Client Update

New York Eases Proposed Cybersecurity Regulation for Financial Sector, But Practical Issues Remain

NEW YORK
Eric R. Dinallo
edinallo@debevoise.com

Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

WASHINGTON, D.C.
Luke Dembosky
ldembosky@debevoise.com

Maryam Casbarro
mcasbarro@debevoise.com

New York's Department of Financial Services (DFS or the Department) has responded to a large volume of comments about its proposed, sweeping cybersecurity regulation for banks, insurers and other financial service providers by softening a number of provisions that many in the industry had criticized as onerous and overly prescriptive. On December 28, 2016, the Department published a revised regulation (the Revised Draft Regulation)[1] that altered its original, "first-in-the-nation" proposal issued on September 13, 2016 (the Original Draft Regulation).

Many had argued that the Original Draft Regulation should be more risk-based, along the lines of the NIST Cybersecurity Framework and similar guidelines-based approaches to cyber risk management, rather than a top-down list of detailed requirements.[2] The Revised Draft Regulation moves towards a more risk-based approach—in particular, elevating the significance of periodic risk assessments that covered entities will undertake. The regulation remains the most detailed and comprehensive ever introduced in the financial sector, however.

The Revised Draft Regulation is subject to a 30-day notice and comment period, ending January 27, 2017, which DFS has stated will focus on any new comments that were not previously raised in the original comment process.[3] Subject to any

---

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

2 *See* National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

3 http://www.dfs.ny.gov/about/press/pr1612281.htm.

further revisions that arise out of the new comment process, the Revised Draft Regulation goes into effect on March 1, 2017 (extended from January 1 in the Original Draft Regulation), with a general transition period of six months from the effective date, subject to the new, section-specific transition periods noted below.

NOTABLE REVISIONS TO THE ORIGINAL PROPOSAL

The Revised Draft Regulation adjusts many aspects of the Original Draft Regulation. DFS issued no redline version or explanation of its changes. We discuss here revisions to some of the most significant provisions.[4] We also have created a redline version, which appears at the back of this update.

Cybersecurity Program and Policies, and Roles of Senior Management and the Board

Section 500.02 of the Revised Draft Regulation adds that the umbrella "cybersecurity program" that each Covered Entity must have shall be based on a periodic Risk Assessment, as further described in new language to Section 500.09, that the entity must conduct to identify the cybersecurity risks it faces and must use to shape its information security policies and procedures. The cybersecurity program itself must track the familiar NIST Framework categories with some modification: identification (of risks), defense (of systems and information), detection (of Cybersecurity Events), response and recovery (to said events), and fulfillment of regulatory reporting obligations. The upshot is that Covered Entities are given more latitude to design their cybersecurity programs (including the policies and procedures they contain) based on their periodic Risk Assessment. A notable change in the Revised Draft Regulation, clearly made in response to comments about duplication and other inefficiencies, allows a Covered Entity to adopt the qualifying cybersecurity program of an Affiliate.

One of the concerns of the Original Draft Regulation was the proposed requirement both for the board of directors to review and a Senior Officer to approve the firm's cybersecurity policies and procedures (pursuant to Section 500.03). The Revised Draft Regulation eases this requirement by eliminating mention of board review and by allowing for approval either by the board or a Senior Officer.

[4] We retain here DFS's capitalization of defined terms and refer the reader to Section 500.01 of the Revised Draft Regulation for complete definitions of these terms.

Definition of Nonpublic Information

The Original Draft Regulation included three approaches to defining the sort of "Nonpublic Information" that DFS requires Covered Entities to protect: a general category of business information that would cause a "material adverse impact" if tampered with or disclosed; a category of information provided to a Covered Entity by consumers in connection with "seeking or obtaining" financial services; and a category of healthcare information.

The business information and healthcare category definitions are essentially unchanged in the Revised Draft Regulation. In preserving the "material adverse impact" test for business information, DFS overrode comments from the industry to the effect that such a test is vague and overbroad.

DFS did, however, rewrite the definition for the consumer information category. Where the previous version covered essentially all information that a consumer provides to a Covered Entity, the new definition is limited to markers that "can be used to identify such individual," such as social security numbers, drivers' license numbers, account numbers, passwords, and biometric identifiers. The net effect is to bring the scope of covered information substantially in line with New York's breach disclosure statute, which includes a similar definition of covered personal information.[5]

Chief Information Security Officer, Periodic Reporting, and Annual Certification

On another governance point, although the requirement for each Covered Entity to have a Chief Information Security Officer (CISO) or equivalent is unchanged, the Revised Draft Regulation makes clear that the CISO may be employed by an Affiliate (or, as permitted before, by a Third Party Service Provider) and extends the CISO's required periodic written reports to the board of directors from bi-annual to annual. The Revised Draft Regulation also limits the CISO's reporting duty regarding cybersecurity risks and Cybersecurity Events to those that are "material." Although the revision deletes the requirement that the report be made available to DFS, elsewhere in the Revised Draft Regulation (at Section 500.02), DFS has added a new requirement that "[a]ll documentation and information relevant to the Covered Entity's cybersecurity program shall be made available to the superintendent upon request." Notably, the Revised Draft Regulation retains the requirement that senior management annually certify compliance with the new rules.

[5] New York General Business Law § 899-aa(1).

Multi-Factor Authentication, Encryption and Access Privileges

One of the most troublesome aspects of the Original Draft Regulation had been the very broad requirements—tied largely to the broad definition of Nonpublic Information—to use Multi-Factor Authentication for seemingly all network access, and to encrypt nearly all data in transit or at rest. The Revised Draft Regulation makes welcome changes to both requirements. Multi-Factor Authentication is required only for individuals accessing the Covered Entity's internal networks from an external network, and even then, only when the CISO has not approved the substitution of "reasonably equivalent or more secure access controls." In all other cases, a Covered Entity need only implement "effective controls," which "may include" Multi-Factor Authentication or Risk-Based Authentication. Perhaps even more significantly, the mandatory encryption requirements noted above are relaxed, in cases where encryption is "infeasible," to allow for "alternative compensating controls" reviewed and approved by the CISO at least annually.

A small but significant change concerning access privileges eliminates the requirement that entities limit user access to Information Systems and Nonpublic Information on a "need to know" basis, requiring instead that access be limited (and reviewed periodically) based on the entity's Risk Assessment.

Third Party Service Providers

Another controversial provision of the Original Draft Regulation required Covered Entities to establish third party information security policies and procedures that arguably treated all vendors the same way in terms of the risks they presented and the information security terms that could be imposed on them. Here, DFS made significant changes to move to a risk-based, guidelines approach by allowing each Covered Entity to base the specific terms of its vendor policies and procedures on the vendor risks identified in the entity's overall Risk Assessment. The Revised Draft Regulation does require that policies and procedures at least address, "to the extent applicable," how vendor risks will be assessed, what minimum security requirements are expected, and what due diligence is appropriate, among other considerations. Further, rather than compelling Covered Entities to impose particular contractual terms on all vendors, the Revised Draft Regulation softens this obligation by instead requiring entities to establish "relevant guidelines" addressing due diligence and/or contractual provisions covering such topics as the vendor's relevant policies and procedures, representations and warranties concerning those policies and procedures, and notice of Cybersecurity Events, among other items.

Incident Response Plan

The detailed requirements in the Original Draft Regulation related to incident response planning were relaxed somewhat by the introduction of a materiality threshold, such that a Covered Entity's incident response plan shall apply to a Cybersecurity Event "materially affecting" the confidentiality, integrity, or availability of the entity's systems or operations. Given the extremely broad definition of Cybersecurity Event, which includes even unsuccessful attempts to gain unauthorized system access regardless of how insignificant or common they may be, this change should have a significant limiting effect, depending on how DFS will interpret the materiality threshold.

Breach Notification to DFS

The Original Draft Regulation included rigorous requirements for reporting Cyber Events to DFS within 72 hours to a degree that industry commenters said would be unduly burdensome and would require the over-reporting of incidents that ultimately prove to be unverified or immaterial. DFS has responded by narrowing the reporting thresholds in the Revised Draft Regulation: While the 72-hour trigger is preserved, the clock now begins to run from a determination that a Cyber Event either (i) is otherwise required to be reported to any government, self-regulatory or supervisory body (eliminating the previous tripwire that would have required DFS notice, for example, even when the Covered Entity seeks law enforcement help voluntarily), or (ii) causes a "reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity" (eliminating the troublingly broad requirement of notice for any "actual or potential unauthorized tampering"). The revised approach should substantially reduce the reporting burden as a practical matter.

Miscellaneous Provisions

- DFS has clarified and broadened the scope of exemptions from the new regulation—in particular, specifying that an "employee, agent, representative or designee" is exempt, so long as that person "is covered by the cybersecurity program of the Covered Entity." This change will make obligations clearer and more predictable for companies that operate through decentralized networks of branches, independent agents and the like.
- Training and testing requirements are now modified, so that the training curriculum and periodic system testing must be tied to issues identified in a Covered Entity's Risk Assessment, and allowing for "continuous monitoring" instead of otherwise required annual penetration testing and bi-annual vulnerability assessments.

- Audit trail documentation requirements are reduced from six years to five, and the requirements are now more focused on materiality.
- Data retention requirements have been made somewhat more flexible by allowing retention of whatever is necessary for business operations "or for other legitimate business purposes" of the entity, or where targeted disposal is "not reasonably feasible" due to the manner in which the information is maintained.
- A new confidentiality standard specifies that information disclosed under the regulation is subject to exemption from disclosure requirements that would apply under other laws, such as the Banking and Insurance Laws and, apparently, New York's Freedom of Information Law.
- Various new transitional periods are specified for particular sections, the net effect of which collectively is to give industry more time to comply; the longest of these is two years to implement the Third Party Service Provider Security Policy requirements.

OPEN QUESTIONS AND PRACTICAL ISSUES

One of the most significant questions raised in the initial comment period that remains largely unaddressed by the Revised Draft Regulation is the extent to which DFS intends extraterritorial application of the Revised Draft Regulation. For example, as to a foreign-based banking institution with an affiliated branch in New York, will the bank choose to align its global cybersecurity program with New York's broad requirements (thereby allowing the branch to take advantage of the new provision allowing a Covered Entity to fall under the qualifying program of an Affiliate), or instead develop a separate cybersecurity program only for its New York operations? If the latter, will DFS seek to inquire about how information security is managed for interconnected systems that extend outside of New York?

While the move to a more risk-based, guidelines-style approach is certainly welcome, the Revised Draft Regulation remains very broad and detailed. The scope of the Revised Draft Regulation likely will make compliance a challenge for many Covered Entities and particularly for smaller, less-resourced firms that will need to rely on outside vendors to become compliant. And, of course, with the favorable change to more flexible concepts such as "reasonable likelihood" and "material[ity]" as to cyber risks and events comes a degree of uncertainty

about how DFS will interpret these concepts in practice. It will likely take several years before DFS's expectations on these points are clarified.

* * *

Please do not hesitate to contact us with any questions.

Debevoise & Plimpton | D&P

NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
PROPOSED
[23 NYCRR Part 500 (Financial Services Law)]

Cybersecurity Requirements for Financial Services Companies

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 upon publication in the State Register, 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 ~~cyber~~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:

(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~~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~~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~~concerning 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;~~which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account; or (v) biometric records.

(3) Any information or data, except age or gender, ~~that is~~in any form or medium created by~~,~~ or derived ~~or obtained~~ from a health care provider or an individual and that relates to

(i) 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~~, (ii) the provision of health care to any individual, or ~~from~~(iii) 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~~,~~ or any non-governmental entity, including but not limited to any nongovernmental partnership, corporation, branch, agency or 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 by attempting unauthorized penetration of databases or controls from outside or inside the Covered Entity's Information Systems.

(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 Assessment* means the risk assessment that each Covered Entity is required to conduct under section 500.09 of this Part.

~~(k)~~(l) *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)~~(m) *Senior Officer(s)* ~~mean~~means 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.

(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 500.02 Cybersecurity Program.

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

(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions:

(1) identify and assess internal and external ~~cyber risks by, at a minimum, identifying the~~cybersecurity risks that may threaten the security or integrity of 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~~applicable regulatory reporting obligations.

(c) A Covered Entity may meet the requirements of this Part by adopting a cybersecurity program maintained by an Affiliate, provided that the Affiliate's cybersecurity program covers the Covered Entity's Information Systems and Nonpublic Information and meets the requirements of this Part.

(d) All documentation and information relevant to the Covered Entity's cybersecurity program shall be made available to the superintendent upon request.

Section 500.03 Cybersecurity Policy.

(a) Cybersecurity Policy. Each Covered Entity shall implement and maintain a written ~~cybersecurity policy~~ policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, 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 be based on the

Covered Entity's Risk Assessment and address~~, at a minimum,~~ the following areas to the extent applicable to the Covered Entity's operations:

(1) information security;

(2) data governance and classification;

(3) asset inventory and device management;

~~(3)~~(4) access controls and identity management;

~~(4)~~(5) 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~~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 (for purposes of this Part, "Chief Information Security Officer" or "CISO"). The CISO may be employed by the Covered Entity, one of its Affiliates or a Third Party Service Provider. To the extent this requirement is met using ~~third party service providers~~a Third Party Service Provider or an Affiliate, the Covered Entity shall:

(1) ~~Retain~~retain responsibility for compliance with this Part;

(2) ~~Designate~~designate a senior member of the Covered Entity's personnel responsible for direction and oversight of the ~~third party service provider~~Third Party Service Provider; and

(3) ~~Require the third party service provider~~require the Third Party Service Provider to maintain a cybersecurity program that ~~meets~~protects the Covered Entity in accordance with the requirements of this Part.

(b) Report. The CISO of each Covered Entity shall ~~develop a~~ report~~,~~ in writing at least ~~bi-annually, as described herein. Such report shall be timely presented~~annually 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:~~The CISO shall report on the Covered Entity's cybersecurity program and material cybersecurity risks. The CISO shall consider to the extent applicable:

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

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

(3) ~~identify~~material cyber risks to the Covered Entity;

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

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

~~(6)~~(5) ~~include a summary of all~~ material Cybersecurity Events ~~that affected~~involving the Covered Entity during the time period addressed by the report.

Section 500.05 Penetration Testing and Vulnerability Assessments.

(a) The cybersecurity program for each Covered Entity shall~~, at a minimum, include:~~ include monitoring and testing, developed in accordance with the Covered Entity's Risk Assessment, designed to assess the effectiveness of the Covered Entity's cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments, and shall be done periodically. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct:

(1) annual penetration testing of the Covered Entity's Information Systems ~~at least annually~~determined each given year based on relevant identified risks in accordance with the Risk Assessment; and

(2) bi-annual vulnerability ~~assessment of~~assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems ~~at least quarterly~~based on the Risk Assessment.

Section 500.06 Audit Trail.

(a) ~~The cybersecurity program for each~~Each Covered Entity shall~~, at a minimum, include implementing and maintaining audit trail~~ securely maintain systems that, to the extent applicable and based on its Risk Assessment:

(1) ~~track and maintain data that allows for the complete and accurate reconstruction of all~~are designed to reconstruct material financial transactions ~~and accounting necessary to enable~~sufficient to support normal operations and obligations of the Covered Entity ~~to detect;~~ and ~~respond to a Cybersecurity Event;~~

(2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.

~~(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~~

(b) Each Covered Entity shall maintain records ~~produced as part of the audit trail~~required by this section for not fewer than ~~six~~five years.

Section 500.07 Access Privileges.

As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user 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~~and procedures for evaluating, assessing ~~and~~or testing the security of ~~all~~ externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment.

(b) All such procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the Covered Entity ~~at least annually~~.

Section 500.09 Risk Assessment.

(a) Each Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity's Information Systems sufficient to inform the design of the cybersecurity program as required by this Part. Such Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations. The Covered Entity's Risk Assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems.

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

~~(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 cybersecurity risks or threats facing the Covered Entity;

(2) criteria for the assessment of the confidentiality, integrity, security and availability of the Covered Entity's Information Systems and Nonpublic Information, 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~~Risk Assessment and how the cybersecurity program will address the 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~~utilize qualified cybersecurity personnel of the Covered Entity, an Affiliate or a Third Party Service Provider sufficient to manage the Covered Entity's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in section 500.02(b)(1)-(~~5~~6) of this Part;

(2) provide ~~for and require all~~ cybersecurity personnel ~~to attend regular~~with cybersecurity ~~update~~updates and training ~~sessions~~sufficient to address relevant cybersecurity risks; and

(3) ~~require~~verify that key cybersecurity personnel ~~to~~ take steps to ~~stay abreast~~maintain current knowledge of changing cybersecurity threats and countermeasures.

(4) A Covered Entity may choose to utilize ~~a~~an Affiliate or qualified ~~third party~~Third Party Service Provider 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~~Service Provider Security Policy.

(a) Third Party ~~Information Security~~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 parties doing business with the Covered Entity~~Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address~~, at a minimum,~~ to the ~~following areas~~extent applicable:

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

(2) minimum cybersecurity practices required to be met by such ~~third parties~~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 parties~~Third Party Service Providers; and

(4) periodic assessment~~, at least annually, of such third parties~~ 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 ~~establishing preferred provisions to be included in contracts with third party service providers, including provisions addressing,~~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 ~~set forth in Section~~defined by section 500.12 to limit access to sensitive systems and Nonpublic Information;

(2) the Third Party Service Provider's policies and procedures for use of encryption as defined by section 500.15 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;~~directly impacting the Covered Entity's Information Systems or Non-public Information being held by the Third Party Service Provider; and

~~(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)~~(4) 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~~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~~; and~~.

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

(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.

Section 500.12 Multi-Factor Authentication.

(a) Multi-Factor Authentication. ~~Each~~Based on its Risk Assessment, each Covered Entity shall~~:~~ use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.

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

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

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

~~(c)~~(b) ~~support~~ Multi-Factor Authentication shall be utilized for any individual accessing ~~web applications that capture, display or interface with Nonpublic Information.~~the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.

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~~secure disposal on a periodic basis of any Nonpublic Information identified in 500.01(g)(2)-(~~4~~3) that is no longer necessary for ~~the provision of the products or services for which such information was provided to~~business operations or for other legitimate business purposes of the Covered Entity, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Section 500.14 Training and Monitoring.

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

(1) 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

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

Section 500.15 Encryption of Nonpublic Information.

(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall ~~encrypt all~~implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.

(1) To the extent a Covered Entity determines that encryption of Nonpublic Information in transit ~~is currently~~over external networks is infeasible, the Covered ~~Entities~~Entity may instead secure such Nonpublic Information using ~~appropriate~~effective 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.~~

(2) To the extent a Covered Entity determines that encryption of Nonpublic Information at rest is ~~currently~~ infeasible, the Covered ~~Entities~~Entity may instead secure such Nonpublic Information using ~~appropriate~~effective 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.~~

(b) To the extent that a Covered Entity is utilizing compensating controls under (a) above, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.

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

materially 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 or operations.

(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) identification of requirements for the 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 as necessary 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~~from a determination that a Cybersecurity Event~~. Such Cybersecurity Events include, but are not limited to~~ as follows has occurred:

(1) ~~any~~ Cybersecurity ~~Event~~Events of which notice is required to be provided to any government ~~or~~body, self-regulatory agency or any other supervisory body; and

(2) ~~any~~ Cybersecurity ~~Event involving the actual or potential unauthorized tampering with, or access to or use of, Nonpublic Information.~~Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

(b) Annually each Covered Entity shall submit to the superintendent a written statement by ~~January~~February 15, in such form set forth as ~~Exhibit~~Appendix 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. 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.

~~(1) 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~~Confidentiality.

Information provided by a Covered Entity pursuant to this Part is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law.

Section 500.19 Exemptions.

(a) Limited Exemption. Each Covered Entity with: ~~(1) fewer than 1000 customers in each of the last three calendar years, and~~

(1) fewer than 10 employees including any independent contractors, or

(2) less than $5,000,000 in gross annual revenue in each of the last three fiscal years, ~~and~~or

(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.~~Sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(b) An employee, agent, representative or designee of a Covered Entity, who is itself a Covered Entity, is exempt from this Part and need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the Covered Entity.

(c) A Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information shall be exempt from the requirements of Sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(d) A Covered Entity that qualifies for an exemption pursuant to this section shall file a Notice of Exemption in such form set forth as Appendix B.

~~(b)~~(e) In the event that a Covered Entity, as of its most recent fiscal year end, ceases to qualify for ~~the limited~~an 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 applicable requirements of this Part.

Section ~~500.19~~500.20 Enforcement.

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

Section ~~500.20~~500.21 Effective Date.

This ~~part~~Part will be effective ~~January~~March 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~~section 500.17(b) commencing ~~January~~February 15, 2018.

Section ~~500.21~~500.22 Transitional ~~Period~~Periods.

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

(b) The following provisions shall include additional transitional periods. Covered Entities shall have:

(1) One year from the effective date of this Part to comply with the requirements of sections 500.04(b), 500.05, 500.09, 500.12, and 500.14(a)(2) of this Part.

(2) Eighteen months from the effective date of this Part to comply with the requirements of sections 500.06, 500.08, 500.13, 500.14 (a)(1) and 500.15 of this Part.

(3) Two years from the effective date of this Part to comply with the requirements of section 500.11 of this Part.

Section ~~500.22~~500.23 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~~APPENDIX A (Part 500)

_____

(Covered Entity Name)

February ~~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]

APPENDIX B (Part 500)

(Covered Entity Name)

(Date)_____

Notice of Exemption

In accordance with 23 NYCRR § 500.19(d), (Covered Entity Name) hereby provides notice that (Covered Entity Name) qualifies for the following Exemption(s) under 23 NYCRR § 500.19 (check all that apply):

☐ Section 500.19(a)(1)

☐ Section 500.19(a)(2)

☐ Section 500.19(a)(3)

☐ Section 500.19(b)

☐ Section 500.19(c)

If you have any question or concerns regarding this notice, please contact:

(Insert name, title, and full contact information)

(Name)_____ Date:_____
(Title)
(Covered Entity Name)

[DFS Portal Filing Instructions]