[23 NYCRR Part 500 (Financial Services Law)]

Cybersecurity Requirements for Financial Services Companies

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.

Section 500.01 Definitions.

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

(a) *Affiliate* means any Person that controls, is controlled by or is under common control with another Person. For purposes of this subsection, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise.

(b) *Authorized User* means any employee, contractor, agent or other Person that participates in the business operations of a Covered Entity and is authorized to access and use any Information Systems and data of the Covered Entity.

(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.

(d) *Cybersecurity Event* means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.

(e) *Information System* means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

(f) *Multi-Factor Authentication* means authentication through verification of at least two of the following types of authentication factors:

(1) Knowledge factors, such as a password; or

(2) Possession factors, such as a token or text message on a mobile phone; or

(3) Inherence factors, such as a biometric characteristic.

(g) *Nonpublic Information* shall mean all electronic information that is not Publicly Available Information and is:

(1) Any business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity;

(2) Any information that an individual provides to a Covered Entity in connection with the seeking or obtaining of any financial product or service from the Covered Entity, or is about an individual resulting from a transaction involving a financial product or service between a Covered Entity and an individual, or a Covered Entity otherwise obtains about an individual in connection with providing a financial product or service to that individual;

(3) Any information, except age or gender, that is created by, derived or obtained from a health care provider or an individual and that relates to the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family or household, or from the provision of health care to any individual, or from payment for the provision of health care to any individual;

(4) Any information that can be used to distinguish or trace an individual’s identity, including but not limited to an individual’s name, social security number, date and place

of birth, mother's maiden name, biometric records, any information that is linked or linkable to an individual, including but not limited to medical, educational, financial, occupational or employment information, information about an individual used for marketing purposes or any password or other authentication factor.

(h) *Person* means any individual, partnership, corporation, association or any other entity.

(i) *Penetration Testing* means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System.

(j) *Publicly Available Information* means any information that a Covered Entity has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law.

(1) For the purposes of this subsection, a Covered Entity has a reasonable basis to believe that information is lawfully made available to the general public if the Covered Entity has taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so.

(k) *Risk-Based Authentication* means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions.

(l) *Senior Officer(s)* mean the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems,

compliance and/or risk of a Covered Entity including a branch or agency of a foreign banking organization subject to this Part.

Section 500.02 Cybersecurity Program.

(a) Cybersecurity Program. Each Covered Entity shall establish and maintain a cybersecurity program designed to ensure the confidentiality, integrity and availability of the Covered Entity's Information Systems.

(b) The cybersecurity program shall be designed to perform the following core cybersecurity functions:

(1) identify internal and external cyber risks by, at a minimum, identifying the Nonpublic Information stored on the Covered Entity's Information Systems, the sensitivity of such Nonpublic Information, and how and by whom such Nonpublic Information may be accessed;

(2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts; ;

(3) detect Cybersecurity Events;

(4) respond to identified or detected Cybersecurity Events to mitigate any negative effects;

(5) recover from Cybersecurity Events and restore normal operations and services; and

(6) fulfill all regulatory reporting obligations

Section 500.03 Cybersecurity Policy.

(a) Cybersecurity Policy. Each Covered Entity shall implement and maintain a written cybersecurity policy setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall address, at a minimum, the following areas:

(1) information security;

(2) data governance and classification;

(3) access controls and identity management;

(4) business continuity and disaster recovery planning and resources;

(5) capacity and performance planning;

(6) systems operations and availability concerns;

(7) systems and network security;

(8) systems and network monitoring;

(9) systems and application development and quality assurance;

(10) physical security and environmental controls;

(11) customer data privacy;

(12) vendor and third-party service provider management;

(13) risk assessment; and

(14) incident response.

(b) The cybersecurity policy shall be reviewed by the Covered Entity's board of directors or equivalent governing body, and approved by a Senior Officer of the Covered Entity. If no such board of directors or equivalent governing body exists, the cybersecurity policy shall be reviewed and approved by a Senior Officer of the Covered Entity. Such review and approval

shall occur as frequently as necessary to address the cybersecurity risks applicable to the Covered Entity, but no less frequently than annually.

Section 500.04 Chief Information Security Officer.

(a) Chief Information Security Officer. Each Covered Entity shall designate a qualified individual to serve as the Covered Entity's Chief Information Security Officer ("CISO") responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy. To the extent this requirement is met using third party service providers, the Covered Entity shall:

(1) Retain responsibility for compliance with this Part;

(2) Designate a senior member of the Covered Entity's personnel responsible for oversight of the third party service provider; and

(3) Require the third party service provider to maintain a cybersecurity program that meets the requirements of this Part.

(b) Report. The CISO of each Covered Entity shall develop a report, at least bi-annually, as described herein. Such report shall be timely presented to the Covered Entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a Senior Officer of the Covered Entity responsible for the Covered Entity's cybersecurity program. Such report shall be made available to the superintendent upon request. The report shall:

(1) assess the confidentiality, integrity and availability of the Covered Entity's Information Systems;

(2) detail exceptions to the Covered Entity's cybersecurity policies and procedures;

(3) identify cyber risks to the Covered Entity;

(4) assess the effectiveness of the Covered Entity's cybersecurity program;

(5) propose steps to remediate any inadequacies identified therein; and

(6) include a summary of all material Cybersecurity Events that affected the Covered Entity during the time period addressed by the report.

Section 500.05 Penetration Testing and Vulnerability Assessments.

The cybersecurity program for each Covered Entity shall, at a minimum, include:

(1) penetration testing of the Covered Entity's Information Systems at least annually; and

(2) vulnerability assessment of the Covered Entity's Information Systems at least quarterly.

Section 500.06 Audit Trail.

The cybersecurity program for each Covered Entity shall, at a minimum, include implementing and maintaining audit trail systems that:

(1) track and maintain data that allows for the complete and accurate reconstruction of all financial transactions and accounting necessary to enable the Covered Entity to detect and respond to a Cybersecurity Event;

(2) track and maintain data logging of all privileged Authorized User access to critical systems;

(3) protect the integrity of data stored and maintained as part of any audit trail from alteration or tampering;

(4) protect the integrity of hardware from alteration or tampering, including by limiting electronic and physical access permissions to hardware and maintaining logs of physical access to hardware that allows for event reconstruction;

(5) log system events including, at a minimum, access and alterations made to the audit trail systems by the systems or by an Authorized User, and all system administrator functions performed on the systems; and

(6) maintain records produced as part of the audit trail for not fewer than six years.

Section 500.07 Access Privileges.

As part of its cybersecurity program, each Covered Entity shall limit access privileges to Information Systems that provide access to Nonpublic Information solely to those individuals who require such access to such systems in order to perform their responsibilities and shall periodically review such access privileges.

Section 500.08 Application Security.

(a) Each Covered Entity's cybersecurity program shall, at a minimum, include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, as well as procedures for assessing and testing the security of all externally developed applications utilized by the Covered Entity.

(b) All such procedures, guidelines and standards shall be reviewed, assessed and updated by the CISO of the Covered Entity at least annually.

Section 500.09 Risk Assessment.

(a) At least annually, each Covered Entity shall conduct a risk assessment of the Covered Entity's Information Systems. Such risk assessment shall be carried out in accordance with written policies and procedures and shall be documented in writing.

(b) As part of such policies and procedures, each Covered Entity shall include, at a minimum:

(1) criteria for the evaluation and categorization of identified risks;

(2) criteria for the assessment of the confidentiality, integrity and availability of the Covered Entity's Information Systems, including the adequacy of existing controls in the context of identified risks; and

(3) requirements for documentation describing how identified risks will be mitigated or accepted based on the risk assessment, justifying such decisions in light of the risk assessment findings, and assigning accountability for the identified risks.

Section 500.10 Cybersecurity Personnel and Intelligence.

(a) Cybersecurity Personnel and Intelligence. In addition to the requirements set forth in 500.04(a), each Covered Entity shall:

(1) employ cybersecurity personnel sufficient to manage the Covered Entity's cybersecurity risks and to perform the core cybersecurity functions specified in section 500.02(b)(1)-(5) of this Part;

(2) provide for and require all cybersecurity personnel to attend regular cybersecurity update and training sessions; and

(3) require key cybersecurity personnel to take steps to stay abreast of changing cybersecurity threats and countermeasures.

(b) A Covered Entity may choose to utilize a qualified third party to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in section 500.11 of this Part.

Section 500.11 Third Party Information Security Policy.

(a) Third Party Information Security 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 parties doing business with the Covered Entity. Such policies and procedures shall address, at a minimum, the following areas:

(1) the identification and risk assessment of third parties with access to such Information Systems or such Nonpublic Information;

(2) minimum cybersecurity practices required to be met by such third parties 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 parties; and

(4) periodic assessment, at least annually, of such third parties and the continued adequacy of their cybersecurity practices.

(b) Such policies and procedures shall include establishing preferred provisions to be included in contracts with third party service providers, including provisions addressing, to the extent applicable:

(1) the use of Multi-Factor Authentication as set forth in Section 500.12 to limit access to sensitive systems and Nonpublic Information;

(2) the use of encryption to protect Nonpublic Information in transit and at rest;

(3) prompt notice to be provided to the Covered Entity in the event of a Cybersecurity Event affecting the third party service provider;

(4) identity protection services to be provided for any customers materially impacted by a Cybersecurity Event that results from the third party service provider's negligence or willful misconduct;

(5) representations and warranties from the third party service provider that the service or product provided to the Covered Entity is free of viruses, trap doors, time bombs and other mechanisms that would impair the security of the Covered Entity's Information Systems or Nonpublic Information; and

(6) the right of the Covered Entity or its agents to perform cybersecurity audits of the third party service provider.

Section 500.12 Multi-Factor Authentication.

Multi-Factor Authentication. Each Covered Entity shall:

(a) require Multi-Factor Authentication for any individual accessing the Covered Entity's internal systems or data from an external network;

(b) require Multi-Factor Authentication for privileged access to database servers that allow access to Nonpublic Information;

(c) require Risk-Based Authentication in order to access web applications that capture, display or interface with Nonpublic Information; and

(d) support Multi-Factor Authentication for any individual accessing web applications that capture, display or interface with Nonpublic Information.

Section 500.13 Limitations on Data Retention.

As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the timely destruction of any Nonpublic Information identified in 500.01(g)(2)-(4) that is no longer necessary for the provision of the products or services for which such information was provided to the Covered Entity, except where such information is otherwise required to be retained by law or regulation.

Section 500.14 Training and Monitoring.

As part of its cybersecurity program, each Covered Entity shall:

(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users; and

(b) provide for and require all personnel to attend regular cybersecurity awareness training sessions that are updated to reflect risks identified by the Covered Entity in its annual assessment of risks.

Section 500.15 Encryption of Nonpublic Information.

(a) As part of its cybersecurity program, each Covered Entity shall encrypt all Nonpublic Information held or transmitted by the Covered Entity both in transit and at rest.

(b) To the extent encryption of Nonpublic Information in transit is currently infeasible, Covered Entities may instead secure such Nonpublic Information using appropriate alternative compensating controls reviewed and approved by the Covered Entity's CISO. Such

compensating controls shall not be used in lieu of meeting the requirements of subsection 500.15(a) after one year from the date this regulation becomes effective.

(c) To the extent encryption of Nonpublic Information at rest is currently infeasible, Covered Entities may instead secure such Nonpublic Information using appropriate alternative compensating controls reviewed and approved by the Covered Entity's CISO. Such compensating controls shall not be used in lieu of meeting the requirements of subsection 500.15(a) after five years from the date this regulation becomes effective.

Section 500.16 Incident Response Plan.

(a) As part of its cybersecurity program, each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business.

(b) Such incident response plan shall, at a minimum, address the following areas:

(1) the internal processes for responding to a Cybersecurity Event;

(2) the goals of the incident response plan;

(3) the definition of clear roles, responsibilities and levels of decision-making authority;

(4) external and internal communications and information sharing;

(5) remediation of any identified weaknesses in Information Systems and associated controls;

(6) documentation and reporting regarding Cybersecurity Events and related incident response activities; and

(7) the evaluation and revision of the incident response plan following a Cybersecurity Event.

Section 500.17 Notices to Superintendent.

(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent of any Cybersecurity Event that has a reasonable likelihood of materially affecting the normal operation of the Covered Entity or that affects Nonpublic Information. The Covered Entity must notify the superintendent as promptly as possible but in no event later than 72 hours after becoming aware of such a Cybersecurity Event. Such Cybersecurity Events include, but are not limited to:

(1) any Cybersecurity Event of which notice is provided to any government or self-regulatory agency;

(2) any Cybersecurity Event involving the actual or potential unauthorized tampering with, or access to or use of, Nonpublic Information.

(b) Annually each Covered Entity shall submit to the superintendent a written statement by January 15, in such form set forth as Exhibit A, certifying that the Covered Entity is in compliance with the requirements set forth in this Part. Each Covered Entity shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years.

(1) To the extent a Covered Entity has identified areas, systems, or processes that require material improvement, updating or redesign, the Covered Entity shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the superintendent.

(2) To the extent that a Covered Entity has identified any material risk of imminent harm relating to its cybersecurity program the Covered Entity shall notify the superintendent within 72 hours and include such items in its annual report filed pursuant to this section.

Section 500.18 Limited Exemption.

(a) Limited Exemption. Each Covered Entity with: (1) fewer than 1000 customers in each of the last three calendar years, and (2) less than $5,000,000 in gross annual revenue in each of the last three fiscal years, and (3) less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates, shall be exempt from the requirements of this Part other than the requirements set forth in this section, Sections 500.02, 500.03, 500.07, 500.09, 500.11, 500.13, 500.17, 500.19, 500.20 and 500.21.

(b) In the event that a Covered Entity, as of its most recent fiscal year end, ceases to qualify for the limited exemption as set forth in subsection 500.18(a), such Covered Entity shall have 180 days from such fiscal year end to comply with all requirements of this Part.

Section 500.19 Enforcement.

This regulation will be enforced pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws.

Section 500.20 Effective Date.

This part will be effective January 1, 2017. Covered Entities will be required to annually prepare and submit to the superintendent a Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations under Section 500.17 commencing January 15, 2018.

Section 500.21 Transitional Period.

Transitional Period. Covered Entities shall have 180 days from the effective date of this regulation to comply with the requirements set forth in this Part, except as otherwise specified.

Section 500.22 Severability.

If any provision of this Part or the application thereof to any Person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Part or the application thereof to other Persons or circumstances.

ATTACHMENT A

_____

(**Covered Entity Name)**

January 15, 20__

Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:

(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(2) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity as of _____(date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended_____(year for which Board Resolution or Compliance Finding is provided) complies with Part ___.

(3)

Signed by the Chairperson of the Board of Directors or Senior Officer(s)

(Name)_____ Date:

[DFS Portal Filing Instructions]