Winget | Spadafora | Schwartzberg | LLP

NY | NJ | CT | FL | CA | TX | IL | CO

www.WSSLLP.com

Winget, Spadafora & Schwartzberg, LLP - Client Alert

www.WSSLLP.com

About Us

Offices

Practice Areas

News & Events

New York State Proposes Sweeping Cybersecurity Requirements for Regulated Entities

October 14, 2016

The New York Department of Financial Services ("NYDFS") has proposed sweeping and largely unprecedented cybersecurity requirements on regulated banking, insurance, and financial entities in New York State ("Covered Entities"). These requirements are set to become effective on January 1, 2017, if they are adopted following a notice and public-comment period which expires on November 14, 2016. If adopted, Covered Entities must comply within 180 days of the effective date.

The cybersecurity requirements include the following:

- **Cybersecurity Program:** Each Covered Entity must "establish and maintain a cybersecurity program designed to ensure the confidentiality, integrity and availability of the Covered Entity's Information Systems." The cybersecurity program must perform multiple functions, including: the identification of internal and external cyber risks; the use and implementation of infrastructure, policies, and procedures to protect systems and nonpublic information; the detection of cybersecurity events; the response to identified or detected events to mitigate negative effects; the recovery from cybersecurity events and restoration of operations; and the fulfillment of all regulatory obligations.

- **Cybersecurity Policy:** Each Covered Entity must implement and maintain a written cybersecurity policy for the protection of information and nonpublic information. The policy must have multiple minimum components that address all areas of an adequate information-security program, and the policy must be reviewed and approved by a senior officer at least annually.

- **Chief Information Security Officer:** Each Covered Entity must designate a qualified Chief Information Security Officer ("CISO") with responsibility for overseeing and implementing the cybersecurity program and enforcing the cybersecurity policy. Third-party providers may perform these functions, but only if they comply with the regulatory requirements and are overseen by a senior officer. In addition, the CISO must develop a report, at least bi-annually, to be timely presented to the board of directors or equivalent body, or to a senior officer if no such board or body exists, assessing the cybersecurity protections, identifying cyber risks, proposing remediation steps, and summarizing all material cyber threats, incidents, and breaches.

- **Cybersecurity Program Minimum Requirements:** The proposed regulations detail specific minimum requirements for each cybersecurity program, including penetration testing and vulnerability assessments, audit trails that track and maintain the integrity of data and hardware, access privileges, and application security.

- **Risk Assessments:** Each Covered Entity must conduct a written risk assessment of its information systems, at least annually, in accordance with policies and procedures. The risk assessment must include: criteria for the evaluation and categorization of identified risks; criteria with which to assess the confidentiality, integrity, and availability of information systems; and requirements to document how to mitigate risks or why such risks would be justifiably accepted.

- **Cybersecurity Personnel and Intelligence:** Each Covered Entity must employ sufficient cybersecurity personnel sufficient to manage risks and perform core cybersecurity functions. All such personnel must attend regular updates and training sessions, and take steps to stay abreast of changing cybersecurity threats and countermeasures.

- **Third-Party Information-Security Policy:** Each Covered Entity must implement written policies and procedures to ensure the security of information systems and nonpublic information accessible to, or held by, third parties. These policies and procedures must identify and address cyber risks raised by these third parties, who must be required to maintain minimum cybersecurity practices to do business with the Covered Entity. Furthermore, the policies and procedures also must include preferred contractual provisions with which the third parties must comply, including provisions requiring multi-factor authentication, encryption, notice, identity-theft protection, representations and warranties, and the right to undertake audits.

- **Other Requirements:** There are numerous other requirements with which each Covered Entity must comply, including provisions governing multi-factor authentication, limits on data retention, training and monitoring, encryption of nonpublic information, incident-response plans, and notices to data superintendents within 72 hours of a cybersecurity event.

The proposal would exempt, from certain (but not all) requirements, any Covered Entity with fewer than 1,000 customers in each of the last three calendar years, less than $5 million in gross annual revenue in each of the last three fiscal years, and less than $10 million in year-end total assets.

Winget, Spadafora & Schwartzberg, LLP is closely monitoring these developments. If you would like to discuss the implications of the proposed requirements on your pre-breach preparations, policies, and procedures, please do not hesitate to contact Dianna McCarthy at (212) 221-6900 (mccarthy.d@wssllp.com) or Hillard Sterling at (312) 985-5600 (sterling.h@wssllp.com).

---

www.WSSLLP.com

NY | NJ | CT | FL | CA | TX | IL | CO