaluate the adequacy of third party security practices; and
- Assess the risk posed by third parties to data security.

When a cybersecurity event, including an unsuccessful attempt at unauthorized access, is determined to have occurred, the event must be reported to DFS within 72 hours from a determination that; (i) the Covered Entity is required to report it to another governmental body or regulatory agency; or (ii) that the event had a reasonable likelihood of materially harming a material part of normal operations.

While the effective date of the Final Regulations is March 1, 2017, the Final Regulations specify transition periods of 180 days, 12, 18 and 24 months from the effective date for compliance with various provisions.

For further information about the Final Regulations, contact Tracy E. Miller, Co-Chair, Cybersecurity and Data Privacy Practice, or Curtis A. Johnson.

BOND SCHOENECK & KING ATTORNEYS
Commitment · Service · Value · Our Bond