The Clearing House
At the Center of Banking Since 1853®

January 27, 2017

Via Electronic Mail

Ms. Cassandra Lentchner
New York State Department of Financial Services
One State Street
New York, NY 10004

Re: Proposed Cybersecurity Requirements for Financial Services Companies (ID No. DFS-39-16-00008P)

Dear Ms. Lentchner:

The Clearing House Association L.L.C.[1] appreciates the opportunity to provide our comments on the revised proposal by the New York State Department of Financial Services ("the **NYDFS**") to establish new Cybersecurity Requirements for Financial Services Companies (the "**Revised Proposal**"). We are grateful for your consideration of the comments we submitted on November 14, 2016 on the NYDFS' original proposal, along with the comments from other stakeholders and interested parties. The Revised Proposal in many ways represents a substantial improvement over the NYDFS' original proposal.

We want to emphasize again that the Clearing House and its member-owner banks are deeply committed to the shared public and private sector objectives the Revised Proposal is intended to advance: ensuring the confidentiality and integrity of New York customer financial information, defeating cyber criminals, and ensuring the safety and resiliency of the New York financial services industry's digital infrastructure. We believe that the Revised Proposal includes many helpful provisions that will serve these important goals, and we believe the changes that

[1] The Clearing House is a banking association and payments company that is owned by the largest commercial banks and dates back to 1853. The Clearing House Association L.L.C is a nonpartisan organization that engages in research, analysis, advocacy and litigation focused on financial regulation that supports a safe, sound and competitive banking system. Its affiliate, The Clearing House Payments Company L.L.C., owns and operates core payments system infrastructure in the United States and is currently working to modernize that infrastructure by building a new, ubiquitous, real-time payment system. The Payments Company is the only private-sector ACH and wire operator in the United States, clearing and settling nearly $2 trillion in U.S. dollar payments each day, representing half of all commercial ACH and wire volume.

A list of The Clearing House member banks is available at: https://www.theclearinghouse.org/about-tch/tch-owner-banks.

the NYDFS has made that are designed to make the requirements more risk-based have substantially strengthened and improved the proposed regulations.

Notwithstanding this progress, we believe that elements of the Revised Proposal can be made still more effective and consistent with the NYDFS' goals, and we respectfully offer the following recommendations for further revision.

I. Encryption of Nonpublic Information

The discussion of encryption in Section 500.15 of the Revised Proposal represents an improvement over the requirements outlined in the original proposal in its recognition that decisions about the use of controls, including encryption, should rest on a Covered Entity's Risk Assessments and that alternative controls may in certain cases be used instead of encryption.[2] We acknowledge and appreciate these improvements but believe that this section of the Revised Proposal should still be amended in two respects.

First, as we explained in our earlier letter, treating data transmitted or stored internally and data transmitted externally in the same way when it comes to encryption is not an effective security approach. Encrypting all *internally* transmitted or stored Nonpublic Information as defined in the Revised Proposal would impose an enormous burden on Covered Entities without proportional benefits to them or consumers. Such prescriptive and non-risk based requirements would produce unreasonable infrastructure costs, especially for small and mid-size firms, and unrealistic regulatory compliance validation standards. It would also frequently hinder existing network data monitoring controls. Encryption of internally held data may in some instances require that applications using that data hold decryption keys locally, thereby increasing vulnerabilities. Encryption of internal data in transit would hinder the ability of Covered Entities to monitor internal flows for anomalies, and the data would have to be decrypted to be used in any event. In contrast, encryption for external transmissions is currently considered best practice and should be required unless an exception applies.

Second, while the Revised Proposal recognizes the possibility of Covered Entities using alternative controls rather than encryption, it imposes too high a hurdle for the adoption of such alternatives. It appears to provide for use of alternative controls only when encryption is "infeasible." The test should be relative effectiveness, not feasibility. If encryption is feasible, but less effective than a set of alternative controls, how would it be rational to adopt the less effective alternative? A rigid "infeasibility" standard seems inconsistent with the NYDFS' stated intent that "each Covered Entity should model its Cybersecurity Program on the Covered Entity's cybersecurity risks."[3] Thus, we would recommend revising Section 500.15 to read as follows:

---

[2] As explained in our earlier letter, while encryption is appropriate—and employed—in many circumstances, we think it important to recognize that other controls may be at least as, if not more, effective in certain circumstances. Examples of those compensating controls include network segmentation, logical access controls, monitoring of privileged access activity, strict limitations on privileged access staff, including prompt removal of access upon loss of necessity for it.

[3] "Assessment of Public Comment," NYS Register (Dec. 28, 2016), p. 25.

Section 500.15 Encryption of Nonpublic Information.

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

(1) To the extent a Covered Entity determines that encryption of Nonpublic Information in transit over external networks is ~~infeasible~~ not reasonably feasible or use of reasonably equivalent or more secure controls are available, the Covered Entity may instead secure such Nonpublic Information using effective alternative ~~compensating~~ controls reviewed and approved by the Covered Entity's CISO.

~~(2) To the extent a Covered Entity determines that encryption of Nonpublic Information at rest is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.~~

(b) To the extent that a Covered Entity is utilizing ~~compensating~~ controls other than encryption for Nonpublic Information in transit over external networks under (a) above, the CISO shall review at least annually to determine either that encryption is reasonably infeasible or that the controls are at least as or more effective at protecting the Nonpublic Information to which they are applied than would be encryption.[4]

---

[4] Consistent with the changes just recommended in Section 500.15, we recommend as well parallel revisions to Section 500.11(b)(2) which relates to guidelines of Covered Entities with respect to Third Party Service Providers, as follows:

> (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~~ held or transmitted by the Third Party Service Provider in connection with its services to the Cover Entity, which shall include encryption for Nonpublic Information in transit over external networks;

Similarly, we recommend a technical change to Section 500.11(b)(1) (Third Party Service Provider Security Policy) to align that Section with language included in Section 500.12 of the Revised Proposal which relates to Multi-Factor Authentication:

> (1) the Third Party Service Provider's policies and procedures for access controls including its use of effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to sensitive systems and Nonpublic Information in

~~, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.~~

II. Audit Trail

Information required to be maintained pursuant to Section 500.06 under the Revised Proposal is appropriately linked to a Covered Entity's Risk Assessments. Nonetheless, we remain concerned that the requirements of that Section would appear to impose document retention obligations leading to the retention of too much information especially as it relates to audit trails in Section 500.06(a)(2) as well as to certain interpretative difficulties. Given subsection (a)(2)'s apparently forward-looking purpose, as opposed to the retrospective, forensic focus of subsection (a)(1), it will not be readily apparent whether at some point in the future a given data element could be relevant to a Cybersecurity Event. While the Revised Proposal appropriately indicates that the requirement to create an audit trail is based on Risk Assessments, a five-year retention obligation could effectively lead firms to conservatively retain a broad universe of information under the notion that any audit trail that could be relevant to a future material Cybersecurity Event should be retained for 5 years (including, e.g., log-in information). We also believe that subsection (a)(1)'s use of the term "reconstruct" could lead to differing interpretations. We would thus recommend that Section 500.06 be amended in the following respects:

> 500.06 Audit Trial
>
> (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessments:
>
> (1) are designed to retain evidence of ~~reconstruct~~ material financial transactions sufficient to support the rights ~~normal operations~~ and obligations of the Covered Entity with respect to such transactions; and
>
> (2) include audit trails reasonably designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming a~~ny~~ material part of the normal operations of the Covered Entity.
>
> (b) Each Covered Entity shall maintain records required by Section 500.06 (a)(1) ~~this section~~ for not fewer than five years.

---

connection with its services to the Covered Entity in accordance with Section 500.12 of this Part.

III. Definitions of "Non-Public Information" and "Publicly Available Information"

The revisions made to the definition of "Nonpublic Information" in Section 500.01(g) represent steps forward from the definition used in the original Proposal. However, we believe the revised definition still sweeps in more information than is reasonable. We would recommend the following changes.

First, the definition of "Non-Public Information" relies on the related definition of "Publicly Available Information," but the latter remains restricted to information only from certain sources. We would recommend that the definition of "Publicly Available Information" be revised to be simpler and more in accord with common understandings of that term: "Publicly Available Information is information that a Covered Entity has a reasonable basis to believe is in the public domain."[5]

Second, prong (3) in the definition of "Nonpublic Information," concerning health information, seems unnecessary for a regulation directed at protecting New York consumers and ensuring the safe and sound operation of financial services companies where there is already a well-established federal framework in place to protect against the unauthorized disclosure of personal health information, i.e., the Security and Privacy Rules under the Health Insurance Portability and Accountability Act ("HIPAA"). Thus, we would recommend deleting prong (3).

If the NYDFS nonetheless elects to retain prong (3), its language should be brought into conformity with the appropriate definitions under HIPAA by cross-reference or, at the very least, by revision of the language used in the Revised Proposal. The language in prong (3) appears to draw on terms used in the Security Rule, but it omits language from HIPAA that restricts the definition and so extends even more broadly than the federal definition. At a minimum, the terms of prong (3) should be made no broader than provisions of HIPAA from where they are drawn. The HIPAA definition of "individually identifiable health information" refers to information that:

> (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
>
> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
>
> (i) That identifies the individual; or

[5] In its "Assessment of Public Comment," the NYDFS acknowledged that commenters had raised this concern in response to the original Proposal. In response, the NYDFS simply asserts that it believes the definition "is appropriate in the context of the revised proposed regulation." However, the NYDFS does not explain how it reached that conclusion. We urge the NYDFS to reconsider the point.

> (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Prong (3) omits the limiting language in (2)(i) and (2)(ii) of the HIPAA definition and includes information created by or derived from an individual, which does not appear in the HIPAA definition. Prong (3) also omits the exclusions in the HIPAA definition of "protected health information," among which is "individually identifiable health information" held "[i]n employment records held by a covered entity in its role as employer."

IV. Certification

We appreciate modifications made to the annual certification requirement in Section 500.17(b) of the Revised Proposal. However, it remains overly rigid and overly broad in ways that we believe may not have been intended and which can easily be remedied. Given the liability that may arise from an inaccurate certification, we think it essential that certifying officials be permitted to identify any areas of non-compliance—and/or identified areas requiring improvement—as well through a qualified certification. While Covered Entities will of course strive for complete compliance, the certification requirement should recognize the best practice of identifying areas in need of improvement in the constantly evolving area of information security.

In addition, the document retention requirement for the certification is written in terms (i.e., "*all* records, schedules and data") that might suggest a requirement to maintain literally all documentation that plays a role in supporting the certification. The resources expended to identify, store, and track such materials would be better spent on cyber risk reduction efforts. Accordingly, the document retention requirement should be narrowed to those sufficient to support the certification of compliance.

Finally, in order to give Covered Entities sufficient time to make the required certification of compliance as of the end of the most recent year-end (which appears to be contemplated by the form set forth as Annex A), the deadline should be moved from February 15 to April 15. For the initial certification in 2018, this additional time would assist Covered Entities in their roll-out of the internal processes necessary to support the certification. Going forward, firms recognize the need for additional time in view of end-of-year deadlines and responsibilities and to allow them to coordinate their respective certification processes, as appropriate, with the April 15 deadline provided under Part 504 of the NYDFS' regulations and/or other annual certification processes.

We therefore recommend that Section 500.17(b) be revised to read as follows:

> (b) Annually each Covered Entity shall submit to the superintendent a written statement by <u>April 15</u>, in such form set forth as Appendix A, certifying that the Covered Entity is in compliance with the requirements set forth in this Part, <u>except as specified on such certification</u>. Each Covered Entity shall maintain for examination by the Department ~~all~~ records, schedules and data <u>sufficient to</u> support~~ing~~ 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 during the period of time such documentation is required to be retained under this Part.

As we discuss more fully below, it is important to emphasize that the certifications required under Section 500.17(b) and the documentation required to be maintained in support of the certification—and shared with the Superintendent upon demand—may contain highly sensitive information the confidentiality of which must be strictly protected. Covered Entities could potentially become targets of threat actors of any size and sophistication via simple access to public records should those records contain information regarding a Covered Entity's cybersecurity efforts and risk profile.

V. Definition of "Risk Assessment"

In our November 14 letter addressing the original proposal, we urged the NYDFS to incorporate a risk-based approach into the proposal. We applaud the NYDFS for making revisions in many sections of the Revised Proposal intended to tie the requirements to Covered Entities' assessments of the risks they face. Many of those revisions involve inserting references to the required Risk Assessment in the sections defining particular required practices.

We remain concerned, however, that the Revised Proposal's definition of "Risk Assessment" might be understood to refer to a single, enterprise-wide assessment, conducted periodically, and updated in a single uniform way. A risk-based approach will often entail conducting risk assessments on different components of Information Systems as needed, in accordance with an entity's risk profile. As the National Institute of Standards and Technology ("NIST") has explained, risk assessment is one component of risk management, and its purpose is to identify: (1) threats to the organization; (2) vulnerabilities internal and external to the organization; (3) the harm that may occur given the potential for threats exploiting vulnerabilities; and (4) the likelihood that harm will occur.[6] Once risk is determined based on the assessment, an organization may respond accordingly.

To be most effective, the language should reflect the sound practice that risk assessments should be carried out on different parts of Information Systems as needed, rather than as a single enterprise-wide endeavor.

In addition, we believe Section 500.09's language raises several concerns that could be remedied through simple wording changes.

First, by referring to "a periodic Risk Assessment of the Covered Entity's Information Systems," Section 500.09 would seem to imply the assessment is solely of the Covered Entity's

---

[6] *See* NIST Special Publication 800-30: Guide for Conducting Risk Assessments, Joint Task Force Transformation Initiative, (September 2012).

systems, when firms with multiple affiliates often conduct their broader risk assessments in a more comprehensive way. To avoid misallocation of resources by repeating risk assessments solely at the Covered Entity level, Section 500.09 should be revised to clarify that a broader assessment is acceptable as long as it includes the Covered Entity's Information Systems.

Second, by stating that the "Covered Entity shall conduct" the Risk Assessment, the provision would seem to imply that the Covered Entity must do the Risk Assessment itself, when many firms will have the assessment conducted by an Affiliate. We would thus recommend clarification that an Affiliate's risk assessment may satisfy the provision.

Third, a major objective of doing risk assessments is to allow a firm to assess its risks by impact and probability and then apply the applicable controls as appropriate based on the assessed risk. The current language ("based on its Risk Assessment") does not clarify that firms may apply the controls as appropriate based on the assessed risk (the approach implied in the NYDFS' stated intent of allowing firms to create cybersecurity programs that match relevant risks).

Fourth, some of the Revised Proposal's provisions (namely 500.05 (Pen Testing), 500.12(b) (Multifactor Authentication) and 500.15 (Encryption)), prescribe (subject to varying conditions that must be met to employ an alternative) specific technological procedures or controls that may be superseded in the future. We believe the Revised Proposal should clarify the ability of firms to use superseding controls in each of these cases that are equally or more effective, as determined by the Covered Entity's CISO.

We accordingly recommend that Section 500.09 be revised as follows:

> Section 500.09 Risk Assessments
>
> (a) Each Covered Entity shall conduct periodic Risk Assessments (or adopt those of an Affiliate) that include the Covered Entity's Information Systems (any such assessment, the "Risk Assessment" or "Covered Entity's Risk Assessment") and are sufficient to inform the design of the cybersecurity program as required by this Part, including the appropriateness of the program's controls to the level and likelihood of the risk identified. Such Risk Assessments shall be carried out as reasonably necessary to address material changes to the Covered Entity's Information Systems, Nonpublic Information or business operations. The Covered Entity's Risk Assessments 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. In the event a Covered Entity's CISO (or a qualified designee) has approved in writing the use of reasonably equivalent or more secure controls as

compared to the default control set forth in Section 500.05, 500.12(b), and/or 500.15, the Covered Entity may comply with such Section(s) by applying the equivalent or more secure control.

(b) Risk Assessments shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures may include:

(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 the identified risks; and

(3) requirements describing how identified risks will be mitigated or accepted, as necessary, based on the Risk Assessments and how the Covered Entity will address the risks.

To conform with the revised language in Section 500.09, we would recommend that the term Risk Assessment be made plural throughout the document and the definition of "Risk Assessment" in Section 500.01(k) be revised as follows:

Section 500.01(k) *Risk Assessment* means the risk assessments that each Covered Entity carries out, as necessary, under section 500.01 of this Part.

VI. Definition of "Cybersecurity Program"

In our view, the definition of "Cybersecurity Program" has been improved. We would recommend two further clusters of wording changes, which we believe would capture more accurately NYDFS' intent. The first makes clear that a Covered Entity may in part rely on its own cybersecurity program and in part rely on the cybersecurity program of an affiliate. The second makes clear that the documentation required to be preserved is the documentation specifically tied to the Revised Proposal's requirements, not every document that might in some way be "relevant" to the Covered Entity's cybersecurity program, a term of uncertain scope that will lead to uncertainty about how to fulfill the requirement.

(c) A Covered Entity may meet any particular requirement of this Part by adopting, in whole or in part, a cybersecurity program maintained by an Affiliate, provided that any adopted Affiliate's cybersecurity program (or part thereof) applies to the Covered Entity's Information Systems and Nonpublic Information and, to the extent an adopted portion applies to the Covered Entity's Information Systems and Nonpublic Information, meets the requirements of the Part in question.

(d) All documentation required to be maintained pursuant to this Part shall be made available to the superintendent upon request during the period of time such documentation is required to be retained.

VII. Definition of "CISO"

We are grateful for the revisions to Section 500.04, which have helped address concerns about reliance on affiliates or third-parties to fulfill this requirement. We believe the terms of the Revised Proposal, however, may have inadvertently failed to distinguish sufficiently between reliance on affiliates versus reliance on third parties. We would recommend the following revision in order to clarify that prongs (2) and (3) of the Revised Proposal apply only when a Covered Entity is relying on a Third Party Service Provider, not an Affiliate.

Section 500.04 Chief Information Security Officer.

(a) Chief Information Security Officer. Each Covered Entity shall designate a qualified individual 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 a Third Party Service Provider ~~or an Affiliate~~, the Covered Entity shall retain responsibility for compliance with this Part.~~:~~ To the extent this requirement is met using a Third Party Service Provider, the Covered Entity shall:

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

(~~2~~1) designate a senior member of the Covered Entity's personnel responsible for direction and oversight of the Third Party Service Provider; and

(~~3~~2) require the Third Party Service Provider to maintain a cybersecurity program that protects the Covered Entity in accordance with the requirements of this Part.

VIII. Confidentiality

We believe the addition of a confidentiality provision to the Revised Proposal represents an important improvement. But we are concerned that cross-referencing provisions of other laws will still leave uncertainty about whether information required to be provided to the NYDFS would be protected. Under the Revised Proposal, financial institutions will share sensitive details about risk profiles and their cybersecurity efforts, which would expose them to a variety of risks if obtained by outside actors. We would thus recommend that information required to be provided under the Revised Proposal's Notification requirements be defined as protected under

section 87(2)(d) of New York's Freedom of Information Law. We would therefore recommend that the Section 500.18 be revised as follows:

> Section 500.18 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 and shall be treated as falling within section 87(2)(d) of New York's Freedom of Information Law.

IX. Penetration Testing

We appreciate that Section 500.05 of the Revised Proposal incorporates reliance on a Covered Entity's Risk Assessments. Our recommendations in this regard are intended to recognize that the appropriateness and appropriate frequency of penetration testing and vulnerability assessments will vary across different components of a Covered Entity's IT infrastructure. In order to take this into account, we would recommend revising Section 500.05 to clarify that the annual penetration testing and bi-annual vulnerability assessment requirements (absent alternative effective means to monitor on an ongoing basis) should apply only for the Information Systems determined to be "high risk" pursuant to the Risk Assessment.[7]

> Section 500.05 Penetration Testing and Vulnerability Assessments.
>
> (a) The cybersecurity program for each Covered Entity shall 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. Absent other reasonably effective means for monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct the following, as applicable, for the Covered Entity's Information Systems determined to be high risk pursuant to its Risk Assessments:
>
> (1) annual penetration testing of the Covered Entity's Information Systems ~~determined each given year based on relevant identified risks in accordance with the Risk Assessment~~; and

[7] Not all Information Systems may have an IP address, and accordingly, vulnerability assessment would be performed only on those systems that have an IP address.

(2) bi-annual vulnerability 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 ~~based on the Risk Assessment~~.

X. Definition of "Covered Entity"

A. Clarification of the Scope of the Definition of "Covered Entity"

We believe the definition of "Covered Entity" combined with the exemptions in Section 500.19 might inadvertently be read to include entities and individuals not licensed or chartered by and not subject to primary supervision by the NYDFS and not otherwise intended by the NYDFS to be covered by the Revised Proposal but that are nonetheless required to receive NYDFS authorization to conduct business in New York. In the NYS Register (December 28, 2016), the NYDFS stated its intent that the Revised Proposal cover "financial services providers regulated by the Department." As currently drafted, however, the definition of "Covered Entity" (especially in view of the very broad language used such as "similar authorization") could potentially be read as sweeping in virtually any company that may be subject to an NYDFS filing or notice or similar requirement under one of the enumerated laws (Banking Law, Insurance Law, Financial Services Law) even when the entity is not regulated or principally supervised by the NYDFS as a New York banking, insurance or other type of financial services entity. This language could, for example, possibly be interpreted to cover an out-of-state (domestic) banking entity that is required under the Banking Law, to the extent consistent with the Riegle-Neal and Dodd-Frank Acts, to submit a filing to the NYDFS to establish a branch office in New York[8] or possibly even a non-banking entity that has received NYDFS authorization to do business in New York using certain words in its name (e.g., such as "bank").[9] We do not believe that these are the types of entities that the NYDFS intended to treat as "regulated" entities for purposes of application of Part 500 or that should be appropriately subject to NYDFS cybersecurity supervision.

We would again recommend that the definition of "Covered Entity" also be clarified to ensure that the final regulations would apply only to the New York-licensed branches or agencies of foreign banking organizations, not the foreign banking organization as a whole. Under the current definition of Covered Entity, the foreign banking organization itself might be understood as the "Person operating under or required to operate under a license" and thus a Covered Entity. Applying the regulation to the New York-licensed branches of foreign banks as if they were separate from the home office would be consistent with the approach taken in many other contexts under applicable U.S. federal and state banking law and reduce potential conflicts with

---

[8] *See* The New York Banking Law Sections 223-A and 224. The applicable NYDFS form for an out-of-state (domestic) chartered bank to establish a New York branch is an expedited application form which exempts such banks from providing information (e.g., including a description of security measures) otherwise required by New York chartered banks to establish a New York branch. See Application form entitled "Permission to Open & Occupy a Branch Office" (Part F "New York Branches of Out-of-State Banks").

[9] *See* New York Banking Law Sections 132 and 669.

home country requirements. For example, under the Banking Law and the federal International Banking Act frameworks, a U.S. branch of a non-U.S. bank is treated for most purposes as if it were a U.S. bank (e.g., under New York bank insolvency law, the Superintendent has the authority to seize all the assets of the foreign bank located in New York).

To eliminate the ambiguities described above and to define the scope of Part 500 in a manner which we understand to be consistent with the NYDFS' stated intention, we believe a simple change could ensure these clarifications in the following way:

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

"Banking Law Regulated Entity" would then build upon the definition of "Bank Regulated Institutions" and "Nonbank Regulated Institutions" in NYDFS' Transaction Monitoring Rule (Part 504) as follows:

> *Banking Law Regulated Entities* means (a) all banks, trust companies, private bankers, savings banks, and savings and loan associations and other institutions or entities chartered pursuant to the Banking Law and all branches and agencies of foreign banking corporations licensed pursuant to the Banking Law to conduct banking operations in New York and (b) all check cashers, money transmitters, budget planners, licensed lenders, premium finance agencies, sales finance agencies, and mortgage companies licensed pursuant to the Banking Law.

B. NYDFS Superintendent Authority To Grant Waivers

In certain cases, an entity may be required to receive an NYDFS license to engage in New York in a specific activity (e.g., insurance brokerage) but the entity may already be subject to a requirement to apply a cybersecurity framework on a firm-wide or enterprise-wide basis by its principal regulator. Such an entity could include, for example, a national bank regulated by the OCC and subject to federal cybersecurity standards with a relatively small NYDFS-licensed insurance brokerage business representing a *de minimis* portion of its overall business. We applaud the NYDFS' statement in the NYS Register (December 28, 2016) that the "Department has been continually mindful of other standards and approaches" as it suggests that the NYDFS recognizes that the impact of its regulations (e.g., because they appear to impose requirements at the Covered Entity level rather than only covering the information generated by or systems used for NYDFS-licensed activities) could go well beyond New York and New York consumers.[10]

[10] The NYS Register, page 23-24 (Dec. 28, 2016) notes the NYDFS' interest in protecting New York consumers of NYDFS regulated entities and the safe and sound operation of NYDFS-regulated entities. These interests appear to be greatest with respect to the in-state activities of New York-licensed entities organized outside of New York and, more generally, with respect to the Nonpublic Information of New York consumers. In this

Particularly helpful in these cases would be for the Superintendent to have the authority to determine that the applicable enterprise-wide requirements are equivalent or substantially equivalent to the Part 500 requirements and thus application of Part 500 could be waived on the grounds that they are not necessary to ensure customer protection or safety and soundness. We suggest that this is a practical approach where the objectives of the NYDFS may be accomplished through otherwise applicable non-NYDFS requirements. In certain cases, we believe that conflicting requirements, additional complexities of complying with multiple frameworks, and/or other considerations could potentially outweigh strict application of Part 500.[11]

A waiver provision might look like this:[12]

> Section 500.24 Waiver.
>
> (a) The superintendent or his designee shall have the power to waive certain requirements of this regulation and exempt certain Covered Entities provided such variations are in harmony with its spirit, if the superintendent shall find that such variations are necessary or appropriate in his sole discretion.
>
> (b) Waivers shall be granted in accordance with the following procedure: Requests for waivers shall be in writing; addressed to the superintendent; and state in reasonable detail satisfactory to the superintendent the basis of the request for the waiver.
>
> (c) No provision of this regulation shall be deemed waived unless written notice of waiver from the superintendent shall have been issued.

C. Clarification of Application to Individuals

The Section 500.19(b) exemption addresses important questions and concerns regarding compliance with Part 500 responsibilities for employees, agents, representatives or designees of Covered Entities. We suggest, however, that the NYDFS make clearer that (whether through

---

regard, the NYDFS should consider specifically limiting the reach of the regulation to the Nonpublic Information of New York consumers of licensed businesses or specifically tying the *de minimis* exception thresholds in Section 500.19 to New York-related business such that institutions with only a *de minimis* impact on New York customers need not come under the rule.

[11] It is not clear whether certain federally regulated banking organizations may become subject to conflicting regulatory requirements in the future. *See, e.g.*, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Enhanced Cyber Risk Management Standards, 81 Fed. Reg. at 74,315 (Oct. 26, 2016) (advance notice of proposed rulemaking on enhanced cyber risk management standards for financial institutions that have consolidated assets of $50 billion or more on an enterprise-wide basis, certain systemically important financial market infrastructures, and third-party service providers to these); *see also* 12 C.F.R. Part 7, Subpart D (OCC preemption and visitorial powers rules).

[12] *See generally* New York Banking Law Section 14(p) (granting the Superintendent authority to make variations from requirements of the New York Banking Law under certain circumstances).

modifications to the definition of Covered Entity, the Section 500.19(b) exemption or otherwise): (i) the Section 500.19(b) exemption is broadened to also cover any employees, agents, representatives or designees to the extent that they are covered by the cybersecurity program of a financial institution that is exempt under New York Banking Law, Insurance Law or Financial Services Law or NYDFS regulation from requirements to operate a business or activity under a NYDFS license, registration, charter, certificate, permit, or accreditation (and, therefore, the financial institution is not a Covered Entity as a technical matter), (ii) individual independent contractors of a Covered Entity (or "exempt" Covered Entity as described in (i) above) fall within the scope of the Section 500.19(b) exemption to the extent they are covered by the cybersecurity program of the Covered Entity, and (iii) as described in greater detail below, natural person licensees are only considered Covered Entities when performing NYDFS regulated/licensed activities. We believe that such clarifications would be consistent with the NYDFS' policy objectives and scope of the definition of Covered Entity.

Some companies and organizations that are not Covered Entities may employ individually licensed or authorized individuals (e.g., such as NYDFS-licensed insurance agents) who are Covered Entities under the Revised Proposal. In certain cases, such licensed employees/Covered Entities may be dual employees of a Covered Entity (e.g., a NYDFS-licensed insurance agency) and another affiliated entity that is not a Covered Entity (e.g., a broker-dealer or national bank that is not licensed under New York law). We believe that the Revised Proposal should clarify that a company which is not itself a Covered Entity should not be required to comply with Part 500 simply by virtue of employing individuals who are NYDFS-licensed and, conversely, such individuals will not be treated as Covered Entities in their capacity as employees of a non-Covered Entity assuming that such individuals do not engage in any NYDFS regulated/licensed activities in such capacity. We believe that in such cases, the individual employees should not be considered Covered Entities as they would not be "operating under" or required to operate under a license in such circumstances.

XI. No Private Right of Action

We think it important to make explicit a point we believe the NYDFS intended: that these regulations are to be enforced by the NYDFS and not by private parties. Allowing a private right of action would only divert resources away from efforts by Covered Entities to improve their cybersecurity. Making clear that the Revised Proposal may not create a private right of action would also be consistent with many other data security regulatory regimes, such as HIPAA, which make express that they do not afford the basis for private lawsuits. We would therefore recommend that Section 500.20 be revised as follows:

> Section 500.20 Enforcement; No Private Right of Action.
>
> (a) This regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws.
>
> (b) Any asserted noncompliance or attempt by the superintendent to enforce this regulation shall not give rise to a private right of action.

XII. Application Security

In order to ensure that this requirement, like others, is tied to a Covered Entity's Risk Assessments, we would recommend making that connection explicit:

> Section 500.08 Application Security
>
> (a) Each Covered Entity's cybersecurity program shall include written procedures, guidelines and/or standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment, in each case developed based on the Covered Entity's Risk Assessments.

* * * *

The Clearing House appreciates the opportunity to comment on the Revised Proposal. If you have any questions, please contact the undersigned by phone at 212.612.9220 or by email at gregg.rozansky@theclearinghouse.org.

Respectfully submitted,

Gregg Rozansky
Managing Director and
Senior Associate General Counsel
The Clearing House Association L.L.C.