NY State Department of Financial Services Proposes Cyber Security Requirements for Financial Services Companies (23 NYCRR 500)

October 21, 2016

Section 500.0 Introduction:

The New York State Department of Financial Services ("DFS") has been closely monitoring the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors. Recently, cybercriminals have sought to exploit technological vulnerabilities to gain access to sensitive electronic data.

Cybercriminals can cause significant financial losses for DFS regulated entities as well as for New York consumers whose private information may be revealed and/or stolen for illicit purposes. The financial services industry is a significant target of cyber threats. DFS appreciates that many firms have proactively increased their cybersecurity programs with great success.

Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances.

Accordingly, this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization's cybersecurity program and file an annual certification confirming compliance with these regulations.

A regulated entity's cybersecurity program must ensure the safety and soundness of the institution and protect its customers. It is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs. The number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark. Adoption of the program outlined in these regulations is a priority for New York State.

Specifically, the proposed rules would require financial institutions to undergo the following measures, among other things:

- Establish and maintain a Cybersecurity Program and Cybersecurity Policy;
- Identify internal and external cyber risks by at a minimum, identifying the nonpublic information stored on the firms' information systems, a risk classification for the information, who has access to the information, and how they are able to access the information;
- Appoint a Chief Information Security Officer (CISO) to be responsible for the implementation and administration of the cybersecurity program and oversight over third party service providers;
- Adopt policies and procedures "designed to ensure the security of information systems and nonpublic information accessible to, or held by, third-parties";
- Implement multi-factor authentication for any individual accessing the firms' internal systems from an external network and privileged access to nonpublic information;
- Provide cybersecurity training and awareness for all personnel that are updated to reflect the firms' identified risks as well as an annual assessment of risks;
- Firm is required to encrypt all nonpublic information held or transmitted by the firm;
- Perform penetration testing at least annually;
- Establish and maintain an incident response plan;
- Perform an assessment of vulnerabilities of the firms' information systems at least quarterly;
- Annual certification of adherence to the rules.

The proposal was posted to the New York State register on September 28, 2016. The proposed rule will be subject to a 45-day notice and comment period before the rules become finalized. The transitional period will be 180 days form the effective date of the regulation to comply with the requirements.

For more information and to view the proposed rule in its entirety:

http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf