sifma

Invested in America

August 17, 2022

Submitted via email: cyberamendment@dfs.ny.gov

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

**Re: Cybersecurity Requirements for Financial Services Companies (July 29, 2022)**

Dear Sir or Madam,

The Securities Industry and Financial Markets Association ("SIFMA")[1] appreciates the opportunity to comment on the pre-proposed outreach from the New York State Department of Financial Services ("NYDFS") amending the Cybersecurity Requirements for Financial Services Companies dated July 29, 2022 ("Preproposal").[2] SIFMA understands that this is a preview of the forthcoming official rule proposal but gives stakeholders an opportunity to provide initial comments. SIFMA appreciates this foresight and would like to highlight some significant concerns for consideration. We would welcome the opportunity to meet with the NYDFS to further discuss these concerns prior to the rule proposal being issued.

As you know, SIFMA members take cybersecurity very seriously not only due to the significant regulatory requirements imposed by federal and state governments, but also because protecting client assets and information is paramount to gaining public trust and maintaining competitiveness in the industry. In other words, cybersecurity is not just a regulatory obligation but a critical component of any financial institution's business strategy. Further the imposition of prescriptive regulatory requirements with little benefit to consumers, may cause companies to divert resources from proactively guarding against emergent threats to meeting prescriptive

[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] *See* New York Department of Financial Services Pre-Proposed Outreach re: 23 NYCRR 500 Cyber Security Requirements for Financial Services Companies (July 29, 2022).

regulatory obligations. Maintaining principles-based requirements provides financial institutions with the groundwork needed to maintain a high level of cybersecurity.

SIFMA notes that new technology requirements, such as multifactor authentication for all privileged accounts, password vaults, endpoint detection, and centralized logging, are all significant multi-year investments in cybersecurity, which would be required as early as 2023, under the Preproposal. The proposed technology requirements are more prescriptive than the previous requirements, and do not provide flexibility for members to be agile in implementing and resourcing technologies to support cybersecurity programs.

Additionally, SIFMA urges the NYDFS to provide additional public assurances/disclosure as to its own/internal data security practices. The data/information that NYDFS is requiring is highly sensitive/proprietary and could make the NYDFS vulnerable to attack. This will ensure that member firms are able to meet their regulatory obligations while ensuring the security of third-party data collection disclosure.

Before discussing our more detailed concerns with the Preproposal below, SIFMA urges NYDFS to consider the following broad changes:

- Replace granular requirements with outcome-based requirements, such as universally allowing qualified experts to adopt alternative technologies and equivalent compensating controls in achieving the required outcome. This recommendation applies to Sections 500.2(c), 500.2(d), 500.4(b), 500.4(c), 500.7(a), 500.7(b), 500.12(a), and 500.14(b) of the Preproposal, as explained below.

- Allow flexibility in implementation of requirements that entail high costs, organizational disruption, or a long timeline to implement, such as: (i) allowing Covered Entities to consider cost-benefit analysis as part of the risk-based approach in implementing certain requirements; (ii) allowing Covered Entities to adopt equivalent compensating controls in achieving the required outcome; and (iii) extending the implementation timelines. This recommendation applies to Sections 500.2(c), 500.9(c), 500.9(d), and 500.13(a) of the Preproposal, as explained below.

- Clarify the NYDFS's intention within the text of the amended rule, to avoid ambiguity and the possibility of an overly broad interpretation of the requirements. Some concepts in the Preproposal that may be prone to misinterpretation include independence, ability to delegate authority, and threshold for materiality. Accordingly, this recommendation applies to Sections 500.1(f) and 500.4(a) of the Preproposal, as explained below.

This is a brief preliminary overview of the areas that we believe need to be addressed prior to the release of the official rule proposal. Please note that given the short comment period, this is not an exhaustive list.

1. **Expansion of Covered Entities**. The definition of "Covered Entity" was expanded to include "entities that are also regulated by other government entities." The NYDFS should provide additional guidance on what this clause is intended to cover and to make clear that it is not intended to regulate entities it does not license due to such entities being regulated by any government agency, either within or outside the State of New York. (Section 500.1(d))

2. **Classification and Obligations for "Class A" Companies**. The Preproposal introduces a Class A company designation for firms with over 2,000 employees or over $1 billion in gross annual revenue, inclusive of affiliate operations, and subjects them to new, prescriptive requirements. The NYDFS does not specify how it arrived at these human capital and financial thresholds and does not account for the significance of cyber threats to the financial industry generally. To advance a holistic approach to cybersecurity preparedness within the financial industry, and across economic sectors, the NYDFS should defer such categorizations and related regulation to other agencies' well-established classifications (e.g., Cybersecurity and Infrastructure Security Agency and the designation of critical infrastructure firms.) Any requirements for risk assessments and controls should be based on the sensitivity/risk level of data rather than corporate headcount revenue. Such distinctions put Class A companies at a competitive disadvantage and give non-Class A companies an arbitrary pass. Furthermore, the Preproposal includes several new requirements for Class A Companies that will have little to no apparent benefit for consumers but that will impose significant costs as drafted. These include annual audits, triennial "independent" audits, password controls, the gathering and retention of affiliate and outside vendor documentation in support of the written certification of compliance, and monitoring. (Sections 500.2(c) and (d), 500.7(b), 500.14(b))

3. **Independent Audit**. SIFMA appreciates that the NYDFS has recognized that an independent audit can be conducted by either internal or external auditors, but the NYDFS should provide clear guidance on how companies should assess the independence of internal auditors. Further, by prescribing the annual timeframe, organizations are not able to leverage a risk-based approach as dictated throughout the regulation. Also, this independent audit requirement could be deemed to be duplicative of the regular NYDFS examinations that validate the cybersecurity program of the company. (Section 500.1(f))

4. **Senior Governing Body and Board Reporting**. The definition of "Senior Governing Body" should expressly include delegates of the senior governing body, including senior officers. Imposing new requirements on boards of directors

relating to active involvement (versus oversight) in cybersecurity policies and procedures is not practicable or reasonable and should be limited to a notification requirement for significant cyber events and not day-to-day processes. Further, the Preproposal requires the Chief Information Security Officer ("CISO") to address specific topics in the written report to the board instead of allowing briefings on the evolving nature of cyber risks and specific aspects of each company's defensive posture. This would allow boards to rely on the expertise of those delivering the briefings, rather than explicitly dictating the content of board briefings. Finally, the NYDFS should not require boards to include cybersecurity experts as there are a limited number of qualified persons and these companies would face considerable competition to retain such directors. The NYDFS should also clarify what constitutes evidence of "expertise" for the purposes of this section. SIFMA supports the integration of cybersecurity expertise and decision making through their board members and management, but these decisions should be left to businesses and not mandated by the NYDFS or other regulatory bodies. (Section 500.4(b) and (c))

5. **CISO Independence**. The NYDFS should provide additional guidance on how to determine whether a CISO has sufficient independence. (Section 500.4)

6. **Pen Testing and Vulnerability Assessments**. The NYDFS should provide additional guidance on what is meant by "qualified independent party" for pen testing and vulnerability assessments. As with the undefined parameters of CISO independence noted above, absent such guidance, covered entities may spend money to retain third parties to perform this work that may ultimately not be deemed "qualified" and independent for this work. (Section 500.5(a))

7. **Privileged Accounts**. The NYDFS should amend Section 500.7(b)(2) to read "an automated method of blocking commonly used passwords <u>for privileged accounts</u>" (new text underlined) so that this provision aligns with the rest of this section.

8. **Risk Assessments**. The Preproposal requires companies to conduct an impact assessment when a change in the business or technology causes a material change in cyber risk. Because the existing regulation already embodies a risk-based approach to cybersecurity, the NYDFS should define what constitutes a "material change to cyber risk." Conducting a risk assessment for most changes to a business without specified parameters could be excessive and overly burdensome with no material consumer benefit. Further, adding the obligation on a Class A Company would subject a registrant to five or more redundant risk assessments and examinations of the same cybersecurity control structure, including a: 1) NYDFS 3-year Independent Review; 2) NYDFS Annual Risk Assessment; 3) NYDFS Regulatory Examination; 4) NYDFS Execution of the Cyber Program Review; 5) Internal Audit Cybersecurity Program Review. This level of review

would be overly burdensome, costly, inefficient, and unnecessarily disruptive to business operations and cybersecurity programs. Additionally, in the case of large organizations that already have enterprise risk assessment processes which align to previous NYDFS requirements, the additional specifications will require them to perform a unique "NYDFS" risk assessment for each Covered Entity to satisfy these new requirements due to the specificity of the requirements creating an undue burden for large organizations. The NYDFS should also define what constitutes an impact assessment. (Section 500.9(c) and (d))

9. **Third Party Service Provider Policies**. The Preproposal eliminates the ability of employees, representatives, and designees of a covered entity to adopt and rely on the enterprise policies relating to third party vendors and would require them to adopt their own. Not only is this contrary to the way many Class A companies operate, but companies would likely adopt the identical plan or "hire" the parent company for this function, thus coming to the same result. This limited exception should be retained. (Section 500.11(c))

10. **Access Controls**. Certain requirements in the Preproposal for access controls are overly prescriptive and do not leave enough flexibility for organizations to manage technology access and authentication using a risk-based approach for the criticality of applications and the sensitivity of data held by the company. Further, the Preproposal would no longer allow for reasonably equivalent or more secure access controls for remote network access instead of multifactor authentication. The NYDFS should allow companies to maintain the flexibility to implement compensating controls, because companies must manage risks in different ways and cannot always be tied to one method of authentication. In addition, the broad language documented in Section 500.12(b) mandates the use of multi-factor authentication for "enterprise and third-party applications" which conflicts with Section 500.12(a) which indicates required authentication would be based on a risk assessment. As the NYDFS found in one enforcement action, the use of multi-factor authentication is no guarantee against cybersecurity incidents or related losses.[3] Further, NYDFS should supply its definition for privileged accounts. (Sections 500.7(a) and 500.12(a) and (b))

11. **Asset Inventory.** The NYDFS is looking to expand data retention requirements by requiring Covered Entities to maintain asset inventories for "all information systems and their components such as hardware, operating systems, applications, infrastructure devices, APIs, and cloud services." These inventories must also include sensitive metadata such as data classification, recovery requirements, asset locations, and owners. Maintaining detailed asset inventories is an onerous data aggregation effort for large firms with a large data footprint. Moreover, as

[3] In the matter of Residential Mortgage Services, Inc., Consent Order (March 3, 2021).

this data footprint grows, it will increase the attack surface through which a firm can be impacted by unauthorized access or tampering. Further, even though the provision on tracking information includes the caveat, "as applicable," such requirements tend to become default rules, so Section 500.13(a)(1) should be revised to read: "(1) appropriate tracking key information for each asset." The NYDFS should also clarify whether the CISO will in fact have to sign off on IT asset inventories and whether the asset inventory must include third parties. Given the level of detail and complexity required for complete asset inventories, the compliance date for this provision should be extended by at least an additional year. The NYDFS should also consider the application of a reasonableness standard to the inventory requirements, recognizing that IT components are continuously changing. (Section 500.13)

12. **Encryption**. The removal of Section 500.15(a)(1) seems to indicate that firms maintain the obligation to encrypt data in transit over external networks but no longer are able to rely on alternative compensating controls when the encryption is infeasible. Additionally, companies are no longer allowed to rely on risk assessments when making encryption decisions. The NYDFS should clarify that the inclusion of "industry standards" in this provision modifies the encryption standards themselves (i.e., using NIST standard encryption) rather than what firms ultimately decide to encrypt. (Section 500.15(a)(1))

13. **Operational Resilience**. The Preproposal would require a covered entity's Chief Executive Officer (CEO) to be personally involved in the periodic tests of the company's incident response plan. This is unnecessary as most plans involve the CEO and other C-suite employees on a limited basis but forcing a company's most senior executive to sit through extensive exercises to play a limited and unique role is not an efficient use of resources. (Section 500.16(d))

14. **Notifications**. Certain reporting requirements in the Preproposal are duplicative of existing requirements or do not provide any material consumer benefit. To the extent a cyber-event involves access to a privileged account, it may already be reportable under existing Section 500.17(a)(2). This new requirement does not include the materiality threshold and would require reporting an event in cases where access is obtained to a privileged account of little to no value, or one that does not have access to non-public information. This is especially true given the broad definition of "privileged account." The NYDFS should also consider including an option to provide a preliminary notification of a cyber-event by phone with subsequent, additional, information provided through the electronic form after the investigation, similar to what is required by federal prudential regulators.[4] (Section 500.17(a))

[4] 12 CFR Part 225.

15. **Notice of Compliance**. The Preproposal would require companies to include as part of their annual compliance notice of all the provisions of the rule that the company did not comply with and identify "all areas, systems, and processes that require material improvement, updating, or redesign." Compliance should be viewed to include compliance with terms of a Part 500 provision and/or application of compensating controls (i.e., the written acknowledgement of non-compliance should not require detailing application of compensating controls but limited to areas of no compliance.) Additionally, the certification should not be required from the CEO, but deferred to personnel within the Covered Entity that is appropriately positioned to comment on the firm's cybersecurity program (e.g., CISO or other senior officer responsible for a program's cybersecurity). Finally, such a notice if leaked or obtained by a third-party could be used as a roadmap for a cyber-attack by bad actors. (Section 500.17(b))

16. **Extortion Payments.** The NYDFS has proposed that Covered Entities notify the NYDFS within 24 hours of an extortion payment being made. Extortion events made in connection with a cybersecurity event are not necessarily indicative of a weak cybersecurity posture, and the prescriptive requirements seem punitive by adding burden and pressure to the attacked target experiencing strain. Additionally, should the NYDFS continue to require an explanation of the payment as proposed under 500.17(c)(2), the NYDFS should represent that it will maintain such information as strictly confidential and will not publicly disclose such information given potential, unwarranted reputational risk to disclosing firms. We also note that Congress recently passed the Cyber Incident Reporting for Critical Infrastructure Act, which will require critical infrastructure entities to report material cybersecurity incidents and ransomware payments to CISA within 72 and 24 hours, respectively. We urge the NYDFS to coordinate with federal regulators including CISA and ensure that that companies are not double victimized and being unnecessarily punished in these instances. (Section 500.17(c))

17. **Violations & Penalties**. SIFMA believes that a violation constituting "the failure to comply for any 24-hour period with any section or subsection of this Part" does not adequately allow companies acting in good faith more than 24 hours to remedy even a minor compliance deficiency. Further, a major cyber-event may warrant more than 24-hours of work to bring a firm back into compliance with the rules. Even where mitigating factors are considered by the NYDFS when assessing any penalty, the amended process appears to be inefficient, unfair, and unnecessarily burdensome. (Section 500.20)

18. **Implementation Period**. SIFMA is concerned that 180 days will not be enough time to implement the rules the complexity of these requirements. SIFMA encourages the NYDFS to extend that timeline to at least two years. Proposed

amendments to Section 500.22 (c) and (d) relate to transitional periods for rule implementation. The NYDFS should not make any aspect of the proposal effective for calendar year 2022 (i.e., in scope for the certification to be completed by April 15, 2023). In particular, given Section 500.22 (d) (1), there is a significant possibility that the requirements of Part 500.17, including new certification requirements/acknowledgment of non-compliance requirements, would be in effect for the next certification period due April 15, 2023. Firms should be afforded sufficient time to address and uplift programs for any proposed additions to Part 500.

19. **Cost-Benefit Analysis**. SIFMA urges the NYDFS to conduct a careful cost-benefit analysis of the Preproposal as SIFMA believes that the implementation costs of these changes could far exceed the existing rule requirements. Some of what is being proposed may require significant reorganization of personnel for some firms and calls for the retention of layers of additional third-party consultants and experts.

* * *

We look forward to continuing to work with the NYDFS to find solutions that help better protect New York State consumers as well as businesses. We would welcome the opportunity to meet with the NYDFS staff to discuss these concerns. Please contact Melissa MacGregor at mmacgregor@sifma.org or Tom Wagner at twagner@sifma.org at your convenience to schedule a meeting.

Sincerely,

*Melissa MacGregor*

Melissa MacGregor
Managing Director & Associate General Counsel

*Thomas Wagner*

Thomas Wagner
Managing Director, Technology & Operations

cc: Justin Herring, Executive Deputy Superintendent, Cybersecurity Division, NYDFS
Marin Gibson, Managing Director, State Government Affairs, SIFMA
Nancy Lancia, Managing Director, State Government Affairs, SIFMA
Thomas Price, Managing Director, Technology & Operations, SIFMA