INSTITUTE OF INTERNATIONAL BANKERS

299 Park Avenue, 17th Floor
New York, N.Y. 10171
Direct: (646) 213-1149
Facsimile: (212) 421-1119
Main: (212) 421-1611
www.iib.org

RICHARD W. COFFMAN
General Counsel
E-mail: rcoffman@iib.org

Submitted electronically

January 27, 2017

Ms. Cassandra Lentchner
New York State Department of Financial Services
One State Street
New York, NY 10004
CyberRegComments@dfs.ny.gov

Re: Proposed Addition of Part 500 to Title 23 NYCRR
"Cybersecurity Requirements for Financial Services Companies"
(I.D. No. DFS-39-16-00008-P)

Dear Ms. Lentchner,

The Institute of International Bankers ("IIB") appreciates the opportunity to comment on the updated version of the above-referenced proposed rulemaking published by the Department of Financial Services (the "Department") in the New York State Register on December 28, 2016.[1] A substantial majority of IIB member banks conduct a banking business in New York through New York branches,[2] which account for a very substantial portion of the entities regulated by the Department under the Banking Law. These operations are principally wholesale in nature, and we estimate that in the aggregate they had total assets of more than $1.8 trillion as of June 30, 2016. The Updated Proposal accordingly is of keen concern to the IIB and its members.

The IIB commented on the original proposal published in the State Register on September 28, 2016 (the "Original Proposal"), and we appreciate the Department's efforts to reflect those comments in the Updated Proposal. Our comments in this letter focus on our persisting concerns regarding the intended scope of the Part 500 requirements and standards as

[1] New York State Register, December 28, 2016, pp. 23 - 26. Our comments are based on the text of the updated proposed Part 500 (the "Updated Proposal") published on the Department's web site (available at: http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf). Capitalized terms used in this letter have the meanings ascribed in the Updated Proposal except where otherwise provided or required by the context.

[2] As used in this letter the term "New York branches" refers to New York-licensed branches and agencies of FBOs, collectively.

applied to banking organizations headquartered outside the United States ("foreign banking organizations" or "FBOs") having New York branches. These concerns focus on the following two questions:[3]

1. **In the context of foreign banking organizations, which entity is the "Covered Entity" to which the requirements and standards of Part 500, including the annual certification, apply?**

   As discussed below, we respectfully request that the definition of Covered Entity be revised to clarify that the "Covered Entity" is only the New York branch in the context of FBOs, which we believe is what is intended, and we propose for the Department's consideration suggested language that we believe more precisely expresses this purpose.

2. **What are the Department's intended limits to the extraterritorial application of Part 500?**

   As discussed below, clarification of this key implementation question is essential to enable FBOs to understand, assess and successfully discharge their compliance obligations under the regulation, especially taking into account the different degrees to which New York branches are interconnected with the cybersecurity programs of their FBO head office or other offices outside the United States.

   This consideration focuses especially on the application of the provisions of Section 500.02(c), which have been included in the Updated Proposal in response to concerns raised during the Original Proposal's comment period by the IIB and others regarding the extent to which a Covered Entity may rely on the cybersecurity program of an Affiliate to comply with Part 500 requirements and standards. The inclusion of these provisions in Part 500 is very helpful, but there remain uncertainties regarding how the prescribed requirements are intended to apply to New York branches.

Clarity on both questions is crucial to delineating the application of Part 500 to FBOs but, between the two, the extraterritorial application question raises especially complex compliance challenges. The discussion below seeks a resolution of the extraterritorial application question in a manner that appropriately adapts application of the Part 500 requirements and standards to the circumstances of New York branches as offices of much larger and internationally active foreign banking organizations. Our suggested solutions take an approach that seeks to facilitate the implementation of Section 500.02(c) in a manner that is fully consistent with the purposes of Part

[3] Our focus on the two questions addressed in this letter underscores the centrality of these concerns to our members. Regarding other aspects of the Updated Proposal, we agree with the concerns raised in the letters submitted separately by The Clearing House Association L.L.C. and the Securities Industry and Financial Markets Association (joined by others) (collectively, the "TCH and SIFMA Letters").

500 and enables appropriate flexibility in attaining feasible, pragmatic and effective methods of compliance.

THE DEFINITION OF "COVERED ENTITY"

We recognize and appreciate the Department's inclusion of references to "branch" and "agency" in the definition of "Person" in the Updated Proposal. The addition of these terms to the definition helpfully responds to the request in our letter on the Original Proposal to clarify that the "Covered Entity" is only the New York branch in the context of FBOs. However, we believe there remains an unintended ambiguity in the Covered Entity definition in that an FBO, rather than its New York branch, is the entity (Person) which under the Banking Law is required to obtain a license to operate through a branch and therefore could be viewed as the Covered Entity – that is, under this construction of the language, the FBO itself would be understood to be the "Person operating under or required to operate under a license" and thus the Covered Entity.

If the FBO were a Covered Entity, then the FBO itself would be required to satisfy all the requirements of the regulation, including the annual certification. Our overriding concern regarding this prospect is that the entirety of the Part 500 requirements would apply to the FBO such that the FBO would be required on a global basis to conform its cybersecurity programs, policies, systems and practices to the requirements of the regulation, and its certification would apply to all of those global aspects. In addition, the FBO would be required to notify the Superintendent of any in-scope "Cybersecurity Event" occurring anywhere throughout its global operations.[4]

Such broad, extraterritorial application of the Part 500 requirements would be unprecedented and a stark rupture with the longstanding and well-established regulatory and supervisory regime applicable to FBOs and their New York branches, and it would risk substantial, unnecessary and potentially counterproductive conflicts with other country's requirements. Moreover, it would very significantly diminish the value and attractiveness of maintaining a New York branch license, and we anticipate it would be strongly weighed against pursuing entry into the New York market through a New York branch. We do not believe any of these severely adverse consequences are intended, and respectfully urge the Department to revise the definition of Covered Entity to eliminate any ambiguity regarding its scope as applied to foreign banking organizations.

We respectfully offer for the Department's consideration the following suggestion, which builds on the definition of "Regulated Institutions" under the recently-effective Part 504

[4] Regarding the notification requirements of Section 500.17(a), we note that, even if the Covered Entity under Part 500 is only the New York branch (and not the FBO), the intended scope of the requirements of subparagraph (1) are unclear. We accordingly respectfully request clarification that notice to the Superintendent pursuant to subparagraph (1) is required only with respect to notices that are required to be provide to any U.S. government body, self-regulatory agency or other supervisory body.

regulations[5] and supplements it by including a generic reference to the additional Persons overseen by the Department under other Articles of the Banking Law that we understand are intended to be within the scope of Part 500. This result could be achieved as follows: [6]

Add the following new definition:

> *Banking Law Regulated Entities* means (a) all banks, trust companies, private bankers, savings banks, and savings and loan associations 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, (b) all check cashers and money transmitters licensed pursuant to the Banking Law and (c) any other Person that is not a foreign banking corporation and is operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization issued by the Superintendent pursuant to any other Article of the Banking Law.

Modify the definition of Covered Entity to read in its entirety as follows:

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

LIMITING PART 500's EXTRATERRITORIAL APPLICATION: SECTION 500.02(c)

The cybersecurity program of New York branches to varying degrees operate within parameters established by the programs adopted by their FBO head offices. Indeed, in some cases, and with respect to certain aspects of its program, a New York branch may be closely interconnected with the FBO's cybersecurity program, including information systems maintained by and information technology developed and provided by the FBO outside the United States (and in some instances at multiple locations), and the New York branch's cybersecurity efforts may be supported to varying extents by personnel of the FBO working outside the United States.

There is considerable variety among New York branches in this regard depending on, among other things, the relative scale of the branch's business compared to that of the FBO in its

[5] As defined in Section 504.2, these "Regulated Institutions" are (a) all banks, trust companies, private bankers, savings banks, and savings and loan associations 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 and money transmitters licensed pursuant to the Banking Law.

[6] Our intention is simply to clarify that the "Covered Entity" is only the New York branch in the context of FBOs and not to exclude any Person otherwise intended by the Department to be within the scope of Part 500 or include any Person not intended to be in-scope.

entirety, including the number of employees and the types of products offered, and the structure and complexity of the FBO's combined U.S. operations. The integrated, interconnected and cross-border aspects of New York branch cybersecurity programs and policies strengthen the cybersecurity defenses of New York branches, and it is essential that any final cybersecurity regulations appropriately accommodate the diversity of approaches New York branches and their FBO head offices take in designing and implementing their cybersecurity programs.

We recognize and appreciate the Department's inclusion of the new provisions of Section 500.02(c) in the Updated Proposal, and we have considered extensively the efficacy of these provisions in addressing our concerns regarding the potential extraterritorial overreach of the Part 500 requirements and standards.[7] As discussed below, we continue to have serious concerns regarding how these provisions are intended to apply in practice in the context of New York branches vis-à-vis their FBO Affiliates, and we respectfully request that the final rule more precisely demarcate the intended extraterritorial applicability of Part 500.

The key challenge in this context is prescribing, by means of a regulation, requirements and standards that incorporate sufficient flexibility to accommodate the wide variety of interconnections between New York branches and their FBO Affiliates while giving sufficient assurance that the purposes of Part 500 will be achieved. Analyzed from the perspective of a New York branch and its FBO Affiliate, the requirements of Section 500.02 raise two overriding concerns.

- First, would a New York branch, with the goal of enhancing its cybersecurity program, be permitted to adopt a portion of its FBO Affiliate's program to satisfy certain compliance obligations under Part 500, such as a firewall, intrusion detection application or user authentication module (to mention several illustrative examples), or does the regulation contemplate that a New York branch must adopt an "all or nothing" approach?

  For example, a New York branch may have some capacity to develop its own applications while also utilizing applications developed by its FBO Affiliate. In addition, the type of training and monitoring required under Part 500 may involve Authorized Users of either the New York branch and/or its FBO Affiliate, and incident response planning may be relevant to Cybersecurity Events that could affect the New York branch directly or indirectly through Information Systems at the FBO Affiliate (or at other offices of the FBO Affiliate outside the United States) that support the New York branch. We do not believe it is intended that in any of these types of situations a New York branch would be precluded from looking to the FBO Affiliate for support because such support would not cover the entirety of that part of

[7] The starting point of our analysis is the conclusion that an FBO head office should be treated for purposes of Part 500 as an Affiliate of its New York branch consistent with the "control" standard contained in the Updated Proposal's "Affiliate" definition.

the New York branch's cybersecurity program. At the same time, we believe that the provisions of Section 500.02(c) are intended to apply only insofar as a New York branch in fact looks to its FBO Affiliate for support.

The structure of the regulation and the Department's evident and welcome intention to facilitate reliance on Affiliates' cybersecurity programs indicate adoption of a portion of an FBO Affiliate's program is permissible, but this is not clear from the Updated Proposal's language. Where a requirement is embedded in a regulation, noncompliance with which constitutes a violation of New York law, it is essential to minimize ambiguity to maximize compliance. With this purpose in mind, we respectfully suggest for the Department's consideration the following revisions to Section 500.02(c) (suggested additional language is underscored):

> 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 this Part in question.

- Second, determining compliance with the proviso – *i.e.*, that the FBO Affiliate's cybersecurity program must meet the requirements of Part 500 to be eligible for adoption by the New York branch – raises very significant interpretive and practical implementation difficulties.

  It is unclear exactly what this requirement entails, especially in circumstances where the design of a New York branch's cybersecurity program is significantly dependent on its FBO Affiliate's cybersecurity program. By way of illustration, consider the situation of a New York branch with between 50 and 100 employees, and whose FBO head office has several thousand employees, in which the Nonpublic Information (or a portion thereof) of the New York branch is stored in an Information System maintained and operated by its FBO head office. That head office Information System also stores information of non-U.S. customers that have no connection to the operations of the New York branch, and it is not technically feasible to isolate or segregate the New York branch Nonpublic Information on the system. This may be the case, for example, where the back-office support for a New York branch's foreign exchange and capital markets-related activities resides at the FBO Affiliate on systems that also serve the FBO's non-U.S. offices. Especially where the New York branch is transacting with non-U.S. customers of the FBO Affiliate, the existence of shared files relating to the customer (including, for example, credit and other risk-related information that encompasses Nonpublic Information), presents considerable compliance challenges.

  In a typical situation, personnel of the New York branch would have access only to Nonpublic Information relating to customers with which the New York branch transacts, but

select head office staff may have access to such information as well (such as system administrators or select individuals in globally-integrated business units who collaborate with or provide support to the New York branch). In our illustrative example of a New York branch with between 50 and 100 employees whose head office has several thousand employees it is unclear from the Updated Proposal, among other things, whether the Multi-Factor Authentication requirement would be limited to only those New York branch employees having access to the information or whether the FBO would have to heavily invest in making all relevant systems conform with Multi-Factor Authentication for all employees. The former approach may be achievable with a reasonable cost-benefit effort, but the costs of the latter would be wholly out of proportion to the benefits. It would require the FBO to spend substantial amounts of money first to conform all its systems that store Nonpublic Information for customers which transact with the New York branch and then to invest in additional equipment, such as fingerprint scanners or access card readers to permit access to information technology systems that enable recognition by Multi-Factor Authentication.

Thus, there is a serious and very practical concern that in this scenario, which is not uncommon, the FBO would be required to conform the entirety of these systems and related operations to the requirements of Part 500, thereby risking all the severely adverse consequences discussed on page 3 which underlie our concerns regarding the definition of Covered Entity.

To take another example, it is unclear how far-reaching into the systems and practices of an FBO Affiliate the audit trail requirements of Section 500.06(a)(1) would be required to run in order to reconstruct material financial transactions of a New York branch processed through shared Information Systems operated by the FBO Affiliate and whether, or to what degree, the requirements of Section 500.06(a)(2) would have to extend to Cybersecurity Events that may affect an Information System containing New York branch Nonpublic Information whether or not such information would in fact be put at risk as a result of the Cybersecurity Event. Regarding encryption, because the requirements of Section 500.15 are not limited to encryption of Nonpublic Information of the Covered Entity (here, the New York branch), there is a very real concern that an FBO Affiliate would be required to apply these requirements throughout its Information Systems.

The potential reach of the recordkeeping requirements of Section 500.06(b) also is unclear. More generally, clarity is needed regarding the reach of the data retention requirements of Section 500.13 (for example, in the case of shared customer files). Similarly, where Penetration Testing of shared Information Systems is performed by an FBO Affiliate, there is concern that those requirements would be extended to such Information Systems in their entirety.

Especially where the New York branch accounts for a very small portion of the FBO's global operations (in foreign exchange or capital markets, for example),[8] this "exportation" of Part 500 requirements to the FBO head office would present very significant cost-benefit disadvantages regarding the value and utility of the New York branch license and a very high barrier to FBO entry into New York in reliance on a Banking Law-based license. Put colloquially, at some point this calculus would support the determination to no longer permit the New York branch "tail" to wag the FBO "dog."

Our members are strongly committed to compliance with all applicable regulatory requirements, and there is an accordingly keen desire for appropriate resolution of these very real and complex concerns. Our purpose in raising them is to facilitate the implementation of Section 500.02(c) in a manner that is consistent with the purposes of Part 500 and provides a New York branch appropriate flexibility in determining how the regulatory requirements should be met in practice.

We offer for the Department's consideration the following approaches to a solution, none of which are mutually exclusive.

- Provide further clarification regarding the intended relationship between a New York branch's Risk Assessment and its reliance, to whatever extent, on Section 500.02(c).

  For example, the first sentence of Section 500.09(a) would be modified to provide as follows (additional suggested language is underscored):[9]

  > 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, including whether and the extent to which the Covered Entity would adopt a cybersecurity program maintained by an Affiliate pursuant to Section 500.02(c).

  This aspect of a New York branch's Risk Assessment would require it to articulate, analyze and document its cybersecurity dependency upon each element of an FBO Affiliate's cybersecurity program and explain the measures taken to attain and maintain compliance with the Part 500 requirements that apply thereto, including those designed to protect the New York branch's Nonpublic Information. For example, we believe this Risk Assessment would be especially helpful in framing the parameters of determining

[8] By way of illustration, we estimate that for a significant number of New York branches, the operations of the New York branch, measured in terms of assets, account for well under 5% of the FBO's total consolidated assets.

[9] The suggested revision to Section 500.09(a) is limited to clarifying the operation of Section 500.02(c). In addition to this revision, we agree with the suggested other revisions to Section 500.09 discussed in the TCH and SIFMA Letters.

user access privileges under Section 500.07 and applying the encryption provisions of Section 500.15.[10]

We would anticipate as well that any such dependencies, and the measures required to maintain compliance with applicable provisions of Part 500, would be appropriately memorialized in documentation detailing the New York branch's cybersecurity program, a process which may entail review and updating of service level agreements between the branch and the FBO Affiliate.

These actions by the New York branch would provide an effective framework for assessing whether the arrangements in place between it and the elements of the FBO Affiliate's cybersecurity program which it may adopt "meet the requirements of [Part 500]" as provided under Section 500.02(c).

- Provide what in effect would be a written statement of policy regarding the Department's intentions and expectations regarding the extraterritorial limits on the applicability of Part 500 to New York branches' dependencies on information technology and other cybersecurity resources maintained and operated by the FBO outside the United States.

  At a minimum, it would be very helpful for the Department to confirm both that Part 500 (i) is not intended to cause its requirements to be "exported" in a wholesale manner such that they must be universally applied to an FBO's global cybersecurity program and mandate changes to its design and contours, and (ii) is intended to provide New York branches appropriate flexibility to adapt those requirements to the circumstances of their cybersecurity programs. Clarifying the extraterritorial applicability of Part 500 in this manner would not exempt the FBO's global cybersecurity program from adequately safeguarding the FBO's systems and data; rather, it would leverage existing and significant safeguards already implemented by FBOs based on leading industry frameworks (such as ISO 27001 and the NIST Cybersecurity Framework) to secure their centralized, globally-shared operations. Lingering uncertainty on this fundamentally important question serves no helpful purpose and would result in needless vexation regarding compliance with Part 500.

  We respectfully submit that written memorialization of the Department's intentions and expectations is critical to effective implementation of the Part 500 requirements by New York branches. Such memorialization might take a variety of forms – for example,

[10] With respect to encryption, we share the concerns expressed in the TCH and SIFMA Letters and note further that the challenges raised in having to delineate between external networks and data at rest and determine the feasibility of encryption in both situations are only compounded in the context of a New York branch and its FBO Affiliate, where the Nonpublic Information of the New York branch may be stored in shared Information Systems at the FBO Affiliate.

through issuance of guidance under Part 500, the inclusion of an explanation in the State Register notice of the final rule, or inclusion in Part 500 itself.

- An additional transitional period should be provided for compliance with Section 500.02(c). FBOs face uniquely complex challenges in designing cybersecurity programs that fully accommodate Part 500 in all its particulars. Those challenges include, without limitation:

  - identifying any cross-border information technology dependencies that are material to the design of their New York branches' cybersecurity programs;

  - achieving a common recognition and understanding with remote internal constituencies of those dependencies, the challenges they present and agreement on how to address them to achieve Part 500 compliance where necessary;

  - reconciling the potentially conflicting mandates and regulatory expectations a global enterprise commonly encounters which emanate from concurrently applicable home and host country legal authorities;

  - obtaining required internal approvals, allocating budgetary and other resources and implementing any information technology upgrades and changes to Information Systems necessary to comply with applicable requirements;

  - establishing, testing and validating the controls and other processes necessary to support the New York branch's certification to the Superintendent, taking into account the interconnectedness of its program with that of the FBO Affiliate; and

  - the inherent cost and complexity in all matters pertaining to information technology and cybersecurity.

  Given these considerations, we respectfully suggest that the work that lies ahead under Part 500 for the typical FBO having a New York branch whose cybersecurity program is in part or in whole dependent on elements of the FBO's cybersecurity program is not materially different than that of a Covered Entity that must establish Part 500-compliant relationships with one or more Third Party Service Providers.

  We accordingly believe it would be appropriate to extend the same transitional period applicable to Third Party Service Providers to the provisions of Section 500.02(c), and we respectfully suggest for the Department's consideration the following revision to Section 500.22(b)(3) (additional suggested language is underscored):

  > (3) Two years from the effective date of this Part to comply with the requirements of section 500.02(c) and section 500.11 of this Part.

This approach would maintain the distinction under Part 500 between a Third Party Service Provider and an Affiliate, but it would recognize and give appropriate effect to the similarities, as a practical matter, between a New York branch's reliance on a Third Party Service Provider and, to the extent applicable under Section 500.02(c), its FBO Affiliate for purposes of meeting the Part 500 requirements. The additional time provided to New York branches would enhance the robustness of their compliance with the requirements, which in turn would facilitate the examination process and promote efficient allocation of supervisory resources.

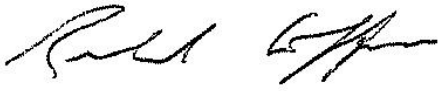
Consistent with the suggested clarification that a New York branch may adopt a portion of its FBO Affiliate's cybersecurity program, the suggested two-year transitional period would apply only with respect to those parts of its FBO Affiliate's program a New York branch adopts.

* * *

The IIB and its members share the Department's commitment to strengthening the financial sector's cybersecurity. Consistent with this shared purpose, our comments are intended to reinforce the foundation of the Department's proposed cybersecurity regime and enhance the robustness and effectiveness of Covered Entities' cybersecurity programs. We look forward to continuing to work constructively with the Department on these matters and would welcome the opportunity to discuss further our comments and suggestions.

We appreciate your consideration of our comments and recommendations and would welcome the opportunity to discuss them further with you and your colleagues. In the meantime, please contact the undersigned or Paul Begey (pbegey@iib.org; 646-213-1146) at the IIB if you have any questions.

Sincerely,



Richard Coffman
General Counsel