INSTITUTE OF INTERNATIONAL BANKERS

Stephanie Webster
General Counsel
E-mail: swebster@iib.org

299 Park Avenue, 17th Floor
New York, N.Y. 10171
Direct: (646) 213-1147
Facsimile: (212) 421-1119
Main: (212) 421-1611
www.iib.org

January 9, 2023

BY ELECTRONIC SUBMISSION

New York State Department of Financial Services
c/o Cybersecurity Division
One State Street, Fl. 19
New York, NY 10004

VIA Electronic Mail: cyberamendment@dfs.ny.gov

Re: ***Proposed Second Amendment to 23 NYCRR Part 500 Cybersecurity Requirements for Financial Services Companies***

Dear Sir or Madam:

The Institute of International Bankers (the "IIB") appreciates the opportunity to submit this letter to the New York State Department of Financial Services (the "DFS") on the proposed amendments to 23 NYCRR 500 (the "Proposed Rule") regarding cybersecurity requirements for financial services companies.[1] The IIB represents internationally headquartered financial institutions from over 35 countries around the world doing business in the United States. Our members consist principally of international banks that operate branches and agencies, bank subsidiaries and broker-dealer subsidiaries in the United States.

The IIB supports the DFS's efforts to establish cybersecurity standards that protect consumers, ensure entities continue operating in a safe and sound manner and protect the stability of the financial system. We appreciate the changes the DFS made from the pre-proposal, including with respect to the new limitation on the scope of "Class A companies" and clarifications regarding companies with a CEO or a board of directors, penetration testing by internal personnel and the use of segmented secure backups.[2]

However, we believe that the Proposed Rule remains unnecessarily prescriptive and rigid and does not sufficiently consider the diversity of entities that will be subject to the Proposed Rule.

[1] DFS, "Proposed Second Amendment to 23 NYCRR Part 500" (Nov. 9, 2022), https://www.dfs.ny.gov/system/files/documents/2022/10/rp23a2_text_20221109_0.pdf.
[2] DFS, "Proposed Second Amendment to 23 NYCRR Part 500" (Jul. 29, 2022), https://web.archive.org/web/20220802040430/https://www.dfs.ny.gov/system/files/documents/2022/07/pre_proposed_draft_23nycrr500_amd2.pdf.

The Proposed Rule fails to consider the roles different employees of a covered entity should play and introduces proposals that would shift the role of the board of directors from oversight to management and require the chief information security officer (the "CISO") to oversee areas in which it is unfamiliar. In general, we believe the Proposed Rule should provide more flexibility for entities to design their cybersecurity programs to address their particular risks. We endeavor in this comment letter to suggest specific areas where more flexibility can be introduced into the Proposed Rule.

Executive Summary

Our recommendations are as follows:

I. The in-state gross annual revenue threshold for "Class A companies" should be (A) changed to, or supplemented with, an in-state asset threshold of $50 billion or, if not, (B) increased to at least $100 million.

II. The requisite independent audit should be permitted to be performed (A) by either internal or external auditors and (B) periodically but at least every three years, at an appropriate frequency based on the company's risk assessment, not annually.

III. The scope of the business continuity and disaster recovery ("BCDR") plan should be limited so that (A) it is only required to be reasonably designed to ensure the availability and functionality of the covered entity's material services and (B) such plans are limited to responding to cybersecurity emergencies or other cybersecurity-related disruptions to its normal business activities.

IV. A covered entity should be required only to certify that it has *materially* complied with and is currently in compliance with the Proposed Rule.

V. If our recommendation in Section III.B is not accepted, the annual certification should be required to be signed only by the covered entity's highest-ranking executive, not the CISO.

VI. Penetration testing should be limited to the high-risk areas identified by the covered entity's risk assessment.

We also include a list following our formal recommendations with smaller issues or ambiguities we identified in the Proposed Rule that we suggest the DFS consider.

I. The in-state gross annual revenue threshold for "Class A companies" should be (A) changed to, or supplemented with, an in-state asset threshold of $50 billion or, if not, (B) increased to at least $100 million.

A. Shifting to an Asset Threshold

As the IIB conveyed in its letter in response to the pre-proposal, we appreciate the DFS's decision to tailor the Proposed Rule to the risk profile and resources of companies. More specifically, the IIB appreciates the inclusion of a new threshold in the Proposed Rule's

definition of Class A companies, which would exclude from the definition entities having less than $20,000,000 in gross annual revenue in each of the last two fiscal years from the New York business operations of the covered entity and its affiliates. As we noted in our previous letter, without any in-state limitation, the Proposed Rule would capture many small and medium-sized New York branches of international banks with limited activities and relatively low cybersecurity risk solely because they are a part of a large international bank.

The revenue threshold is a step in the right direction to properly scope the definition of Class A companies, but we do not think it is the right measure for banks such as our members. While we cannot speak to the suitability of a revenue threshold for other types of covered entities, we believe that total assets is a more appropriate measure of the size and risk profile of a bank.

Federal regulators generally use total assets to categorize banks or bank holding companies ("BHCs"). For example, the Board of Governors of the Federal Reserve System (the "Federal Reserve Board") imposes enhanced prudential standards based on a BHC's average total U.S. consolidated assets with categories at $100 billion, $250 billion and $700 billion.[3] In its statistical release on large commercial banks, the Federal Reserve Board lists only a bank's assets and number of branches, not revenue.[4] Finally, the U.S. Small Business Administration (the "SBA") also classifies "commercial banking" entities based on assets, while most other entities are classified by revenue or workforce.[5]

For banks, revenue, especially at the relatively low threshold set in the Proposed Rule, tends to be more volatile than assets, which tend to be more stable. As such, a revenue threshold could result in many covered entities regularly falling in and out of the "Class A company" definition. Total assets also more accurately represent risk, including cybersecurity risk, as they reflect the amount of assets the bank is responsible for and therefore, the amount that would be threatened in a potential cyber incident.

We therefore recommend that the DFS adopt an initial threshold of $50 billion in total U.S. consolidated assets within New York state, either in place of or in addition to the current revenue threshold. This would capture any large New York branches and agencies of international banks operating in New York state but avoid capturing many of the smaller and less risky entities. Further, it would align with the original Dodd–Frank Wall Street Reform and Consumer Protection Act thresholds and be familiar to banks already complying with federal regulations.[6]

B. Increasing the Revenue Threshold

If the DFS were to not adopt an asset threshold, then it should consider increasing the revenue threshold to at least $100 million. The revenue threshold is still set too low and would continue

[3] 12 CFR part 252.
[4] Federal Reserve Board, "Large Commercial Banks" Federal Reserve Statistical Release (Sep. 30, 2022), https://www.federalreserve.gov/releases/lbr/current/default.htm.
[5] 13 CFR § 121.201 (the maximum allowed for a commercial banking concern and its affiliates to be considered small is "750 million in assets").
[6] *See, e.g.,* Dodd–Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 165, 124 Stat. 1376, 1423 (2010) ("the Board of Governors shall … establish prudential standards for nonbank financial companies … with total consolidated assets equal to or greater than $50,000,000,000").

to capture many small and medium-sized New York branches of international banks with limited activities and relatively low cybersecurity risk.

The requirements for Class A companies are outsized compared to the risks presented by institutions with less than $100 million in revenue. New York branches of large international banks with less than $100 million in revenue are small (by asset size) and engage in limited activities. Imposing on them the same regulatory compliance burdens as those applicable to the largest institutions in New York state solely because such branches or subsidiaries are affiliated companies with large international operations would be inappropriate.

Because a foreign bank branch or subsidiary will not typically be competing with the larger domestic companies that would qualify as "Class A companies," imposing costly cybersecurity requirements on small branches and subsidiaries would make them unnecessarily less competitive given the incremental level of protection such procedures would have on entities that small.[7] Bigger companies will be less negatively affected by the Class A company requirements and will pose larger cybersecurity risks.[8]

A $100 million revenue threshold would also make the categorical measurements in the Proposed Rule more consistent. Currently, the Proposed Rule creates three tranches of covered entities: (i) Class A companies, (ii) standard covered entities and (iii) covered entities subject to the limited exemption. A covered entity would be a Class A company if it has at least (i) $20,000,000 in in-state revenue and (ii) either 2,000 employees or $1 billion in consolidated revenue. A covered entity is subject to the limited exemption if it has (i) fewer than 20 employees and independent contractors, (ii) less than $5,000,000 in in-state gross annual revenue and (iii) less than $15 million in year-end total assets.[9] Standard covered entities are those that are not Class A companies or covered entities subject to the limited exemption.

Comparing the different thresholds, there is a significant gap between companies with 20 and 2,000 employees, but the difference between companies with gross annual revenues of $5,000,000 versus $20,000,000 is fairly small. Moving from 20 employees to 2,000 employees is a sizable ramp up in size, so it is understandable that companies of 2,000 or more employees would be subject to more stringent cybersecurity requirements. However, moving from $5,000,000 in revenue to $20,000,000 is not nearly as sizable an increase and does not represent the same increase in risk as the shift from 20 to 2,000 employees would. $100 million would get closer to creating more targeted tranches of risk.

---

[7] While, as noted above, the SBA generally classifies commercial banks based on total assets, investment banking and securities intermediation companies, consumer lending companies, real estate credit companies and companies dealing with financial transactions processing, reserve and clearinghouse activities are classified as "small" if they have less than $41,500,000 in gross receipts. The Small Business Jobs Act of 2010 also defines a business as an "eligible small business" "if the average annual gross receipts of such [company] for the 3-taxable-year period preceding such taxable year does not exceed $50,000,000." 26 USC § 38(c)(5).

[8] It is worth noting that branches and agencies of international banks, the entities that might be excluded from the "Class A company" definition if the threshold is raised, do not appear to have had any public enforcement actions against them under the current rule versus other types of covered entities.

[9] The existence of an asset limit for the exemption also supports the use of an asset limit in the Class A company definition rather than a revenue threshold.

Therefore, if an asset threshold is not used, we would ask that the DFS increase the revenue threshold to at least $100 million.

II. The requisite independent audit should be permitted to be performed (A) by either internal or external auditors and (B) periodically but at least every three years, at an appropriate frequency based on the company's risk assessment, not annually.

A. Permitting Internal or External Auditors to Conduct Independent Audits

We recommend reverting to the pre-proposal definition of "independent audit," which permitted the audit to be performed by either internal or external auditors. The Proposed Rule would require Class A companies to conduct an annual independent audit of their cybersecurity programs. "Independent audit" is defined as "an audit conducted by external auditors free to make decisions not influenced by the covered entities being audited or by its owners, managers or employees." We believe this definition should also define "independent audit" to include an audit conducted by internal auditors.

As banks, the internal auditor of many of our members are subject to regulatory expectations and professional standards regarding their independence and expertise.[10] The DFS encourages branches of international banks to use internal auditors; requiring Class A companies to use only external auditors for their cybersecurity programs would thus seem contrary to DFS's regulatory guidance.[11] Further, as a result of the DFS's guidance, many banks have already developed the necessary expertise internally or engaged expertise externally to perform necessary audit functions.

While for some covered entities an external auditor is ideal, often, an internal auditor can prove more effective and efficient because internal personnel are less costly, have familiarity with the bank by working there day after day and can more easily interact with supervisors and regulators. This can be particularly beneficial for cybersecurity risks where knowledge of the systems the covered entity uses is at a premium. Further, requiring the use of external auditors can impose unnecessary and considerable cost, especially on smaller entities.

While the IIB appreciates that for some banks an external auditor may be necessary for safety and soundness purposes, a Class A company should have the flexibility to choose to use an external auditor based on its risk assessment. A bank should only otherwise be required to use an external auditor if there is a specific determination by the DFS.

B. Frequency of the Independent Audit

We agree that regular audits are important. However, given the significant cost of an external auditor, and the internal resources needed to support an external auditor, we recommend that the DFS amend the frequency of the independent audit. Rather than requiring an annual independent audit, we suggest that the frequency be based on the covered entity's risk assessment but with a requirement that the audit be conducted at least every three years. Requiring them annually for

[10] *See, e.g.*, 3 NYCRR § 5.4; 12 CFR § 362.2(a) (regarding general audit requirement).
[11] 3 NYCRR § 5.4(a) ("The superintendent encourages all foreign bank offices to employ qualified internal auditors as an important aspect of adequate internal control.").

all cybersecurity measures would be unnecessary for many covered entities, especially smaller Class A companies, and would not justify the cost if the company's risk assessment does not necessitate such frequency.

Furthermore, the Proposed Rule already contains a number of annual requirements that would cover similar ground to the independent audit. Under the Proposed Rule, covered entities are required to certify that they have complied with the Proposed Rule for the past year. This means a covered entity is already required to monitor its cybersecurity measures and review them for compliance annually. The Proposed Rule also requires the risk assessment be reviewed and updated annually, which would also require a comprehensive review of the company's cybersecurity program.[12] An annual audit might thus be redundant.

As such, we believe it would be more appropriate to have the frequency of the audit be determined by the company's risk assessment, which will require many to have annual audits nonetheless but not restrict those for which it is unnecessary. We would also suggest setting the audit frequency at a minimum of three years to provide flexibility but ensure that an audit is performed at least as frequently as the external risk assessment.

III. The scope of the BCDR plan should be limited so that (A) it is only required to be reasonably designed to ensure the availability and functionality of the covered entity's *material* services and (B) such plans are limited to responding to cybersecurity emergencies or other cybersecurity-related disruptions to its normal business activities.

A. Materiality

We believe the BCDR plan should be limited to covering only *material* services. As currently drafted, the Proposed Rule would require all covered entities to have their BCDR plans ensure the availability of *all* services and functionalities, including those that are immaterial. However, in times of emergency, an effective BCDR plan needs to allow the prioritization of material services and not allocate critical resources to maintaining immaterial services. For example, passenger airplanes are required to carry extra drinking water and fuel in case the flight is diverted to a more distant airport, but they do not need to ensure that the Wi-Fi works on the diverted route. In that same vein, the DFS's BCDR plan requirement should emphasize that the BCDR plan does not have to be comprehensive, but it should maintain essential services to the covered entity. By leaving this unqualified, a company may be pressured to dedicate resources to keeping immaterial services functioning to comply with these requirements, to the detriment of its other services.

[12] Other annual requirements in the Proposed Rule include (i) a review of the company's cybersecurity policy (Section 500.3); (ii) a written report from the CISO on the cybersecurity program (Section 500.4(b)); (iii) penetration testing (Section 500.5(a)(1)); (iv) a review of user access privileges (Section 500.7(a)(4)); (v) a review of the application security procedures, guidelines and standards (Section 500.8(b)); (vi) a review of approvals with respect to compensating controls (Section 500.12(c)); (vii) periodic cybersecurity awareness training (Section 500.14(a)(3)); (viii) a test of the entity's incident response plan with all staff critical to the response (Section 500.16(d)(1)); (ix) a test of the entity's BCDR plan with all staff critical to the continuity and response effort (Section 500.16(d)(2)); and (x) a test of the entity's ability to restore its systems from backups (Section 500.16(d)(3)). To the extent an annual independent audit requirement is retained, to avoid redundancy, the DFS should consider changing the frequency of some of these requirements.

B. Limiting the Scope of the BCDR Plan

We believe that the Proposed Rule's language is not precise regarding the types of emergencies the BCDR plan should cover. As the BCDR plan will be part of the cybersecurity program and therefore under the purview of the CISO, it should be limited to cybersecurity-related incidents. The CISO should not, for example, be responsible for a covered entity's pandemic response (though it may play a role in such response). Many of our members currently require different experts within the organization to respond to different types of emergencies; forcing them to shift non-cybersecurity-related responsibilities to the CISO might actually serve to undermine their current measures rather than enhance them.

Alternatively, the final rule could explicitly limit the CISO's responsibilities for the BCDR plan to cybersecurity-related matters. This would tailor the CISO's responsibilities to sections of the BCDR plan over which he/she has expertise. While we believe the entire BCDR plan should be limited in line with the focus of the Proposed Rule, this would at least avoid forcing the CISO to be responsible for parts of the BCDR plan for which he/she is not held responsible within the covered entity.

IV. A covered entity should only be required to certify that it has *materially* complied with and is currently in compliance with the Proposed Rule.

The certification in Section 500.17(b) requires a covered entity to either certify that it complied with the Proposed Rule over the previous year or acknowledge that it did not comply and identify all sections with which it has not fully complied. This could be read, particularly in light of the addition to what constitutes a violation in Section 500.20, to expand the scope of the certification from that in the current rule by requiring the covered entity to certify that it has not had any lapses of more than 24 hours with any of the provisions of the Proposed Rule throughout the prior year.

IIB appreciates the value of a certification of compliance. However, the new construct would make it difficult for any covered entity to provide the certification as even small, immaterial mistakes could qualify as noncompliance under the Proposed Rule. As such, the DFS should add a materiality qualifier to any historical aspect of the certification provision, or to the definition of a violation in Section 500.20, so as to exclude temporary gaps in compliance with the rule that are not material and have been remedied at the time of certification. Full compliance with every provision of the rule should only be required at the time of certification. We believe this achieves the goal of the certification requirement without overburdening covered entities by requiring them to monitor compliance with every provision of Part 500 throughout the year and without inundating the DFS with disclosures of immaterial temporary lapses in compliance.

V. If our recommendation in Section III.B is not accepted, the annual certification should be signed only by the covered entity's highest-ranking executive, not the CISO.

Section 500.17(b)(2) of the Proposed Rule requires that the covered entity's highest-ranking executive and its CISO sign a certification annually stating that the covered entity has complied with the requirements of the rule for the prior year. To the extent our recommendation in Section

III.B above is not accepted and the BCDR plan is required to cover more than cybersecurity-related incidents, we recommend requiring only the signature of the highest-ranking executive.

The rationale for this, as discussed above, is that the CISO typically is not responsible for all of the rule requirements. Rather, covered entities engage several departments to comply with the rule, including business continuity management, information technology and cybersecurity. The CISO is not traditionally involved in, or responsible for, some of these areas (e.g., business continuity management, information technology), so the CISO's signature on the certification will either be irrelevant or require the CISO's responsibilities to be expanded into areas beyond its current expertise. As discussed in Section III.B above, shifting to the CISO responsibilities that belong with experts in those other areas could undermine the safety and soundness of a covered entity rather than enhance it.

We note that removing the CISO from the certification requirement would not affect its reporting to the covered entities' senior management. Indeed, the Proposed Rule itself requires that the CISO report annually to the covered entity's senior governing body on the cybersecurity program in Section 500.4(b). Thus, if the signature on the certification were limited to the highest-ranking executive, that executive's certification would likely be supported by statements from the CISO and the heads of the other departments responsible for compliance with the rule. So limiting the signatory would avoid imposing an unnatural hierarchy in these departments but still require accountability through the subject matter expert's responsibilities to the covered entity.

VI. Penetration testing should be limited to high-risk areas identified by the covered entity's risk assessment.

Section 500.5(a)(1) of the Proposed Rule requires that a covered entity perform "penetration testing of their information systems from both inside and outside the information systems' boundaries by a qualified internal or external independent party at least annually." In addition to adding that testing must be performed both inside and outside the information system and that it must be performed by a qualified internal or external party, the Proposed Rule changes the current rule (and the pre-proposal) by deleting the requirement that the penetration testing be "based on relevant identified risks in accordance with the risk assessment."

Penetration testing is costly and potentially disruptive. While some covered entities' risk assessment may necessitate a system-wide penetration testing, covered entities that can identify specific components of their systems that are susceptible should not be required to undergo penetration testing where their assessment deems it unhelpful or not worth the cost and disruption. We believe the DFS should continue to limit the penetration testing requirement to high-risk areas identified by the covered entity's risk assessment, which should provide sufficient protection without overburdening covered entities with no increased benefit.

VII. Other areas of technical ambiguity.

In addition to our more significant points above, we also identified the following issues and ambiguities that we recommend the DFS can address in the final rule:

- Clarify the scope of the independent audit requirement and which requirements of the Proposed Rule are intended to be audited;

- Clarify the meaning of "qualified" in the penetration testing requirement ("penetration testing of their information systems from both inside and outside the information systems' boundaries by a **qualified** internal or external independent party at least annually" (**emphasis added**)); and

- If the gross annual revenue threshold is retained, define the scope of "gross annual revenue."

VIII. Conclusion

If desired by the DFS, IIB would be pleased to assist the DFS in the development of any of the recommendations discussed in this letter or in any other manner as the DFS undertakes to implement the statutes appropriately and effectively.[13]

* * *

We appreciate your consideration of the issues raised in this letter and stand ready to provide any further information that may be helpful. Please contact the undersigned (646-213-1149, swebster@iib.org) or our Chief Executive Officer, Beth Zorc (646-213-1147, bpolichene@iib.org).

Very truly yours,

Stephanie Webster
General Counsel

[13] While we did not comment on it herein, we note that the revised penalty provision in the Proposed Rule would impose a penalty for every 24-hour period a party fails to comply with a requirement of the Proposed Rule. We are concerned that this appears to impose a daily penalty when the statute under which the provision was promulgated authorizes only a "per violation" penalty. We believe doing so is beyond the DFS's statutory authority.