November 14, 2016

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 proposal by the New York State Department of Financial Services ("**NYDFS**") to establish new Cybersecurity Requirements for Financial Services Companies (the "**Proposal**"). The Clearing House and its member-owner banks are deeply committed to the shared public and private sector objectives the Proposal is intended to advance: ensuring the confidentiality and integrity of customer financial information, defeating cyber criminals, and ensuring the safety and resiliency of the financial system's digital infrastructure. We believe that the Proposal includes many helpful provisions that will serve these important goals. We are concerned, however, that in some respects the Proposal could actually hinder rather than promote these goals, particularly by mandating certain specific practices or technologies that could potentially make the customer information and information technology of regulated entities less secure. Accordingly, we recommend that the NYDFS revise certain components of the Proposal to help ensure that any final regulations both are appropriately tailored to achieve their consumer

[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.

protection, information security and business continuity purposes, and allow regulated institutions to continue to employ a risk-based approach to respond effectively to the rapidly evolving cybersecurity threats.

This letter begins by addressing our principal thematic concern: that the final regulations be sufficiently principles-based and adaptable to permit evolution of Covered Entities' practices within a risk-management framework. We believe that such an approach is critical to enable institutions to adopt new technologies and risk-management techniques to respond to future threats while meeting consumer expectations. The letter then highlights specific elements of the Proposal that we believe should be modified to achieve the Proposal's overall policy objectives in a more effective, secure, and tailored manner consistent with a risk-based approach.

I. Risk-Based Approach

We understand that the NYDFS is seeking to establish generally applicable minimum regulatory standards for NYDFS-regulated financial institutions. Even with that goal in mind, we believe that a less prescriptive and more risk-based approach is essential. A "one size fits all" approach threatens to deprive Covered Entities of the flexibility and adaptability that are necessary to respond to the rapidly evolving landscape of cybersecurity threats and to take advantage of the rapidly evolving arsenal of cybersecurity best practices. As the recent *Guidance on Cyber Resilience for Financial Market Infrastructures* published by the Board of the International Organization of Securities Commissions notes, in stressing both the importance of a risk-based approach to cybersecurity and the wisdom of avoiding imposition of specific data security practices, "[t]he guidance is principles-based, recognising that the dynamic nature of cyber threats requires evolving methods to mitigate these threats. Guidance requiring specific measures today may quickly become ineffective in the future."[2] As the National Institute of Standards and Technology's ("**NIST**") Cybersecurity Framework similarly observes, "[t]o ensure extensibility and enable technical innovation," cybersecurity standards should be "technology neutral."[3] We believe our suggestions comport with Superintendent Vullo's statements that the Proposal was intended to provide "flexibility necessary to ensure that institutions can efficiently adapt to continued innovations."[4] For these reasons, placing specific requirements in the context of an overall risk-based approach—one that allows Covered Entities to assess their particular risk profile and employ appropriate compensating risk mitigation controls—is crucial to promoting the reduction of cybersecurity risk.[5]

---

[2] Board of the International Organization of Securities Commissions, *Guidance on Cyber Resilience for Financial Market Infrastructures* 7 (June 2016), available at http://www.bis.org/cpmi/publ/d138.pdf; *see also id*. at 4 ("cyber risks should be managed as part of an FMI's overall operational risk management framework").

[3] NIST Framework for Improving Critical Infrastructure Cybersecurity, v. 1.0, at 4 (Feb. 12, 2014) ("NIST Cybersecurity Framework").

[4] Christopher Mathews, Global Finance: New York Plans Cybersecurity Regulation for Banks, *Wall Street Journal* (Sept. 14, 206).

[5] Reliance on a risk-based framework is a fundamental common feature of every piece of cybersecurity guidance of which we are aware—from federal agencies, from industry experts, and from foreign regulators alike. As the Department of Homeland Security has put it, for example, "[c]ybersecurity is about more than implementing a

The NYDFS' own recently finalized Part 504 regulations prescribing anti-money laundering/economic sanctions transaction monitoring and filtering program requirements provide an instructive contrast to the Proposal in this respect. The transaction monitoring regulations require that regulated institutions maintain transaction monitoring and filtering programs "reasonably designed for the purpose of" accomplishing the regulations' core goals, drawing on a menu of "attributes, to the extent they are applicable." § 504.3(a), (b). Thus, unlike the Proposal, which includes more than a dozen specific requirements regardless of the extent of the required practices' contribution to any particular regulated institution's cybersecurity risk profile, the transaction monitoring regulations more clearly recognize that regulated institutions should be allowed to structure their own programs in light of their own operations and risk assessments in order to achieve the shared regulatory goal.

The Proposal's Introduction indicates that the NYDFS intended the Proposal to be risk-based.[6] We recognize that the NYDFS may have intended the incorporation of a "material

---

checklist of requirements—Cybersecurity is managing cyber risks to an ongoing and acceptable level." Department of Homeland Security, *Cyber Risk Management Primer for CEOs* , available at https://www.dhs.gov/sites/default/files/publications/C3%20Voluntary%20Program%20-%20Cyber%20Risk%20Management%20Primer%20for%20CEOs%20_5.pdf. As a recent study on federal cybersecurity efforts similarly concluded, "[t]he Department of Defense (DoD), Intelligence Community (IC), and Federal agencies via representation by the National Institute of Standards and Technology (NIST) have collectively taken action to move from a compliance-oriented approach to cyber security to one based on risk management." MITRE Corporation, "The Risk Management Framework and Cyber Resiliency" (2016), available at https://www.mitre.org/sites/default/files/publications/pr-16-0776-cyber-resiliency-and-the-risk-management-framework.pdf. For other examples reflecting the centrality of risk management as an organizing principle for cybersecurity, see FFIEC Cybersecurity Assessment Tool Frequently Asked Questions 1 (Oct. 17, 2016), available at https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT%20FAQs.pdf ("Management of financial institutions and management of third-party service providers are primarily responsible for assessing and mitigating their entities' cybersecurity risk. FFIEC member agencies developed the Assessment to help institutions' management identify their risks and determine their cybersecurity preparedness."); The Financial Industry Regulatory Authority (FINRA), *Report on Cybersecurity Practices* (February 2015), available at http://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf ("FINRA's objective is to focus firms on a risk management-based approach to cybersecurity. This enables firms to tailor their program to their particular circumstances; as every firm in our sweep emphasized, there is no one-size-fits-all approach to cybersecurity."); National Association of Insurance Commissioners, *Principles for Effective Cybersecurity: Insurance Regulatory Guidance*, available at http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf. ("Cybersecurity regulatory guidance for insurers and insurance producers must be flexible, scalable, practical and consistent with nationally recognized efforts such as those embodied in the National Institute of Standards and Technology (NIST) framework[; r]egulatory guidance must be risk-based and must consider the resources of the insurer or insurance producer, with the caveat that a minimum set of cybersecurity standards must be in place for all insurers and insurance producers that are physically connected to the Internet and/or other public data networks, regardless of size and scope of operations."); G7, *Fundamental Elements of Cybersecurity for the Financial Sector* (Oct. 2016), available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/559186/G7_Fundamental_Elements_Oct_2016.pdf. ("Entities in the financial sector should establish cybersecurity strategies and frameworks tailored to their nature, size, complexity, risk profile, and culture.").

[6] *See* Section 500.0 of the Proposal ("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

adverse impact" standard in the definition of "Nonpublic Information" and materiality standards in certain other provisions, along with the requirement in Section 500.09 for Covered Entities to undertake annual Risk Assessments, to achieve a risk-based approach. We believe, however, these provisions are not sufficient to ensure such an approach.

First, a properly-deployed risk-based approach requires, as the NIST Cybersecurity Framework and many other leading forms of guidance indicate, consideration of both the "likelihood that an event will occur and the resulting impact,"[7] while the term "material" only considers impact. Second, a materiality standard does not appear in many of the Proposal's provisions. Third, a materiality standard does not expressly authorize firms to use superseding controls where new or better technology or methods are available, or compensating controls where the prescribed controls are infeasible. Fourth, the results of the risk assessment required in Section 500.09 do not clearly relate to the application of the prescribed controls that would be required by the Proposal (e.g. encryption, data mapping, penetration testing, vendor assessments, etc.).

In light of all these considerations, and in order to achieve the NYDFS' stated objective to rely on a risk-based approach, we respectfully recommend that the NYDFS add a provision to the Proposal expressly recognizing the centrality of a risk-based approach, along the following lines:

> **Section 500.XX**
>
> To allow for strategic prioritization and revision of controls to respond to technological developments and evolving threats, companies may comply with any provision of this Part by employing a Risk-based approach and, by doing so in a manner satisfying the requirements of a Risk-based approach, will be in compliance with such provision, notwithstanding any provision in this Part 500. If a Covered Entity employs a Risk-based approach, the time periods specified in this Part shall be interpreted to be the regulatory minimum for the highest-risk categories (as applicable) and to apply to lower-risk categories only if appropriate, as determined pursuant to the Risk-based approach.[8] Upon the superintendent's request or the request of an examiner, Covered Entities shall provide the documentation required by the Risk-based approach or a summary thereof, or both, to demonstrate that appropriate controls have been deployed with respect to the applicable risk.

---

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.").

[7] NIST, Cybersecurity Framework 5 (2014) (risk-based approach requires an "ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance").

[8] These include the periods defined in Sections 500.05, 500.06, 500.08 and 500.11(a)(4) of the Proposal.

We would propose that the following definition of "Risk-based Approach" be added to Section 500.01, along the following lines:

> Risk-Based Approach means complying with a provision by (i) carrying out a risk assessment (including, as applicable, an assessment of Information Systems pursuant to § 500.09), for the purpose of identifying relevant risks and categorizing such risks by severity and probability, (ii) implementing the applicable measures or other superseding or compensating controls, in each case as appropriate in accordance with the level of risk, and (iii) maintaining supportive documentation of steps (i) and (ii).

Adding an express provision addressing compliance through a risk-based approach will ensure the establishment of the core minimum standards the NYDFS intends because Covered Entities would be expected to implement risk-management frameworks that, at a minimum, expressly address the areas of risk and controls the NYDFS identifies throughout the Proposal and document that appropriate controls have been deployed. Adding an express risk-based framework will also ensure the vitality of the NYDFS' regulatory regime over time because it is technology-neutral. And, for enterprises that have entities subject to both federal and NYDFS cybersecurity requirements, it will ensure greater efficiency in firms' compliance with their regulatory obligations, thus maximizing the resources available to reduce cybersecurity risk.

II. Definition of "Nonpublic Information"

The definition of "Nonpublic Information" in Section 500.01(g) plays a central role in defining the scope of the Proposal. A number of our concerns stem from the Proposal's broad definition of "Nonpublic Information." That definition is substantially broader than the definitions of sensitive information used in the guidance issued by federal financial regulators and by New York State itself in its data breach notification law.[9] Indeed, it is so broad that it could cover nearly all information maintained by a firm. The current definition would appear to encompass and thus require enhanced protective measures for documents or data with limited sensitivity, such as business email addresses, which may be "linkable to an individual," and single data elements, such as name, in isolation.

---

[9] New York's data breach notification law defines "private information" as:

> personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired: (1) social security number; (2) driver's license number or non-driver identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; "Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.

N.Y. General Business Law, § 899-aa(1)(b). "Personal information" in turn means "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person." *Id.* § 899-aa(1)(a).

The definition of "Nonpublic Information" encompasses two basic types of information: (i) "[a]ny business related information . . . the tampering with which, or unauthorized access, disclosure or use of which, would cause a material adverse impact to the business, operations or security" of a Covered Entity and (ii) three categories of nonpublic information about individuals, including "any information that is linked or linkable to an individual." § 500.01(g). Replacing the definition of the three categories of nonpublic information with a definition in alignment with the definition of "private information" in New York's data breach notification law would thus represent an important step in addressing many of our concerns. Because many firms already have data mapping to the definition in New York's data breach notification law, revising the definition of "Nonpublic Information" in this way would allow for alignment in compliance processes and thus avoid the opportunity cost of diverting resources away from more effective cybersecurity activities. We therefore recommend replacing subsection 500.01(g)(2)-(4) with the following definition in general alignment with New York's data breach notification law:

> (2) Any information that can reasonably be used to misappropriate an individual's identity or access an individual's financial account without authorization, including, at a minimum, (i) social security numbers, (ii) driver's license numbers or non-driver identification card numbers or (iii) account numbers, credit or debit card numbers in combination with any security codes, access codes or passwords that would permit access to an individual's financial account.

III. Encryption of Nonpublic Information

Section 500.15 would require Covered Entities to broadly encrypt "all Nonpublic Information," including, by definition, "any information that is linked or linkable to an individual," both in transit and at rest. We urge that any encryption requirement be made subject in its entirety to the express risk-based approach described in Section I above.

While encryption is appropriate—and employed—in many circumstances, we think it important to recognize that other compensating controls may be at least as, if not more, effective in certain circumstances.[10] Although we support the practice of safeguarding sensitive data transmitted *externally*, whether through encryption or through combinations of other superseding or compensating controls, universally encrypting all *internally* transmitted or stored Nonpublic Information as defined in the Proposal, even if feasible, would impose an enormous burden on Covered Entities without proportional benefits to them or consumers. Such prescriptive and non-risk based requirements would produce unworkable infrastructure costs, especially for small and mid-size firms, unrealistic regulatory compliance validation standards, and would 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

[10] 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.

Covered Entities to monitor internal flows for anomalies, and the data would have to be decrypted to be used in any event. Furthermore, a requirement to encrypt data held internally is simply unworkable for many legacy systems, such as mainframe technologies, storage systems based on tapes and backup disks, and in some cases could present significant scalability and performance concerns. Thus, if it could be accomplished at all, the cost of blanket encryption of all internally held or transmitted information would cost our member institutions billions of dollars.

We thus recommend that any encryption requirement exclude internally held or handled data. But again, any encryption requirement of whatever scope, should be made subject to the risk-based approach described in Section I.

IV. Notification Obligations

500.17(a) would seem to impose on Covered Entities an obligation to report to the NYDFS, within 72 hours, *every* attempt, including *unsuccessful* ones, to gain access to any information "linkable to an individual." Even for small institutions, such attempts may number in the tens of thousands per month. Would every firewall packet drop—every automatically blocked attempt to breach a firewall—be included? For larger institutions, those attempts may number in the hundreds of thousands *per day*. It is difficult for us to see what the purpose for the NYDFS' collecting such vast amounts of information would be or how collecting the information would help Covered Entities reduce their cybersecurity risk. As the Proposal appears to recognize, Covered Entities are already subject to several notice obligations with regard to cybersecurity events, both under federal and state law.[11] Moreover, Covered Entities already share information on cyber threats both within the industry and with many government partners, including the Department of Homeland Security, through the longstanding and well-developed information-sharing platform provided by the Financial Services Information Sharing and Analysis Center (FS-ISAC).[12]

We strongly urge the NYDFS to consider whether the proposed additional notice obligation would serve a useful purpose in view of other reporting platforms and associated costs of a new obligation in this regard. We believe a reasoned analysis of these issues is warranted before the NYDFS would adopt the proposed reporting requirements.

The need for a rigorous analysis of costs and benefits is all the more necessary because by amassing a vast collection of information on efforts to gain unauthorized access to Covered Entities' information systems, the NYDFS would be creating a trove of sensitive information that itself might become an appealing target for malicious cyber actors. The risk of unauthorized access to or disclosure of this information from the NYDFS' own systems constitutes another risk that should be considered in assessing the relative costs and benefits of the proposed

---

[11] *See, e.g.*, 12 C.F.R. part 30, app. B, supp. A, parts II and III (GLBA Interagency Guidelines); N.Y. General Business Law § 899-aa (NY data breach notification).

[12] We recommend that the NYDFS consider encouraging Covered Entities to join FS-ISAC. *Cf.* the FFIEC's recommendation that institutions overseen by its members should join FS-ISAC: https://www.ffiec.gov/press/pr110314.htm.

reporting requirement. While we are confident that the NYDFS strives to ensure the security of information on its own networks, previous incidents suggest that the risk of unauthorized access or disclosure should be seriously considered.[13]

In light of these considerations, we recommend that the NYDFS reconsider the notice obligation set out in § 500.17(a). If the NYDFS chooses to retain a notice requirement, we strongly recommend the following:

- First, the definition of "Cybersecurity Event," which is incorporated into § 500.17, should be amended to exclude *unsuccessful* attempts to "gain unauthorized access to, disrupt or misuse" information or information systems. As indicated above, such attempts for a Covered Entity may number in the hundreds of thousands per day. Moreover, it is not clear how Covered Entities could determine which unsuccessful attempts would be material.

- Second, we would urge the NYDFS to limit the reporting trigger in § 500.17(a) to any Cybersecurity Event (defined as modified above) "that has a reasonable likelihood of materially affecting the normal operation of the [c]overed [e]ntity, or any event with respect to which the state attorney general, the department of state and the division of state police must be notified pursuant to New York General Business Law 899-aa(8)(a)." We urge the NYDFS to omit the phrase "or that affects Nonpublic Information," which largely duplicates the reporting obligation already imposed under New York's data breach notification law. Relatedly, we would recommend omitting subsections (a)(1) and (a)(2). They are adequately subsumed within the recommended reporting trigger standard set out above, which aligns more closely to already existing standards under New York law.

- Third, we recommend removing the 72-hour deadline, which may often compel Covered Entities to report to the NYDFS before they have had a reasonable opportunity to assess the significance of the triggering Cybersecurity Event. Again,

---

[13] *See, e.g.*, OCC Notifies Congress of Incident Involving Unauthorized Removal of Information (Oct. 28, 2016), available at https://www.occ.gov/news-issuances/news-releases/2016/nr-occ-2016-138.html; GAO, Federal Information Security: Actions Needed to Address Challenges, Testimony Before the President's Commission on Enhancing National Cybersecurity (Sept. 19, 2016), available at http://www.gao.gov/assets/680/679877.pdf; Committee on Oversight and Government Reform, U.S. House of Representatives, 114th Congress, Majority Staff Report, The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation, available at https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf; FDIC, Office of Inspector General, The FDIC's Process for Identifying and Reporting Major Information Security Events (July 2016), available at https://www.fdicig.gov/reports16/16-004AUD.pdf ; GAO, Opportunities Exist for SEC to Improve Its Controls over Financial Systems and Data (Apr. 26, 2016), available at http://www.gao.gov/products/GAO-16-493?utm_medium=email&utm_source=govdelivery; GAO, Cybersecurity: Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies available at http://www.gao.gov/products/GAO-15-725T ; GAO, Information Security: FDIC Implemented Many Controls over Financial Systems, but Opportunities for Improvement Remain (Apr. 2015), available at http://www.gao.gov/products/GAO-15-426; U.S. Securities and Exchange Commission, Office of Inspector General, Federal Information Security Management Act: Fiscal Year 2014 Evaluation (Feb. 2015), available at https://www.sec.gov/oig/reportspubs/oig-information-security-fy-2014-evaluation-report-529.pdf.

New York's own data breach notification law provides a helpful model. Like many other state data breach notification laws, it requires notification "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement." N.Y. General Business Law § 899aa(2). If the NYDFS maintains a fixed deadline for reporting, we urge that the clock begin to run not from the event, but from the Covered Entity's confirmation of the nature of the Cybersecurity Event. Determining the nature of cybersecurity incidents through various analytic and forensic methods is often a complex process that may require considerable time to complete. Many other regulators have established more flexible standards and have found those to be workable in practice.[14] Other requirements in the Proposal, in addition to the NYDFS' examination process, should provide the NYDFS with assurance concerning a Covered Entity's reporting processes.

- Fourth, and again drawing on New York's data breach notification law, we recommend adding a qualifier on the reporting obligation to avoid impeding law enforcement investigations: "The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation." *Id*. § 899aa(4).

We have similar concerns regarding Subsection (b)(2) of Section 500.17 which would require Covered Entities to report to the NYDFS within 72 hours of identification "any material risk of imminent harm relating to its cybersecurity program." The scope of this reporting obligation, which we believe would be unprecedented, is unclear. Moreover, to the extent that this provision is geared to more general intelligence-gathering efforts, we believe the long-established FS-ISAC reporting frameworks, which operate on a national scale, provide an effective platform for these efforts. Accordingly, we recommend that it also be reconsidered.

V. Multi-factor Authentication

Section 500.12 would mandate that Covered Entities require multi-factor authentication in a number of specific situations. While multi-factor authentication is often a useful form of access control, other access controls may be just as or more effective in reducing cybersecurity risk. Thus, we recommend that the Proposal be amended to provide that either multi-factor authentication or other at least equally effective access controls be put in place in the specified circumstances. This flexibility will allow firms to take advantage of technological developments that provide equally appropriate and effective forms of authentication, and help avoid some of

---

[14] *See, e.g.*, N.Y. General Business Law, 899-aa(2): "The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement."; Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. part 364, App. B, Supp. A (FDIC) ("Notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information"; "sensitive customer information" means "a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account;" or "any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name or password or password and account number").

the user experience problems that have hindered adoption of multi-factor authentication. For example, SMS-based two-factor authentication was favored and remains in widespread use. More recently, NIST has cautioned against reliance on this method.[15] As a number of studies have reported, experience with multi-factor authentication has shown that malicious actors have been able to develop strategies to exploit the question/answer component of many multi-factor authentication systems, while users have been hesitant to use multi-factor authentication effectively.[16] A requirement to use multi-factor authentication as defined in the Proposal could actually, over time, have the effect of freezing in place practices that have become outdated and therefore an easier target for compromise.

VI. Audit Trail

Section 500.06 would impose a sweeping obligation to maintain several kinds of logging information for six years. While many aspects of the audit trail requirement are reasonable, the scope of its requirements greatly exceeds prudent practices followed by very large financial institutions and would result in Covered Entities storing vast amounts of data, much of which would likely have marginal usefulness for cybersecurity risk reduction. Indeed, for some legacy and specialized systems, amassing this data may be impossible without expensive overhauls. In light of these considerations, we would recommend revising the audit trail requirement to limit it to audit trail systems concerning access to Nonpublic Information and require retention only for a period of time reasonably necessary to investigate anomalies. This period may reasonably vary based on the type of information at issue, which illustrates the need to tie this requirement to an overall risk-based approach.

VII. Data Destruction

Section 500.13 would require Covered Entities to adopt procedures "for the timely destruction of any Nonpublic information (i.e., including "any information that is linked or linkable to an individual") that is "no longer necessary for the provision of the products or services for which such information was provided." As proposed, we believe this requirement would, in many cases, be simply infeasible because of the commingling of the data required to be destroyed with other kinds of data that Covered Entities may need to retain. In addition, the meaning of the phrase "necessary for the provision of the products or services for which such information was provided" is unclear. Firms may need to retain information for regulatory or other legitimate purposes which extend beyond those for which the information was originally provided. We therefore recommend revising this provision to acknowledge that retention should be permitted pursuant to the records retention policy of the business, particularly where targeted disposal is not reasonably feasible due to the manner in which this information is maintained within individual systems, including legacy systems and those where data is commingled.

---

[15] *See* NIST, Draft Special Publication 800-63B, Digital Authentication Guidelines (2016), available at https://pages.nist.gov/800-63-3/sp800-63b.html.

[16] *See, e.g.*, Francois Amigorena, It's Time to find an Alternative to Multi-factor Authentication, SC Media (Sept. 20, 2016), available at https://www.scmagazine.com/its-time-to-find-an-alternative-to-multi-factor-authentication/article/529663/.

VIII. Third-Party Information Security Policy

Section 500.11 would require Covered Entities to 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. The required policies and procedures must include "establishing preferred provisions to be included in contracts with third party service providers" addressing a list of six topics. We believe many of the specified "preferred provisions" are already subjects of negotiation between Covered Entities and many third parties. But many Covered Entities simply lack the practical ability to impose all of these practices on third parties. In addition, the cyber-related risks and nature of relationships with third parties vary greatly. Section 500.11 appears to recognize that such preferred provisions may not be appropriate in every case by use of the qualifying phrase "to the extent applicable." For the sake of clarification, we recommend that the Proposal be revised to make clear that "to the extent applicable" means that the provision will be applied taking appropriate account of the nature of the relationship and in a manner consistent with a risk-based approach described in Section I above.

The proposed requirement for annual third party assessments illustrates a similar concern. Given the hundreds, if not thousands of vendors that a Covered Entity may have, a risk-based approach would best ensure that resources are focused on service providers that pose the greatest risk. For example, it is not feasible in many instances to conduct a periodic, annual assessment of all third parties, as would appear to be required by Section 500.11(a)(4). We accordingly respectfully request that any final cybersecurity regulations limit such assessments to critical third parties, where criticality is determined under a risk-based approach.

IX. Certification

Section 500.17(b) would require the board of directors or a senior official of Covered Entities to certify annually to the NYDFS their compliance with the Proposal. While we appreciate the NYDFS' objective to emphasize accountability and the importance of compliance through the certification, we believe the certification as proposed in the form set out in Appendix A to the Proposal is unnecessary to ensure the NYDFS that a Covered Entity's compliance-related systems (i) are appropriate and (ii) will remain an institutional priority. If the NYDFS maintains a certification requirement without adopting a risk-based approach, the certification requirement would likely cause Covered Entities to expend resources ensuring that controls are applied across-the-board regardless of risk and documenting these compliance efforts, possibly diverting resources away from addressing companies' real vulnerabilities as they change over time. Thus, if a certification requirement is maintained, we urge that it be brought in line with other similar certification requirements that require confirmation that processes reasonably designed to achieve compliance are in place (i.e., rather than strict compliance with the entire universe of substantive and in certain cases subjective requirements of the Proposal).[17]

---

[17] *Cf*. the "Volcker Rule" certification: "Based on a review by the CEO of the banking entity, the CEO of the banking entity must, annually, attest in writing to [Agency] that the banking entity has in place processes to establish, maintain, enforce, review, test and modify the compliance program established under this Appendix

On its face, the certification in the Proposal uses language similar to that in Part 504. In practice, however, the risk-based approach adopted as part of the transaction monitoring regulations creates an important difference.[18] Indeed, many of our concerns regarding the certification would be addressed if the Proposal is revised to adopt a technology agnostic and risk-based approach. For example, under the current formulation of the certification, there could be cases where a board or senior official could no longer execute the proposed certification if the Covered Entity adopts an improved risk control as technology continues to evolve. Moreover, the current formulation of the certification, along with the potential for legal liability associated with execution thereof, may lead to more of a compliance-oriented approach rather than appropriate focus of resources on a more appropriately calibrated risk-based risk management approach (e.g., carefully considering the appropriate controls on a risk-based manner in view of firm cyber-risk tolerances).

We are also concerned about the additional components of the certifications required in subsections (b)(1) and (b)(2) of Section 500.17. Subsection (b)(1) would appear to require Covered Entities to identify areas requiring improvement in their cybersecurity practices and associated remediation efforts even as the board or a senior officer of the Covered Entity is being required to certify to the NYDFS that those practices meet the Proposal's requirements. In order to address the inherent tension between the requirement to execute an annual certification, on the one hand, and the requirements of 500.17(b)(1)-(2), on the other hand, the final regulation should at a minimum clarify that a qualified certification is a possibility (e.g., to provide an opportunity to indicate that during the course of a year an institution identified areas requiring improvement and either completed or is pursuing remediation efforts).

X. Definition of "Covered Entity"

The Proposal applies to "Covered Entit[ies]," defined as any individual or entity "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." § 500.01(c). Several of our member institutions have affiliated entities that share IT resources but are subject to supervision by different regulators. For example, they may have a national bank supervised by the OCC and an insurance business subject to NYDFS licensing, both of which rely on common IT systems. For firms in this position, the prospect of divergence between U.S. federal requirements and the requirements established by the NYDFS presents particular challenges and likely very substantial costs. They may need either to ensure that their shared IT systems would comply with two distinct sets of standards or to separate their affiliates' systems, along with the resources needed to ensure compliance with the different standards applicable to each. These challenges and costs could be compounded if other states follow the NYDFS' lead in establishing their own cybersecurity regulatory regimes.

---

and Section 20 of this part in a manner reasonably designed to achieve compliance with section 13 of the BHC Act and this part." 12 C.F.R. part 248, app. B.

[18] *See* NYDFS Regs. § 504.4.

We understand and assume that the NYDFS will implement the Proposal in a manner to avoid conflicts with other applicable laws and guidelines to which Covered Entities—and/or their parent companies, affiliates and subsidiaries, with which Covered Entities frequently share common IT systems and processes—are subject. This approach would help enable Covered Entities to devote their resources to risk mitigation activities rather than unnecessary duplication of effort. In this regard, both current and proposed U.S. federal and other regulatory requirements should be taken into account.[19]

* * * *

The Clearing House appreciates the opportunity to comment on the 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.

[19] *See, e.g.*, 12 C.F.R. Part 7, Subpart D (OCC preemption and visitorial powers rules); Office of the Comptroller of the Currency, 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 soliciting public comment 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 intrastructures, and third-party service providers to these).

We would also recommend that the definition of "Covered Entity" be clarified to ensure that the final regulations would apply only to the New York-licensed branches of foreign banking organizations, not the foreign banking organization as a whole.