

**NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
23 NYCRR 500**

CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

I, Maria T. Vullo, Superintendent of Financial Services, pursuant to the authority granted by sections 102, 201, 202, 301, 302 and 408 of the Financial Services Law, do hereby promulgate Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, to take effect March 1, 2017, to read as follows:

(ALL MATTER IS NEW)

Section 500.00 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 cybersecurity 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.

Section 500.01 Definitions.

For purposes of this Part only, the following definitions shall apply:

...
(c) *Covered Entity* means any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.

...
(n) *Third Party Service Provider(s)* means a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity, and (iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity....

Section 500.11 Third Party Service Provider Security Policy.

(a) Third Party Service Provider Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible

to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable:

(1) the identification and risk assessment of Third Party Service Providers;

(2) minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity;

(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and

(4) periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

(b) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers including to the extent applicable guidelines addressing:

(1) the Third Party Service Provider's policies and procedures for access controls, including its use of Multi-Factor Authentication as required by section 500.12 of this Part, to limit access to relevant Information Systems and Nonpublic Information;

(2) the Third Party Service Provider's policies and procedures for use of encryption as required by section 500.15 of this Part to protect Nonpublic Information in transit and at rest;

(3) notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or the Covered Entity's Nonpublic Information being held by the Third Party Service Provider; and

(4) representations and warranties addressing the Third Party Service Provider's cybersecurity policies and procedures that relate to the security of the Covered Entity's Information Systems or Nonpublic Information.

(c) Limited Exception. An agent, employee, representative or designee of a Covered Entity who is itself a Covered Entity need not develop its own Third Party Information Security Policy pursuant to this section if the agent, employee, representative or designee follows the policy of the Covered Entity that is required to comply with this Part.