Bond

INFORMATION MEMO
CYBERSECURITY AND DATA PRIVACY

NOVEMBER 2015

Potential New Cybersecurity Regulations for Financial Institutions and Insurance Companies

On the heels of recent high profile cyber-attacks against financial institutions and insurance companies, the New York State Department of Financial Services released a letter on November 9, 2015 that outlines proposed cybersecurity regulations currently under consideration.[1]

The Department is proposing to require all "covered entities"[2] to develop, implement and maintain a cybersecurity program to address twelve identified aspects of cybersecurity planning and readiness, including: information security, data governance and classification, access controls and identity management, business continuity and disaster recovery planning, capacity and performance planning, system operations and availability, system and network security, system and application development and quality assurance, physical security and environmental controls, customer data privacy, vendor and third-party service provider management and incident response.

Businesses subject to the Department's proposed regulations would be expected to stay abreast of new cybersecurity threats and countermeasures and to train and employ personnel to adequately manage their cybersecurity risks. The Department's proposal would allow covered entities to use outside contractors or vendors to assist them in complying with the new regulations, however, each covered entity would be required to designate a qualified employee to serve as its Chief Information Security Officer (CISO). In addition to overseeing and implementing the covered entity's cybersecurity program, the CISO would have the responsibility of preparing an annual report assessing the state of the program and known cybersecurity risks to be reviewed by the covered entity's board of directors and submitted to the Department.

The Department's letter indicates that determinations regarding specific security measures to be undertaken will, for the most part, be left to individual covered entities. At a minimum, however, the Department will likely require covered entities to adopt multi-factor authentication in connection with providing access to their internal systems or data from external networks, including customer access via web-based applications or other privileged access to database servers containing confidential information. The proposed regulations would also require covered entities, as part of their cybersecurity program, to conduct annual penetration testing and quarterly vulnerability assessments, and to maintain a system to collect, store and protect access data in order to preserve an audit trail.

Lastly, businesses would be required to notify the Department of any security breach (i) that has a reasonable likelihood of materially affecting the normal operation of the entity, (ii) which involves the compromise of nonpublic personal health information, private information, payment card information or biometric data, or (iii) which otherwise triggers a notice requirement under New York law.

Many companies in the financial services business have already implemented cybersecurity programs in order to better protect themselves against possible liability resulting from a breach. Existing cybersecurity measures should be reviewed, however, to address new developments and increased threats, and with an eye towards complying with enhanced government regulation in the cybersecurity arena. The proposals outlined by the New York State Department of Financial Services in its recent letter provide useful guidance as to what will be expected from companies in this constantly evolving area of the law.

For more information, please contact Jessica Moller (516.267.6332; jmoller@bsk.com) or Grayson Walter (315.218.8283; gwalter@bsk.com).

1 *Potential New NYDFS Cyber Security Regulation Requirements* (Nov. 9, 2015), available at http://www.dfs.ny.gov/about/letters/pr151109_letter_cyber_security.pdf.

2 It is not evident from the letter what businesses will qualify as "covered entities", but presumably the category would include banks, insurance companies and other large financial services companies subject to the Department's regulatory oversight.

BOND SCHOENECK & KING ATTORNEYS

Commitment · Service · Value · Our Bond