August 14, 2023

Submitted via email: cyberamendment@dfs.ny.gov

New York State Department of Financial Services
1 State Street
New York, NY 10004

**Re: Cybersecurity Requirements for Financial Services Companies (June 28, 2023)**

Dear Sir or Madam,

The Securities Industry and Financial Markets Association ("SIFMA")[1] and the Bank Policy Institute ("BPI")[2] (together, "the Associations") appreciate the opportunity to comment on the New York Department of Financial Services' ("NYDFS" or the "Department") Revised Proposed Second Amendment to 23 NYCRR 500 ("Revised Amendment").

The Associations thank the Department for its responsiveness to the previous comment period. The Associations welcome many of the changes in the Revised Amendment, particularly amending the definitions of "Class A Companies" and "Independent Audit," narrowing the scope of business continuity and disaster recovery ("BCDR") plans to the covered entity's information systems and material services, and amending governance requirements around cybersecurity expertise.

[1] The Securities Industry and Financial Markets Association ("SIFMA") is the leading trade association for broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets. On behalf of our industry's one million employees, we advocate on legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association ("GFMA"). For more information, visit http://www.sifma.org.

[2] BPI is a nonpartisan group representing the nation's leading banks. BPI members include universal banks, regional banks, and the major foreign banks doing business in the United States. Collectively, BPI members hold $10.7 trillion in deposits in the United States; make 68% of all loans, including trillions of dollars in funding for small businesses and household mortgages, credit cards, and auto loans; employ nearly two million Americans; and serve as a principal engine for the nation's financial innovation and economic growth. Business, Innovation, Technology and Security ("BITS"), BPI's technology policy division, provides an executive-level forum to discuss and promote current and emerging technology, foster innovation, reduce fraud, and improve cybersecurity and risk management practices for the financial sector.

These changes represent clear progress toward creating a risk-based regulatory framework that can ensure and improve the safety and resiliency of the New York financial services industry's digital infrastructure. However, the Associations believe there are additional areas where the Revised Amendment can be further enhanced. We respectfully offer the following recommendations for further revision.

## Executive Summary

The recommendations and considerations discussed at greater length below include, among others, the following:

- **MFA Requirements**: The Associations are concerned that the Revised Amendment now states that multi-factor authentication ("MFA") must "be utilized for any individual accessing any of the covered entity's information systems." Section 500.12(a). It is unclear whether these new MFA requirements would encompass employees who are accessing routine parts of the company network while using a computer at the office. The Associations understand that employees using a physical office keycard or ID badge to enter their office would be providing a possession factor that, when paired with a knowledge or inherence factor, would satisfy the MFA requirements. Similarly, the Associations understand that, for employees that access information systems on their mobile devices, when such access involves mobile device management software or other possession tokens, along with password requirements, that would satisfy the MFA requirements. If NYDFS does not share the Associations' understanding of possession factors, the Department should reconsider this approach and revert to the language in the previous draft of the Second Amendment, or, at a minimum, consider reinserting language to allow entities to implement MFA using a risk-based approach. The Associations also urge the Department to clarify that MFA requirements do not apply to customers accessing their own information. If robust MFA requirements were required for customer use, that would impose significant burdens on customers without meaningful additional cybersecurity for the individual or the covered entity.

- **Frequency of Certain Requirements**: The Associations note that, in addition to the annual risk assessment, covered entities have annual assessment requirements for the independent audit, policy and procedure review, penetration testing, user access privilege review, application security development review, testing of incident response plans and business continuity and disaster recovery plans with senior officers and the CEO, and the ability to restore critical data and information systems from backups. The Associations urge the Department to consider retaining the annual risk assessment while removing the annual cadence for other assessment requirements and instead allow companies to fulfill these

requirements periodically, consistent with risks identified in the annual risk assessment, but at least once every three years.

- **Approval of Cyber Policies**: The Associations understand that NYDFS elected not to remove the requirement that governing bodies approve their covered entity's cybersecurity policy to ensure that boards are aware of cybersecurity risks. The Associations agree with the Department that boards must be aware of cybersecurity risk, but do not believe that approving cybersecurity policies is the best or only way to achieve that objective. Instead, management should develop, approve, and implement the cybersecurity policies, and boards, or appropriate board committees, should be aware of those policies in order to effectively carry out their oversight obligations. Doing so would align Part 500 with other regulatory regimes like the Gramm-Leach-Bliley Act.

- **CISO Responsibilities**: The Associations are concerned that the requirements under the new definition for Chief Information Security Officers ("CISO") in Section 500.1(c) could misplace responsibility for potential failures to direct sufficient resources to cybersecurity. The Associations urge the Department to remove the language that requires CISOs to have adequate authority to direct sufficient resources to implement and maintain an effective cybersecurity program or make clear that this responsibility rests with management and not the CISO.

- **Notification of Cybersecurity Events**: As currently drafted, the Revised Amendment has three notification triggers for cyber events that depend on impact to the covered entity. The Associations urge NYDFS to clarify that the notification trigger for unauthorized access to a privileged account also requires an impact to the covered entity and that the unauthorized access involves a privileged account associated with a material part of the covered entity's information system. Additionally, the Associations urge the Department to clarify that covered entities are only required to notify under Section 500.17(a)(1)(i) when notice is required to be provided ***by the covered entity*** to any government body, self-regulatory agency, or any other supervisory body. Finally, the Associations urge the Department to adjust the continuing obligation in Section 500.17(a)(2) such that it only applies to updates on material changes or additions to information previously provided.

- **Notification of Compliance**: The Associations welcome the addition of a materiality threshold for certifying compliance in Section 500.17(b)(1)(i) and urge NYDFS to adopt the same threshold for the documentation requirements for certifications and for the acknowledgment of noncompliance. The Associations also welcome NYDFS removing the requirement that covered entities that submit a written acknowledgement of noncompliance include the areas that required

material improvement. For the same reasons, the Associations urge NYDFS to also eliminate the requirement that covered entities submit a written acknowledgment describing the nature and extent of their noncompliance. Finally, the Associations urge the Department to reconsider requiring CEOs to certify compliance under Section 500.17(b)(2), as CEOs are often not deeply involved in overseeing cybersecurity and instead delegate that responsibility to another member of senior management who would be better positioned to certify along with the CISO.

- **Privileged Access Requirements**: The Associations urge the Department to make the requirement for a Class A company to monitor privileged access activity based upon the company's risk assessment. The Associations also urge the Department to clarify that the requirement for Class A companies to implement an automated method of blocking commonly used passwords applies to all privileged accounts and not to all accounts. Alternatively, the Associations urge the Department to consider replacing the requirement for an automated method of blocking commonly used passwords with a requirement for covered entities to configure password complexity (i.e., letter, number, special character), limits on invalid login attempts before an account is locked, minimum password length, and configuration of password history.

Below, we have categorized these topics and others as follows: **(a)** technical requirements; **(b)** governance requirements; **(c)** notification requirements; and **(d)** timing considerations. We believe these topics need to be addressed in order to achieve the goal of enhancing governance around cybersecurity and keeping our organizations and ecosystem safe.

## Discussion

### Technical Requirements

#### 1. MFA Requirements

The Associations are concerned with the significant expansion of MFA requirements in the Revised Amendment, as it mandates that MFA "be utilized for any individual accessing any of the covered entity's information systems." Section 500.12(a). This would appear to encompass employees who are accessing routine parts of their company's network while using a computer at the office.

The Associations understand that employees that use a corporate-issued physical keycard, ID badge, or equivalent to enter their office would be providing a possession

factor.[3] Thus, an employee that is at the office using one of these possession factors and then uses a knowledge factor such as a password to access the company network would satisfy the requirement to use MFA to access a covered entity's information system. Similarly, for employees that access information systems on their mobile devices, when such access involves mobile device management software of other possession tokens, along with password requirements, that would satisfy the MFA requirements. Our members indicate that these MFA procedures align with industry practice.

To the extent the Associations' understanding does not align with the Department's intention for MFA use, the Associations urge NYDFS to reconsider the scope of this requirement and revert to the language in the previous draft of the Second Amendment to Part 500. Employees accessing a network while on premises are protected by physical security and additional controls on their computer. Mandating that each employee use another control in addition to a username and password to access their given network when on the premises would create a significant burden without meaningful cybersecurity benefits.[4] At a minimum, the Associations urge the Department to allow entities to implement MFA using a risk-based approach.

The Associations also believe that the MFA requirements do not require customers to use MFA to access their own information. To the extent that the Department disagrees, the Associations urge the Department to clarify that the MFA provisions as applied to customers are risk-based and that controls such as trusted devices, login analysis, and impossible travel satisfy the Part 500 MFA requirements.

**2. Clarify Backup Requirements**

As currently drafted, Section 500.16(a)(2)(v) requires BCDR plans to include procedures for backing up information offsite, while Section 500.16(e) requires covered entities to maintain backups. Read together, it is ambiguous whether the offsite requirement in Section 500.16(a)(2)(v) can be met with equivalent on-premises security. The Associations urge the Department to make this clear by adding "or with equivalent on-premises security" after "storing such information offsite" in Section 500.16(a)(2)(v).

**3. Allow for "Effective Compensating Controls" for Encryption in Transit**

The Associations' previous comment discussed data-loss prevention solutions as one example of a potential "effective compensating control" for encryption in transit.

---

[3] NIST, for example, lists "an ID badge" as an example of "something you have" for purposes of authentication. National Institute of Standards and Technology, *NIST Special Publication 800-63-3 Digital Identity Guidelines*, Section 4.3.1 (June 2017), https://pages.nist.gov/800-63-3/sp800-63-3.html.

[4] *See generally Multifactor Authentication: Opportunities and Challenges*, BANK POLICY INSTITUTE (Feb. 27, 2023), https://bpi.com/multifactor-authentication-opportunities-and-challenges/.

The Associations understand the Department's response that this example may not prevent nonpublic information that is actually sent. However, the Department's response leaves open the possibility that secure transmission channels may satisfy the encryption in transit requirements if they encrypt communications being sent.

In addition to secure transmission channels, other controls, such as aggregating or de-identifying data, can allow covered entities to securely send communications. Therefore, the Associations urge the Department to allow for effective compensating controls to encryption in transit requirements under Section 500.15. Specifically, the Associations urge the Department to reinstate the language in the former Section 500.15(a)(1), which allowed covered entities to "secure … nonpublic information [in transit over external networks] using effective alternative compensating controls reviewed and approved by the covered entity's CISO."

**4. Privileged Access Requirements**

The Associations urge the Department to make the privileged access requirements for a Class A company under Section 500.7(c) based upon the covered entity's risk assessment. While Section 500.7(a) attaches access privilege and management policy requirements to a covered entity's risk assessment, Section 500.7(c) provides additional requirements that appear not to be based on a risk assessment. Given that privileged access management solutions vary in purpose and function, it makes sense for Section 500.7(c) to be risk-based, as is the case with Section 500.7(a).

The Revised Amendment also produces an ambiguity around the scope of privileged access requirements. Specifically, Section 500.7(c) provides requirements for Class A companies around ***privileged accounts***. However, Section 500.7(c)(2) states that Class A companies must "implement an automated method of blocking commonly used passwords for ***all accounts***." Given the placement of the requirement around blocking commonly used passwords, the Associations assume the Department intended for this requirement to only apply to privileged accounts. Nonetheless, the Associations urge the Department to clarify this point by adding "privileged" between "all accounts" in Section 500.7(c)(2).

Alternatively, the Associations urge the Department to consider replacing the requirement for an automated method of blocking commonly used passwords with a requirement for covered entities to configure password complexity (i.e., letter, number, special character), limits on invalid login attempts before an account is locked, minimum password length, and configuration of password history. This approach may provide broader cybersecurity benefits, as blocking commonly used passwords is limited to the finite scope of common passwords checked without any parameters for managing access, such as locking out an account after a certain number of invalid attempts. Password configuration and access management parameters may thus provide greater and broader means of minimizing risk to account compromise.

### 5. Vulnerability Management

The Associations believe that the penetration testing requirement should be limited to high-risk areas identified by the covered entity's risk assessment. While the Associations appreciate the Department's statement that covered entities should perform penetration testing in accordance with their risk assessment, Section 500.5(a)(1) nonetheless removes the provision that covered entities perform penetration testing "based on relevant identified risks in accordance with the risk assessment." To align with the Department's risk-based approach, NYDFS should restore the language that makes penetration testing "based on relevant identified risks in accordance with the risk assessment" in Section 500.5(a)(1).

Additionally, the Revised Amendment would require covered entities to "timely remediate vulnerabilities, giving priority to vulnerabilities based on the risk they pose to the covered entity." Section 500.5(c). To provide covered entities more flexibility to remediate vulnerabilities in accordance with the risk those vulnerabilities pose, the Associations urge NYDFS to remove the requirement that all remediations be "timely."

### 6. Asset Management

The Associations note that the Revised Amendment's asset management provisions require covered entities to track key information for each asset, including the "classification or sensitivity" of such assets. As "assets" is an undefined term, the Associations urge NYDFS to clarify the meaning of Section 500.13(a)(1)(iii) by adding "data" in front of "classification" and "sensitivity."

## Governance Requirements

### 7. Incident Response and BCDR Plan Testing

To the extent the Department is unwilling to remove the annual cadences described below, the Associations urge the Department to clarify and adjust the requirements for incident response and BCDR plan testing. First, the Department should clarify that tabletop exercises are within the meaning of incident response plan testing. Specifically, the Department should add "including tabletop exercises" after "incident response" in Section 500.16(d)(1).

Second, the Associations urge the Department to provide covered entities with the option to have the highest-ranking executive either participate in incident response and BCDR plan testing or receive a briefing on the testing. The option to have the CEO briefed on the incident response and BCDR plan testing could come in the CISO requirements as outlined in Section 500.4(b).

If the Department declines this recommendation, the Associations urge the Department to change the cadence for CEO participation in BCDR plan testing from annually to periodically based on the risk assessment, but at least every three years. Given the demands on CEO time, it will be more effective and practical to have the CEO participate in incident response plan testing rather than the more technical BCDR plan testing.

**8. Management, Not Boards, Should Approve Cyber Policies**

The Associations urge NYDFS to again consider removing the requirement that governing bodies approve their covered entity's cybersecurity policies. Given the technical—and often voluminous—nature of such policies, a covered entity's management is much better suited to develop, approve, and implement these policies with oversight from the senior governing body.

The Department cited its position that boards "must be aware of cybersecurity risks and ensure the company has a written cybersecurity policy in place" as reason for not removing this requirement. The Associations agree that boards need to be aware of cybersecurity risks to exercise oversight. We do not, however, agree that "approv[ing] [cybersecurity] policy is the most effective way to achieve this goal."[5] Requiring boards to approve cybersecurity policies likely will not make those policies more robust or result in greater board awareness of cyber risk. Instead, the Associations urge the Department to require that management develop, approve, and implement cybersecurity policies and ensure that boards, or appropriate board committees, are aware of those policies as part of their duty to effectively carry out their oversight obligations.

Doing so would put Part 500 in line with other applicable standards, such as the Interagency Guidelines established pursuant to the Gramm-Leach-Bliley Act,[6] wherein boards, or appropriate board committees, are initially responsible for approving a financial institution's written information security program but after which annual approval is not required. Instead, under the Interagency Guidelines, boards oversee the implementation and maintenance of the program through annual reports. As such, at least after initial approval, cybersecurity policies should be approved by management and reviewed by the board.

**9. Reconsider Resource Allocation Requirements for CISOs**

The Department moved requirements for CISOs to have the ability to direct sufficient cybersecurity resources in the Revised Amendment to the definition for CISO.

---

[5] *Id.* at 22.

[6] 15 U.S.C § 6801 et seq.

While the Department explained that the CISO is subject to a covered entity's regular budgetary approval process, it also warned that "an insufficiently resourced cybersecurity program may result in a covered entity's non-compliance with Part 500 if the covered entity is unable to meet the other requirements contained in Part 500."

The Associations agree with the Department that an insufficiently resourced cybersecurity program may result in a covered entity's noncompliance with Part 500. While we recognize the Department responded to concerns over the CISO having the ability to direct sufficient resources to the cybersecurity program, the Associations believe this requirement is unnecessary, as the consequence for an insufficiently resourced cybersecurity program will, in all likelihood, be that the covered entity will fail to meet the requirements of the rest of Part 500. A failure to direct sufficient resources to cybersecurity is often not a CISO issue. Therefore, the Associations urge the Department to remove this requirement from the CISO definition and instead recommend adding a requirement to Section 500.2 to include "senior governing bodies shall receive sufficient information to assess whether cybersecurity programs continue to be allocated adequate funding to enable covered entities to maintain an effective cybersecurity program in light of changes to the business and evolving risks."

**10. Clarify Language in the Limited Exemption**

The Associations note that the new Section 500.19(b) uses the terminology "wholly-owned subsidiary" for the first and only time in the Revised Amendment. The Associations seek clarification from the Department that "wholly-owned subsidiary" does not have a different meaning than "affiliate."

**Notification Requirements**

**11. Clarify Requirements for Notification of Cybersecurity Event**

The Associations note that three of the four notifiable events under Section 500.17(a)(1)(i)–(iv) require an impact on the covered entity. The Associations suspect that the absence of such a requirement for the notification trigger for unauthorized access to a privileged account is a drafting error and request that NYDFS add this requirement to Section 500.17(a)(1)(iii) in its final rule.

The trigger for access to a privileged account also differs from the trigger for ransomware deployment in that the ransomware deployment must take place "within a material part of the covered entity's information system." The Department should add "within a material part of the covered entity's information system" after "privileged account" in Section 500.17(a)(1)(iii).

Additionally, the Department should clarify that the notification requirement in Section 500.17(a)(1)(i) is triggered only when **a covered entity** must notify any

government body, self-regulatory agency, or other supervisory body rather than when a third-party service provider must notify another regulator. The Department should make this explicit by adding "by the covered entity" after "of which notice is required to be provided" in Section 500.17(a)(1)(i).

Finally, Section 500.17(a)(2) provides that "[c]overed entities shall have a continuing obligation to update and supplement the information provided." The Associations believe this provision is overly broad and could result in over-reporting without corresponding cybersecurity benefits. As such, the Associations urge the Department to use the materiality threshold added throughout Section 500.17(b) so that covered entities have a continuing obligation to update the Department with material changes or new information previously unavailable.

**12. Notice of Compliance Obligations**

As currently drafted, Section 500.17(b)(1) provides an explicit materiality threshold for some obligations but not others. Additionally, the written acknowledgement of noncompliance obligations has been changed to remove some but not all identification requirements that could leave firms vulnerable to cyber-attack. The Associations accordingly urge NYDFS to make the materiality threshold explicit throughout Section 500.17(b)(1) and to remove the requirement that covered entities submitting a written acknowledgment describe the nature and extent of their noncompliance. Finally, the Associations urge the Department to reconsider requiring CEOs to certify compliance under Section 500.17(b)(2), as CEOs are often not deeply involved in overseeing cybersecurity and instead delegate that responsibility to another member of senior management who would be better positioned to certify along with the CISO.

Extend the Materiality Threshold: The Department updated Section 500.17(b)(1)(i) such that covered entities certify that they "***materially*** complied" with Part 500 requirements "during the prior calendar year." Similarly, Section 500.17(b)(1)(ii)(b) now states that covered entities that are providing a written acknowledgment of noncompliance identify sections that they have not "***materially*** complied with."

The Associations welcome these additions and urge NYDFS to extend this threshold throughout Section 500.17(b)(1). Specifically, NYDFS should add "material" after "accurately determine and demonstrate such" in Section 500.17(b)(1)(i) and replace "fully" with "materially" in Section 500.17(b)(ii)(*a*).

Remove the Requirement to Describe Noncompliance: The Associations welcome the removal of the requirement for covered entities submitting an acknowledgment of noncompliance to "identif[y] all areas, systems and processes that require material improvement, updating, and redesign." A covered entity that

documented and submitted such information would provide threat actors with a roadmap to attack it. Similarly, Section 500.17(b)(1)(ii)(*b*)'s requirement that covered entities "describe the nature and extent of such noncompliance" should be removed for the same reason and instead, covered entities should be required to document and maintain that information under 500.17(b)(3).

Allow an Alternative to CEO Certification: The Associations urge the Department to make whomever the CISO reports to an additional signatory for compliance certification. Specifically, the Department should revise Section 500.17(b)(2) to read, in pertinent part, "shall be signed by the covered entity's CISO and the member of senior management to whom the CISO reports."

**13. Compliance Certification Standard**

The Associations are concerned that the Revised Amendment appears to prevent certification if a company is out of material compliance for a 24-hour period at any point during the calendar year. The addition of a materiality threshold for failure to comply with any section of Part 500 in Section 500.20(b)(2) is welcome, and the Associations urge that this threshold apply to both the severity and length of noncompliance in Section 500.20(b)(2). Additionally, the Department should add a materiality threshold to Section 500.20(b)(1) by placing the word "material" between the words "due to" and "noncompliance." In sum, the Associations support the Department's updates to the requirement that would permit covered entities to certify compliance as long as they have been materially compliant during the previous year and on the date of certification. Otherwise, NYDFS will be flooded with filings of immaterial temporary lapses in compliance that have already been remediated.

**14. Event Versus Incident Terminology**:

The Associations urge the Department to use the term "cybersecurity incident" in pertinent notification triggers.

The Associations understand the Department maintained the definition of "cybersecurity event" so that it could obtain information on unsuccessful breach attempts. However, the notification triggers in Section 500.17(a)(1) require a "successful" breach. Therefore, the term "cybersecurity incidents" applies more directly to the triggers described above. The Associations believe the Department can retain the definition of "cybersecurity event" to include unsuccessful events and use this where appropriate elsewhere in Part 500.

**Timing Considerations**

**15. Change the Cadence of Certain Requirements**

The Associations are concerned that the Revised Amendment continues to dictate that many requirements be conducted on an annual basis. As we explained in our previous comment letter, not all elements need a yearly refresh, and a requirement for an annual assessment cadence for the entire cybersecurity program could draw resources away from areas requiring deeper dives, thus reducing an organization's overall security posture. Therefore, the Associations urge NYDFS to replace the annual cadence for many Part 500 requirements with a risk-based approach where such requirements are fulfilled at least every three years.

The Revised Amendment provides for annual requirements for independent audits for Class A companies (Section 500.2(c)), policy and procedure approval (Section 500.3), penetration testing (Section 500.5(a)(1)), user access privilege review (Section 500.7(a)(4)), application security development review (Section 500.8(b)), cybersecurity awareness training (Section 500.14(a)(3)), testing of incident response plans and BCDR plans with senior officers and the CEO (Section 500.16(d)(1)), and the ability to restore critical data and information systems from backups (Section 500.16(d)(2)).

The Associations agree with the Department that the "constantly changing cybersecurity threat and cybersecurity landscape" means companies should revise, update, and re-implement cybersecurity policies and procedures.[7] But this evolving landscape means that companies should have the flexibility to place resources in areas that need them rather than maintain an indiscriminate requirement for an annual cadence for all the assessment requirements.

The Revised Amendment partially provides for this flexible approach in the penetration testing requirements. As the Department explained, Section 500.5 requires covered entities to maintain policies and procedures to conduct penetration testing "in accordance with [the covered entity's] risk assessment."[8] According to the Department, "[e]ach covered entity must determine, in accordance with the risk assessment, which systems and portions of its network to include as part of the penetration testing as the rest of the covered entity's information system."[9] The same flexibility should be given to the other assessment requirements.

The Associations understand that the Department is concerned that "newly disclosed vulnerabilities" would not be captured absent an annual review and implementation cadence. For this reason, the Associations believe that the risk

[7] New York Department of Financial Services, *Assessment of Public Comment*, page 49 https://www.dfs.ny.gov/system/files/documents/2023/06/rev_rp_23a2_apc_20230628.pdf.

[8] *Id.* at 40.

[9] *Id.*

assessment should remain on an annual cadence to inform covered entities of any recently established or emerging vulnerabilities.

Instead of annual requirements, NYDFS should allow companies to fulfill these other assessment requirements periodically, consistent with risks identified in the annual risk assessment, but at least once every three years. This flexible approach will provide companies with the ability to focus their resources effectively on cybersecurity elements that require assessment as indicated by their risk assessment.

**16. Delay Certification Requirements**

The window between the end of the comment period (August 14, 2023) and the date by which the Department will finalize its rule leaves open the possibility that covered entities will need to certify compliance or acknowledge noncompliance according to new requirements in the proposed rule in April 2024. As currently drafted, Section 500.21(d)(1) provides that covered entities have 30 days from the effective date to comply with the new requirements specified in Section 500.17.

Our firms will require time and resources to build out new certification processes given significant changes in the Revised Amendment. By the time the Revised Amendment is finalized, companies will have spent the majority of 2023 with the aim of certifying to current Part 500 requirements. Given that the certification web portal traditionally opens January 1, the Associations urge the Department to delay the effective date for the new requirements in Section 500.17 to at least the certification period in 2025 to allow firms time to adjust to the new requirements and certification processes.

**17. Transition Period**

The Revised Amendment provides a transitional period ranging from 30 days to two years for compliance with new requirements with compliance certification due April 15. The Associations thus urge the Department to confirm that the requirement to identify areas of noncompliance in Section 500.17(b) only applies to provisions for which the transitional period has fully run and are therefore effective.

**18. Compliance Windows**

The Associations urge NYDFS to extend the compliance windows for the requirements for Class A companies to perform independent audits and implement privileged access monitoring and for penetration testing.

Extend the compliance window for the Class A company independent audit requirement: The Revised Amendment currently provides a 180-day compliance window for the Class A company independent audit requirement. Given that requirements for policies and procedures that the independent audit will cover are set to roll out over an

extended period beyond 180 days, the Department should extend the effective date to 18 months to allow for implementation and appropriate direction of resources.

Extend the compliance window for penetration testing: The Department should extend the effective date for compliance with penetration testing requirements to one year to accommodate the increased scope of internal penetration testing and allow for larger companies to execute on a larger scope of testing.

Extend the compliance window for privileged access monitoring for Class A companies: Implementing privileged access management solutions, such as automated password blocking for various custom applications, is a complex task for larger companies that will require time and resources, particularly if the Department rejects our position that the requirement to implement an automated method of blocking commonly used passwords should be limited to all ***privileged*** accounts. The Associations therefore urge the Department to extend the effective date for compliance to two years.

* * *

If you have any questions or would like to discuss these comments further, please reach out to Heather Hogsett at heather.hogsett@bpi.com or Melissa MacGregor at mmacgregor@sifma.org.

Respectfully submitted,

/s/ Heather Hogsett
Heather Hogsett
Senior Vice President, Technology & Risk Strategy, BITS
Bank Policy Institute

/s/ Melissa MacGregor
Melissa MacGregor
Managing Director & Associate General Counsel
Securities Industry and Financial Markets Association

cc: Erez Liebermann, Partner, Debevoise & Plimpton, LLP
Thomas Wagner, Managing Director, Technology & Operations, SIFMA