November 14, 2016

Cassandra Lentchner
Deputy Superintendent for Compliance
New York State Department of Financial Services
One State Street
New York, NY 10004-1511
CyberRegComments@dfs.ny.gov

Re: New York Department of Financial Services' Proposed Rulemaking on Cybersecurity Requirements for Financial Services Companies, I.D. No. DFS-39-16-00008-P

Dear Ms. Lentchner:

On behalf of the Securities Industry and Financial Markets Association ("SIFMA"),[1] the American Bankers Association ("ABA"), the Financial Services Roundtable ("FSR/BITS"), the Financial Services Sector Coordinating Council ("FSSCC"), the Mortgage Bankers Association ("MBA"), the American Financial Services Association ("AFSA"), the American Land Title Association ("ALTA"), and the New York Mortgage Bankers Association ("NYMBA"), we appreciate the opportunity to submit this comment letter to the New York State Department of Financial Services ("DFS") in connection with its proposed rulemaking on Cybersecurity Requirements for Financial Services Companies (the "Proposal"). We commend DFS in its efforts to strengthen and improve cybersecurity in the financial sector, and we look forward to working with DFS to improve cybersecurity protections.

We respectfully request that any rule resulting from the Proposal (a) be complementary and consistent with existing cybersecurity requirements; (b) embody a risk-based approach; and (c) be revised in accordance with our detailed comments. We believe this approach would best enable the financial industry and regulators to continue their coordinated efforts to mitigate cybersecurity risks. Cybersecurity regulations issued by only one state—or by several states—

without an effort to converge and coordinate with existing cybersecurity requirements will lead to confusion, additional costs, and a misalignment of cybersecurity operations within the industry.

We believe these modifications should be implemented in accordance with the National Institute of Standards and Technology ("NIST") Cybersecurity Framework, which has served as a model of collaboration between government and industry in developing a comprehensive risk-based cybersecurity framework widely used across financial firms and more broadly across other critical sectors. Accordingly, we recommend specific changes in the comments below to more closely align any final rule with the NIST Cybersecurity Framework.

* * *

Cybersecurity remains a top priority for the financial industry. Each year, financial firms expend significant resources to safeguard consumer data, protect against cyber crime, and defend against adversaries that target financial institutions—investments that can run as high as $500 million per year for the largest firms. Entities large and small develop information-security plans and deploy all manner of defensive software. They train their front-line employees in best practices and hire experts to revise and further develop protective measures tailored to the specific needs of their firms. Firms also devote a great deal of attention to compliance with cybersecurity regulations. Firms already report that approximately 40 percent of corporate cybersecurity activities are compliance-oriented rather than security-oriented.[2]

SIFMA, ABA, FSR/BITS, FSSCC, MBA, AFSA, ALTA, and NYMBA have taken a leading role in coordinating the industry's response to the demands of cybersecurity by encouraging the adoption of core principles and practices that are risk-based and harmonized across the regulatory environment. The NIST Cybersecurity Framework is the hallmark of such efforts. It was developed as a result of President Obama's Executive Order and involved the participation of over 3,000 cybersecurity professionals from industry, academia, and government, representing the cybersecurity field's consensus on the most effective approach to improve cybersecurity.[3] The NIST Cybersecurity Framework is expressly based on an assessment of risk and designed to improve companies' technical, administrative, and physical protections to combat ever-changing cyber threats. Financial firms already have designed their cybersecurity programs to implement the NIST Cybersecurity Framework and comply with the Federal Financial Institutions Examination Council's ("FFIEC") Cybersecurity Assessment Tool ("CAT") and cybersecurity regulations under the Gramm-Leach-Bliley Act ("GLBA"), which also adopt risk-based approaches.[4]

The Proposal, however, does not adopt or fully recognize the NIST Cybersecurity Framework, the existing federal requirements, and the extensive efforts that firms have made to implement the NIST Cybersecurity Framework and comply with existing requirements.[5] We request that in any final rule DFS adopt a risk-based approach consistent with the NIST Cybersecurity Framework and federal requirements that can adapt to and account for changes in technology and the evolving cybersecurity threat landscape. These revisions would allow firms' cybersecurity programs to leverage existing programs designed to comply with the cybersecurity requirements of other regulators.

Some of the requirements proposed by DFS impose impractical and technically infeasible requirements that would lead to unintended consequences. For example, as we explain below in Section C, the requirement to encrypt data at rest and in transit, deploy multi-factor authentication protections, and maintain audit trails for nearly all information processed by financial firms—as opposed to sensitive data the loss of which would result in significant harm to the consumer—would not align with existing federal requirements and would result in massive inefficiencies and delays in fulfilling customer demands. Such requirements, as explained in greater detail below, also may not strengthen cybersecurity. By changing these and other requirements to incorporate a risk-based approach, any final rule would target the most sensitive data processed by firms and those systems and third parties that are the most vulnerable, while promoting efficiency and compliance. By coordinating with us on these important issues, we believe DFS can facilitate a more robust cybersecurity environment for the financial sector that protects consumer data and the integrity of the markets.

A. Any Rule Resulting From The DFS Proposal Should Complement And Be Consistent With Existing Cybersecurity Requirements.

The financial industry is already subject to numerous cybersecurity regulations and requirements. These regulations, requirements, and guidelines are issued by dozens of regulatory bodies exercising overlapping jurisdiction, including but not limited to the Commodity Futures Trading Commission ("CFTC"),[6] the Securities and Exchange Commission ("SEC"),[7] the Federal Deposit Insurance Corporation ("FDIC"),[8] the Federal Reserve System ("Fed"),[9] the Federal Trade Commission ("FTC"),[10] the National Credit Union Administration ("NCUA"),[11] the Office of the Comptroller of the Currency ("OCC"),[12] the Financial Industry Regulatory Authority ("FINRA"),[13] and the National Futures Association ("NFA"),[14] not to mention requirements and guidelines at the international and state levels.[15] These comprehensive requirements govern all areas of cybersecurity protection, including board engagement, corporate governance, staffing and management, written information security plans, cybersecurity training, technical controls, disposal of sensitive information, and numerous other aspects of cybersecurity.

Government officials and agencies have long-recognized the need for coordination and convergence of cybersecurity regulatory activity. U.S. Treasury Secretary Jack Lew has encouraged agencies "to collaborate with the private sector to establish cyber security best practices and improve information sharing."[16] Comptroller of the Currency Thomas J. Curry has underscored that "[o]ne of the lessons we have learned in the bank regulatory community is that collaboration is vital, especially in dealing with highly complex, rapidly evolving challenges like cybersecurity."[17] And Deputy Treasury Secretary Sarah Bloom Raskin stressed the need to "figure out ways [to]harmonize [cybersecurity standards]. We don't want to see emerge the development of multiple sets of standards, multiple guidances."[18]

DFS has recognized this precise need to collaborate and coordinate on its cybersecurity requirements. The New York Superintendent of Financial Services, at an earlier stage in DFS's efforts to develop cybersecurity requirements, stated "that it would be beneficial to coordinate its efforts with relevant state and federal agencies to develop a comprehensive security framework that addresses the most critical issues, while still preserving the flexibility to address New

York-specific concerns."[19] SIFMA, in its prior comments to DFS, stressed the overriding importance of such coordination and harmonization with existing cybersecurity requirements.[20]

We re-affirm our belief that any final rule would be better served by careful coordination with existing cybersecurity regulations and requirements. In addition to NIST's Cybersecurity Framework discussed above, FFIEC is vested with the power to develop uniform guidance and has separately promulgated the CAT to guide regulators and industry alike in maintaining comprehensive cybersecurity protections at financial firms. FFIEC also has developed comprehensive guidelines, such as the IT Examination Handbook, which consists of detailed guidance on cybersecurity protections.[21] Regulations have also been issued in accordance with the GLBA. These regulations set uniform requirements for the entities regulated by the SEC, FDIC, Fed, OCC, and other agencies with respect to the development and maintenance of a comprehensive information security program. At the international level, G-7 nations developed and released a set of voluntary guidelines for the financial sector. And just last month, the OCC, Fed, and FDIC proposed enhanced cybersecurity requirements for large financial institutions and other firms.[22]

DFS's Proposal introduces standards and requirements that are already covered by these aforementioned requirements. Representative examples include:

- Comprehensive Cybersecurity Program and Policy Documents: The Proposal would require implementation of a comprehensive cybersecurity program and implementation of multiple policy documents, but the GLBA and implementing regulations already require financial institutions to implement a comprehensive information security program that addresses administrative, technical, and physical safeguards. Through the implementation of this flexible standard, firms have developed different administrative controls to satisfy cybersecurity objectives. We note that the rule proposed by the OCC, Fed, and FDIC also would require the development of a comprehensive cybersecurity strategy. Any misalignment between the DFS rule, the existing GLBA requirements, and the proposed new federal requirement would result in additional work streams to develop overall program and strategy documents simply to satisfy different regulatory requirements.

- Administrative Controls: The Proposal would require the establishment of a Chief Information Security Officer and other roles with specific cybersecurity responsibilities, but federal regulations adopt a more flexible standard that financial institutions shall assign "specific responsibility" for the implementation of a firm's information security program to one or more roles.[23] And federal agencies have provided guidance that preserves the flexibility of financial firms to address cybersecurity administrative needs without imposing unnecessarily rigid requirements.[24]

- Specific Technical Directives and Protective Measures: The Proposal would require that financial firms adopt rigid and impractical encryption measures, multi-factor authentication, penetration testing, audit controls, and other specific technical measures. Decisions regarding what measures to adopt for which firms and on what systems and how to test standards and controls are best left to the decision-making authority of individual firms based on risk assessments. The standards that exist already require firms

to "[p]rotect against unauthorized access to or use of customer records or information,"[25] implement "[i]dentification and authentication" controls "for access to systems, applications, and hardware,"[26] and conduct "[r]egular reviews and testing, as applicable . . . to identify vulnerabilities pertaining to internal and external threats, physical hazards, and natural or manmade disasters."[27] These standards preserve the flexibility of firms to adopt technical measures where they are most needed and do not prescribe a singular and possibly ill-fitted response by firms to cybersecurity threats.

The recommendations and suggestions we offer in this letter seek to build on firms' compliance with existing requirements. By modifying any final rule to align with existing requirements, DFS will promote efficiency while simultaneously improving cybersecurity protections.

B. Any Rule Resulting From The Proposal Should Embody A Risk-Based Approach.

Financial firms with sophisticated and well-developed cybersecurity programs have based their protections on a risk-based approach consistent with federal requirements and prevailing industry standards. We urge DFS to revise any final rules to adopt the same risk-based framework. This approach builds on the NIST Cybersecurity Framework, the International Organization for Standardization's ("ISO") risk-based standards, and existing federal requirements, all of which offer flexibility. Indeed, we are not aware of any authoritative guidance on cybersecurity that is not risk based and technology agnostic.

Federal requirements—including, most significantly, the Interagency Guidelines issued by FDIC, Fed, NCUA, and OCC pursuant to the GLBA—adopt a risk-based approach. They require firms to (1) identify "reasonably foreseeable internal and external threats"; (2) "[a]ssess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information"; and (3) assess the "sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks."[28] Technical controls and other security measures must be implemented to "control identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the institution's activities."[29] The requirements, in other words, are flexible and adaptable based on an assessment of the level of risk and permit firms to target resources and controls based on their size and complexity, customers and counterparties, market interconnectedness, and the sensitivity of the information.

The NIST Cybersecurity Framework also expressly adopts a risk-based approach. It focuses on "the likelihood that an event will occur and the resulting impact."[30] By taking this information into account, "organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures" and develop methods to handle the unique risks faced by different firms by "mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services."[31] Similarly, the ISO has developed risk-based standards.[32]

While the Introduction to the Proposal expresses an intent to adopt a risk-based approach, the Proposal appears to impose inflexible, one-size-fits all requirements.[33] Though the Proposal

makes references to the notion of materiality in some of its definitions and requirements, materiality does not take into consideration the likelihood and severity of the applicable risk. Further, the notion of materiality is not incorporated throughout the requirements, most of which appear to apply inflexible requirements on an across-the-board basis, regardless of feasibility, unintended consequences, or emerging new technologies or methods that may provide better protection.

For example, the Proposal would require data mapping of all Nonpublic Information even where this is not the best method of achieving awareness of the location of sensitive information (Section 500.02); annual penetration testing for nearly all technologies used by a firm, including low-risk systems (Section 500.05); maintenance of audit trails for nearly every financial transaction (Section 500.06); a risk assessment that covers nearly all technologies used by a firm (Section 500.09); annual auditing of all third party vendors, including low-risk vendors (Section 500.11); multi-factor authentication for any systems that store nearly all data maintained by firms (Section 500.12); encryption of all nonpublic data that is linked or linkable to a person or otherwise constitutes Nonpublic Information (Section 500.15); documentation of any act or "attempt" that is successful "or unsuccessful" to gain unauthorized access or otherwise constitutes a Cybersecurity Event (Section 500.16); notification to DFS of any Cybersecurity Event that has a reasonable likelihood of affecting the "normal operations" of a firm or "affects" Nonpublic Information (Section 500.17); and other obligations.

While the Proposal requires a risk assessment in Section 500.09, the results of this risk assessment (as currently drafted) do not relate to how the other required controls are applied. These requirements—if not made explicitly risk-based—would undermine the ability of cybersecurity personnel to prioritize sensitive or vulnerable information systems and significant threats and would force firms to reallocate limited resources to fulfilling regulatory obligations and away from targeting high-priority cybersecurity issues. Any final rule should not require firms to implement specific technology methods that may be superseded or may be infeasible, especially where there are equally secure compensating controls.

We encourage DFS to modify the Proposal to expressly authorize companies to comply with the regulations using a risk-based approach that involves:

1) carrying out a risk assessment (including, as applicable, an assessment of an Information System pursuant to § 500.09), for the purpose of identifying relevant risks and categorizing such risks by severity and probability,

2) implementing the applicable measures or other superseding or compensating controls, as appropriate in accordance with the level of risk, and

3) maintaining supportive documentation of steps (1) and (2) that can be provided to DFS on request to demonstrate that appropriate controls have been deployed.

By making this change, DFS will allow firms with established cybersecurity programs to leverage and strategically improve existing programs to increase protections against emerging risks and incorporate newer and better technologies and methods as they emerge. This risk-based approach would allow for strategic prioritization and revision of controls to respond to

technological developments and evolving threats. Specifically, we request that any final rule require penetration testing, audit trails, multi-factor authentication, encryption, documentation of cyber events, reporting to DFS, and other obligations only in accordance with a risk assessment that considers (1) the likelihood that an event will occur, (2) the resulting impact of such an event, and (3) the adoption of compensating measures to combat such risk. By adopting a risk-based approach, DFS would highlight areas it believes deserve more attention, while at the same time aligning its requirements with prevailing industry standards and firm practices.

There is good regulatory precedent for adopting a risk-based approach. Indeed, DFS's own transaction monitoring rule adopts risk-based regulations.[34] We encourage DFS to modify these requirements by adopting a risk-based approach in harmony with NIST's Cybersecurity Framework, ISO standards, and the Interagency Guidelines.

C. Any Rule Resulting From The Proposal Should Be Revised In Light Of Implementation Impracticalities And Unintended Consequences.

In this section, we more specifically address the proposed requirements and respectfully offer detailed comments to improve their functionality. Some of the more impractical consequences of the proposed requirements, as presently drafted, relate to encryption requirements that will slow down information retrieval and inhibit the operations of firms; multi-factor authentication requirements that will not improve cybersecurity protections and will inhibit firm operations; assessment methods such as penetration testing and vulnerability assessments that may grow obsolete and are not targeted to high-risk vulnerabilities; data deletion requirements that apply to comingled data and that—without significant resources, changes, and new technologies—cannot be implemented; notification requirements to DFS of millions of incidents across financial firms for every event that may affect personal information; third-party monitoring requirements that broadly apply to nearly every vendor and service provider and do not target higher-risk entities; and other requirements that if implemented as currently drafted would have detrimental effects on the provision of services to consumers. By modifying these requirements to incorporate a risk-based approach, we believe any final rule would be greatly strengthened.

1. Scope of the Proposal

We suggest that any final rule would benefit from definitions that narrowed the scope of application of the substantive requirements. The definitions of "Nonpublic Information," "Information System," and "Cybersecurity Event" are so broad that they cover nearly all information maintained by a firm, any firm information system, and any event, successful or unsuccessful, that may involve an attempt to access information without authorization. We believe that the definition of Nonpublic Information should be narrowed and made consistent with New York State law to only concern personal information that is sensitive,[35] and we suggest modifications to the definitions of Information System and Cybersecurity Event that will narrow the scope to data, technology, and events that legitimately may affect a firm's operations and the protection of important information. Accordingly, we recommend that DFS adopt the following definitions:

- "Nonpublic Information" means all electronic information that is not Publicly Available Information and is: (1) Any business-related information of a Covered Entity, the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity; or (2) Any information that can reasonably be used to misappropriate an individual's identity or access an individual's financial account without authorization, including, at a minimum, (i) social security numbers, (ii) driver's license numbers or non-driver identification card numbers or (iii) account numbers, credit or debit card numbers in combination with any security codes, access codes or passwords that would permit access to an individual's financial account.

- "Information System" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information.

- "Cybersecurity Event" means any successful attempt to materially compromise the security, confidentiality, integrity, or availability of an Information System or Nonpublic Information stored on such Information System.

To avoid an overly broad application of the requirements that follow, we suggest that these definitions be more narrowly targeted.

We also suggest that the Proposal narrow the definition of a Covered Entity. The Proposal would apply requirements to all Covered Entities, defined to include DFS-registered and -licensed entities. (Section 500.01(c)). Some DFS-registered and -licensed entities, however, do not maintain any "Information Systems" and do not possess any "Nonpublic Information," as those terms are defined in the Proposal. In some instances, entities become licensed in New York for the limited purpose of complying with requirements under the insurance laws and related regulations requiring licensure for insurance producers as a condition of receiving commission payments. Other firms may only open a sales office in New York State that must be registered pursuant to DFS requirements. But if these entities do not actually maintain information systems and personal data or other information, then any final rule resulting from the Proposal, we suggest, should not apply. Accordingly, we suggest that DFS revise the definition of "Covered Entity" to exclude entities that do not operate or maintain an Information System and that do not generate, receive, or possess Nonpublic Information.

2. Administrative Controls

The Proposal would require designation of a Chief Information Security Officer ("CISO") (Section 500.04) and employment of cybersecurity personnel (Section 500.10). We recommend that any final rule accommodate other titles that might already exist within a firm that fulfill the same functions as a CISO but may not have this title. Firms should not be forced to rename job titles to comply with the rule. Further, the rule should be flexible with respect to organizational structure to accommodate firms that have information systems governed by the CISO of an affiliate and subsidiary (or an employee operating in a CISO-like capacity).

Additionally, the Proposal includes a reporting requirement that may require firms to create an entirely new DFS-reporting team (Section 500.04(b)). We think it more efficient for these requirements to mirror and tie to firms' regular audit programs. The report should be elevated at the discretion of the firm in accordance with the degree of risk presented and decision-making factors adopted by firms' internal operating procedures.

Section 500.10 is unclear in various respects. We recommend that DFS issue guidance clarifying what is meant by "sufficient" personnel. Section 500.10(a)(2) requires training, but does not specify certification requirements (*e.g.*, CISSP, CISM). Section 500.10(a)(3) does not define "key cyber personnel." Without further clarification, firms will not be able to determine whether they are compliant with the rule. Accordingly, we recommend that any final rule permit firms to exercise flexibility in their organizational structure and with respect to staffing personnel focused on cybersecurity issues.

3. Cybersecurity Program Requirements

The Proposal would require firms to establish and maintain a cybersecurity program designed to perform core cybersecurity functions and to create and maintain various policies and practices. We recommend revising these requirements in accordance with the comments below to incorporate a risk-based approach and eliminate inefficiencies.

a. *Scope of the Program Requirements*

As drafted, Section 500.02 imposes a data mapping requirement for "Nonpublic Information stored on the Covered Entity's Information Systems." Because this requirement could be interpreted to cover every technology used by a firm and include "any information that is linked or linkable to an individual," the implementation of a such a widespread data mapping requirement may not be practicable and could unduly consume resources needed to target areas of higher risk. Further, different firms design their information architecture differently and utilize different methods of controlling access and protections for protected information that do not involve a comprehensive mapping of all information stored on all systems. Accordingly, we suggest that this requirement be revised to permit firms to devote heightened attention to nonpublic data and information systems that present greater risks. Further, we recommend that Section 500.02 be revised to clarify that firms need not create and maintain a unique "cybersecurity program" if the core cybersecurity functions in question are already addressed by existing programs and policies.

b. *Written Policies*

Similarly, Sections 500.03 and 500.16 require firms to implement and maintain a written cybersecurity policy and an incident response plan, detailing the elements that such policies must cover and how they should be reviewed and approved. As with our above recommendations, we recommend that the review or approval of these policy documents be conducted pursuant to a risk-based approach as determined by the internal controls appropriate to each business. We also suggest that DFS clarify—in guidance or in the regulations—that firms need not develop separate policy documents and that general policies that cover multiple business lines are sufficient. For example, a parent corporation not registered with DFS may have a policy that

fully complies with DFS's requirements and comprehensively governs all subsidiaries, some of which may be registered with DFS. Such a policy should be deemed to satisfy DFS's requirements.

c. *Penetration Testing*

Section 500.05 requires the cybersecurity program to include annual penetration testing and quarterly vulnerability assessments. We recommend that these requirements be converted to risk-based requirements as determined by the firm's assessment of risks and vulnerabilities. As drafted, the Proposal may require firms to conduct penetration testing and vulnerability assessments for nearly every piece of technology operated by a firm. Such requirements would be prohibitively expensive, difficult to administer, and counterproductive to the protection of sensitive information.

We agree that an effective testing framework is important. However, we suggest that DFS promote a firm's ability to determine penetration testing and vulnerability assessments on an as-needed basis and in accordance with its primary regulator's guidance. The level of testing and assessment necessary to achieve these objectives should be permitted to vary based on each firm's unique risk profile. For this reason, we encourage DFS to revise any final rule to incorporate such a risk-based approach and to clarify its expectations through guidance.

d. *Audit Trails*

We recommend that Section 500.06's requirements to maintain audit trails be revised to clarify that audit trails should be maintained in accordance with a firm's risk assessments. Section 500.06(1) requires an audit trail for "all financial transactions." The term "financial transaction," however, is not defined and could apply to every single transaction processed by a firm. Further, the Proposal would require that firms maintain such data for a minimum period of six years. The across-the-board six-year data retention period represents an exponential increase in data retention periods for some data, with a significant implementation burden and no material improvement to cybersecurity. And it would require costly modifications to firms' legacy systems, which are not designed to record information relating to every financial transaction. We suggest that any final rule only require preservation of data that firms decide need to be maintained in order to fulfill auditing needs. The objective of such auditing requirements should be limited to a defined set of critical Information Systems, as determined under a firm's risk assessment criteria.

e. *Risk Assessments*

Section 500.09 requires firms to conduct detailed annual risk assessments of all systems. This requirement is overly broad and should be revised to be consistent with a firm's risk profile. The frequency of risk assessments should be risk-based and conducted based on criticality and on an as-needed basis.[36] Further, as noted above, different firms design their information architecture differently and utilize different methods of controlling access and protections for sensitive information that do not necessitate comprehensive assessment of risk on all information systems. We suggest that DFS draft any final rule to make clear that a parent or affiliate entity's risk assessment may satisfy the DFS-registered entity's obligation under this section and that

such risk assessments must be conducted in accordance with the firm's assessment of vulnerability and the type of data maintained on such systems.

f. *Third-Party Oversight*

Section 500.11 imposes requirements with respect to third-party vendors that require assessments on an annual basis. We suggest that these requirements be revised to focus on a risk-based approach to avoid the potentially onerous requirement that *all* third parties servicing a firm would be within scope. Not every third party that performs services for a firm poses a risk or the same degree of risk. If assessments are required for nearly every third party, it would divert important resources and deplete the ability of firms to focus their efforts on reducing more significant vulnerabilities. Accordingly, we recommend that any final rule require such assessments be based on such important factors as the type of information processed, the criticality of the vendor to the firm's operations, and compensating controls that manage the risk exposure associated with a third party.

It is important to note that the Proposal's requirement that entities obtain representations and warranties that the service or product provided is free of viruses, botnets and other vulnerabilities is in conflict with many third-party engagements where firms face liability waivers with respect to these issues. For many smaller entities, the requirement that contractual language be revised to include these terms and audit rights may not be possible when negotiating with larger third parties and may force such entities to use less reputable vendors. Further, some third parties force firms to disclaim liabilities. For example, many third parties that engage in penetration testing force firms to disclaim liabilities associated with such tests. Given that there are a limited supply of third parties that engage in such activities, this will further deplete the availability of such services. Accordingly, we recommend that these contractual requirements be struck from any final rule and, if they remain, that firms be required to implement these requirements to the extent reasonably possible, taking into account the risk profile of the firm, the risks posed by third parties, and compensating controls to manage risk.

Further, as we detail below, the requirement to encrypt data in transit and at rest is not practicable. Global encryption of data also may increase the operational risks of financial firms due to the significantly increased risk of data corruption and encryption key management. In addition, requiring all vendors to do so would constitute a massive undertaking and would be impractical to administer. Requiring encryption of nearly all data at third-party vendors would cause material data processing delays. These requirements should instead be risk-based.

g. *Data Retention*

Section 500.13 imposes data retention requirements that do not meet current business practice and data destruction requirements. Information preservation requirements should be governed by the records retention policies of the business, which set forth the retention period for various categories of data. Firms need to retain data beyond what is "necessary for the provision of the products or services for which such information was provided to the Covered Entity."[37] The scope of such retention is the subject of firms' record retention policies. Requiring targeted disposal will be technically infeasible in many circumstances due to the manner in which

information is maintained within individual systems, particularly legacy systems and those where data is commingled. Data stored on magnetic data tapes and commingled data on servers present significant feasibility challenges with respect to any requirement for targeted data destruction. Accordingly, we ask that this requirement be revised to recognize that firms may retain data pursuant to the records retention policy of the business or where targeted disposal is not reasonably feasible due to the manner in which this information is maintained within individual systems, including legacy systems and those where data is commingled.

h. *Training*

Section 500.14 imposes training requirements relating to cybersecurity. The term "regular cybersecurity awareness training" and the scope of the training, however, are not clearly outlined. Detailed cyber training is not necessary for all personnel who do not have access to Nonpublic Information or Information Systems. Accordingly, we recommend that training should be conducted based on a firm's risk profile and a firm's assessment of personnel determined to require such training and the degree to which such training should be provided.

4. Incident Reporting Requirements

Section 500.17 provides for information security reporting and notice requirements. To fulfill this requirement, a firm would have to report unsuccessful attacks, of which there may be millions daily. For example, the rule as written requires notification for "any Cybersecurity Event involving the . . . potential unauthorized . . . access to . . . Nonpublic Information." The definition of "Cybersecurity Event" includes an unsuccessful attempt to gain unauthorized access to an Information System. Thus, under the Proposal, notification would be required for any unsuccessful attempt to gain unauthorized access to an Information System if that Information System contains Nonpublic Information.

To prevent such over-reporting to DFS, we request that any final rule require notification only where there is a substantial risk of material harm, rather than all events involving nonpublic information or every event that may "affect the operation" of a firm. The final rule should be modified by adopting the proposed definition of Cybersecurity Event and requiring notification only where there is a substantial risk of material harm. Revising the rule in this manner would align with existing data breach notification requirements within 47 states, including New York, and with the federal Interagency Guidelines, which provide that in the event of unauthorized access or use of sensitive customer information, firms must notify the firm's primary regulator, law enforcement, and (when warranted) customers.[38]

Further, we recommend that the requirement to notify DFS within 72 hours be revised to align with existing federal and state requirements. No state or federal agency requires notification within such a short period of time. It often takes days to investigate incidents while receiving real-time information and attempting to stop the attack. Imposing a requirement to provide notice to DFS in the middle of a response would hamper a firm's ability to devote skilled resources to protecting its technology, customer information, and resources and could require firms to provide notice based on unconfirmed information regarding the scope and nature of the incident. Accordingly, we recommend that any final rule align with the existing New York State

requirement that notification be provided in the "most expedient time possible and without unreasonable delay."[39]

We also request that DFS incorporate a delay provision for law enforcement. In the aftermath of an event, firms often must coordinate with law enforcement, which may request that the event not be disclosed to third parties. Many state laws, including New York's, permit delay in such instances.[40] We request that DFS ensure its rule does the same.

DFS should also consider that reporting requirements may create additional risk and liability. Of particular concern is the method by which the sensitive reports produced pursuant to this section will be collected and protected. The information required to be produced includes, among other things, the results of each Covered Entity's penetration testing. Accordingly, any final rule should clarify whether information must be provided in encrypted form, whether it will be stored in encrypted form, and the manner in which DFS will provide access to and use of the reported information.

5. Technical Requirements

The Proposal would mandate specific testing and technical requirements, including access privileges (Section 500.07), application security (Section 500.08), multi-factor authentication (Section 500.12), and encryption of nonpublic information (Section 500.15). We agree that the subject areas these provisions address are critical to an effective and robust cybersecurity program. As we stress in the prior section, however, we request that any final rule clearly recognize each entity's unique risk profile and clarify that any corresponding obligations should be proportional to the entity's independent risk assessment.

a. *Access Requirements*

Section 500.07 regulates access privileges. This section appears to require role-based access, but the text requires clarification as to which system should be monitored based on a given risk profile. Further, while need-to-know access is a reasonable requirement, this provision incorporates the overly broad terms "Information Systems" and "Nonpublic Information," and could conceivably require firms to limit access privileges to every system, no matter its use or particular risk profile. We request that this section be amended to make clear that access privileges must be limited based on a risk assessment.

b. *Application Security*

Section 500.08 imposes requirements relating to the use of applications and assessment of their risk. As written, the requirements appear overly broad. Annual security testing of all applications, for example, may not be necessary and, instead, should be based on a risk assessment of the business. Any final rule should clarify that the required "secure development practices" need not be uniform across all applications but rather that firms should prioritize critical applications. Further, as noted above, different firms design their information architecture differently and utilize different methods of controlling security that do not involve an assessment of the security for all applications but instead focus on categories of information and how they are treated within a firm. Accordingly, any final rule should enable firms to assess risk in the manner most appropriate to its risk profile and information architecture.

c. *Multi-Factor Authentication*

Section 500.12 sets out requirements relating to the use of multi-factor authentication. As drafted, this section would require use of multi-factor authentication with respect to virtually every information system and access to virtually all data stored by financial firms. Requiring multi-factor authentication to this extent would be onerous and may ultimately be self-defeating, likely resulting in the creation of *ad hoc* workarounds and noncompliance. Further, it may delay the ability to fulfill customer needs in the delivery of contracted services. We recommend that any final rule only require the use of multi-factor authentication based on a risk-based assessment by financial firms with respect to the types of information at issue, potential threats faced, and compensating controls. Firms should be able to apply different approaches that are consistent with their risk and to adopt new technologies and methodologies as they are developed.

d. *Encryption*

Section 500.15 imposes encryption requirements for all Nonpublic Information held or transmitted by the firm both in transit and at rest. This requirement does not consider the serious practical obstacles to encryption and that data is generally stored and transmitted in various capacities with varying degrees of risk. In many circumstances, the requirement would simply be unworkable. Implementation of this requirement for mainframe systems, commingled archives, legacy archives, and backup systems would require enormous resources and personnel time, not to mention technical expertise to keep systems running. Even if encryption could be implemented to the extent required, there would be enormous delays in data processing, and firms would be unable to satisfy timely requests for information. Further, requiring firms to encrypt all data thwarts firms' agile adoption of new technologies that supersede encryption in terms of ability to protect systems and data. For example, some firms are investigating the use of tokenization as a method that may be better than encryption at protecting sensitive data. If firms invest heavily in encrypting all data, it would preclude them from moving to newer and better technologies as they are developed. The requirement to encrypt nearly all data at rest or in transit also may weaken other security controls by (a) blocking surveillance of such data to detect intruders and (b) requiring the broad distribution of encryption keys to allow applications to access such data, increasing vulnerability points through which the information could be hacked. Accordingly, we recommend that any final rule only require encryption based on a risk-based analysis to the extent technically feasible and in light of compensating controls, including but not limited to access controls, network segmentation, and physical controls.

6. Effective Date and Transition Period

For the reasons stated herein, it would be impractical to comply with an effective date of January 1, 2017, given the short transitional period (*see* Sections 500.20, 500.21). Even with the suggested modifications, many of the necessary changes will take over a year or multiple years to implement. Many of these changes will have to be made with significant advance notice to customers and staff and will be limited to select maintenance and upgrade windows to ensure firms are able to successfully implement these changes while continuing operations and meeting customers' needs. Even with the suggested modifications, the implementation schedule does not permit sufficient time to complete financial and operational planning processes for new technical

implementations and to transition all systems and negotiate changes with third-party service contracts. Accordingly, we recommend that the effective date be extended to January 1, 2018; that the transition period should be extended to 365 days beyond the effective date; and that compensating controls for encryption should remain available in perpetuity.

7. Certification Requirement

The Proposal's certification requirement is an unprecedented new government cybersecurity requirement that is also highly impractical—especially to the extent it requires firms to certify complete compliance. Section 500.17 requires each Covered Entity to annually submit to the Superintendent the certification form. Exhibit A includes a provision, to be signed by the "Chairperson of the Board of Directors or Senior Officer(s)," that to the best of their knowledge the Covered Entity's cybersecurity program complies with the final approved DFS cybersecurity requirements. The language of Exhibit A does not recognize that cybersecurity is an iterative process, and it leaves no room for instances where complete compliance has not been achieved but remediation plans have been duly put in place.

This absolute compliance certification requirement does not align with the Proposal's recognition that a firm may need to identify areas, systems, or processes that require material improvement. Section 500.17(b)(1) instructs a firm to document remedial efforts planned and underway to address any such areas, systems, or processes and to make such documentation available for inspection by the superintendent. Exhibit A, by contrast, requires certification of compliance with no apparent mechanism to note areas that may not be in complete compliance at the time of certification but that have been identified for remediation.

Such a certification could result in criminal liability if the controls are found lacking. Firms should not be required to operate under such heightened standards and onerous penalties for noncompliance, especially in an environment that is inherently uncertain and fraught with unknown risks. In this regard, cybersecurity is fundamentally unlike other areas of regulatory compliance, given that there are always degrees of uncertainty and risk no matter how robust a firm's information security protections.

If the language remains as stated in the proposed regulations, we believe that it could lead to a paper exercise of downstream certifications to protect senior officers from liability, with a focus on checking the box rather than on addressing cyber risk. To avoid this outcome, we suggest eliminating the certification requirement. To the extent that DFS deems it essential, we suggest modifying the language of Exhibit A to certify that the entity "has in place processes to establish, maintain, enforce, review, test and modify the compliance program to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Part __." This revision would align the certification with the goals of the proposed regulations, incorporate a risk-based approach, and avoid conflict with other portions of the Proposal and the inability to certify complete compliance.

* * *

We welcome further engagement and discussion with DFS about the comments in this letter. We look forward to working with DFS on the creation of cybersecurity protections that

complement existing requirements and standards to facilitate effective management of cybersecurity risk. If you have any questions or require further information, please do not hesitate to contact Thomas Wagner at 212-313-1161 or twagner@sifma.org.

Sincerely,

/s/ Rich Baich
Rich Baich
Chair
FSSCC

/s/ Thomas M. Wagner
Thomas M. Wagner
Managing Director
SIFMA

/s/ Michael Fratantoni
Michael Fratantoni
Chief Economist and Senior Vice President
MBA

/s/ Doug Johnson
Doug Johnson
Senior Vice President
ABA

/s/ Danielle Fagre Arlowe
Danielle Fagre Arlowe
Senior Vice President
AFSA

/s/ Chris Feeney
Chris Feeney
President
FSR/BITS

/s/ Justin Ailes
Justin Ailes
Vice President, Government & Regulatory Affairs
NYMBA

/s/ Marianne Collins
Marianne Collins
Executive Director and COO
ALTA

cc: Alan Charles Raul, Sidley Austin LLP
Clayton G. Northouse, Sidley Austin LLP

[1] SIFMA brings together the shared interests of hundreds of securities firms, banks, and asset managers. SIFMA's mission is to support a strong financial industry, investor opportunity, capital formation, job creation, and economic growth, while building trust and confidence in the financial markets. 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* PwC, "Global State of Information Security Survey 2016 (Oct. 9, 2015), http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.

[3] *See* Executive Order – Improving Critical Infrastructure Cybersecurity, E.O. 13636 (Feb. 12, 2013).

[4] Firms have already made significant advances to implement NIST and CAT and comply with existing federal standards since DFS conducted its study in 2014.

[5] While DFS recognizes "duplication" and that there is some "overlap" with the requirements of GLBA, the Proposal does not take into full consideration extent to which its regulations overlap with GLBA and other existing federal requirements nor does it consider the impact of such overlap and duplication. Specifically, DFS does not consider the fact that the Proposal does not incorporate a risk-based approach, whereas existing cybersecurity requirements do incorporate a risk-based approach. DFS, *Proposed Rule Making: Cybersecurity Requirements for Financial Services*, I.D. No. DFS-39-16-00008-P, NYS Register at 68 (Sept. 28, 2016).

[6] Enforcing Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.*; Commodities Exchange Act, 7 U.S.C. § 7b–2; CFTC Safeguards Rule, 17 C.F.R. § 160.30; Risk Management Program Rule, 17 C.F.R. §23.600; CFTC Staff Advisory No. 14-21, Best Practices Memo; DCO Cybersecurity Rule, 80 Fed. Reg. 80114-01; System Safeguards Rule, 80 Fed. Reg. 80140-01.

[7] Enforcing Securities Act of 1933, 15 U.S.C. § 77a *et seq.*; Securities Exchange Act of 1934, 15 U.S.C. § 78a *et seq.*; Sarbanes-Oxley Act, Pub. L. No. 107-2014, 116 Stat. 745; Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.*; Regulation S-P, 17 C.F.R. § 248.30; Regulation SCI, 17 C.F.R. §§ 242.1000–1007; OCIE's 2015 Cybersecurity Examination Initiative (Sept. 15, 2015); OCIE's Cybersecurity Examination Sweep Summary (Feb. 3, 2015); OCIE's Cybersecurity Initiative (Apr. 15, 2014).

[8] Enforcing Federal Deposit Insurance Act and Federal Deposit Insurance Corporation Improvement Act, codified at 12 U.S.C. §§ 1811–1835a; Bank Service Company Act, 12 U.S.C. § 1861 *et seq.*; Interagency Guidelines, 12 C.F.R. pt. 364, App. B; Cybersecurity Awareness Resources (including Cyber Challenge Announcement), FIL-55-2015; Technology Outsourcing: Informational Tools for Community Bankers, FIL-13-2014; Clarifying Supervisory Approach to Institutions Establishing Account Relationships with Third-Party Payment Processors, FIL-41-2014; Pre-Employment Background Screening Guidance on Developing an Effective Pre-Employment Background Screening Process, FIL-46-2005; Final Guidance on Response Programs Guidance on Response Programs for Unauthorized Access to Customer Information and Customer, FIL-27-2005; Supervisory Policy on Identity Theft, FIL-32-2007.

[9] Enforcing Federal Reserve Act, 12 U.S.C. § 248(a); Bank Holding Act of 1956, 12 U.S.C. § 1844(c); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809; *Bank Holding Company Supervision Manual* § 2124; *Commercial Bank Examination Manual* §4060.

[10] Enforcing Federal Trade Commission Act, 15 U.S.C. § 45; Gramm-Leach-Bliley, 15 U.S.C. §§ 6801–6809; Safeguards Rule, 16 C.F.R. pt. 314; Identity Theft Rule, 16 C.F.R. pt. 681.

[11] Enforcing Federal Credit Union Act, 12 U.S.C. §§ 1751–1795k; Interagency Guidelines, 12 C.F.R. 748, App. A; Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice (Adoption of the Interagency Guidelines with slight modifications), 12 C.F.R. pt. 748, App. B.

[12] Enforcing Bank Service Company Act, 12 U.S.C. § 1867; Interagency Guidelines, 12 C.F.R. pt. 30, App. B.

[13] Enforcing FINRA Rule 2010; FINRA Rule 3110; FINRA Rule 3120.

[14] Enforcing NFA Compliance Rule 2-9; NFA Compliance Rule 2-36; NFA Compliance Rule 2-49.

[15] Forty-seven states have implemented data breach notification requirements and numerous states have implemented information security requirements.

[16] Remarks of Secretary Jacob J. Lew, Department of the Treasury, at the 2014 Delivering Alpha Conference (July 16, 2014), http://www.treasury.gov/press-center/press-releases/Pages/jl2570.aspx.

[17] Thomas J. Curry, Comptroller of the Currency, *Remarks at BITS Emerging Payments Forum* (June 3, 2015), http://www.occ.treas.gov/news-issuances/speeches/2015/pub-speech-2015-78.pdf ("One of my top priorities as Comptroller . . . has been to address the risks that cyber threats pose to individual banks and the banking

system. This effort necessarily requires extensive and ongoing coordination among regulators and banks, large banks and small banks, regulators and the rest of the Government, and the financial sector and other critical infrastructure.").

[18] Lalita Clozel, *Regulators Must Improve Cybersecurity Coordination: Top Treasury Official*, American Banker (Mar. 17, 2016) (quoting Deputy Treasury Secretary Sarah Bloom Raskin) (emphasis added), http://www.americanbanker.com/news/law-regulation/regulators-must-improve-cybersecurity-coordination-top-treasury-official-1079975-1.html.

[19] Anthony J. Albanese, *Letter to Financial and Banking Information Infrastructure Committee Members Regarding Potential New DFS Cyber Security Regulation Requirements* (Nov. 9, 2015), http://www.dfs.ny.gov/about/letters/pr151109_letter_cyber_security.pdf.

[20] SIFMA Letter to DFS (Jan. 25, 2016).

[21] FFIEC, IT Examination Handbook, http://ithandbook.ffiec.gov/.

[22] Office of the Comptroller of the Currency, Federal Reserve System, Federal Deposit Insurance Corporation, *Announced Notice of Proposed Rulemaking: Enhanced Cyber Risk Management Standards*, (Oct. 19, 2016), https://www.federalreserve.gov/newsevents/press/bcreg/bcreg20161019a1.pdf.

[23] *See, e.g.*, 12 C.F.R. pt. 364, App. B, at III.A.

[24] *See, e.g.*, SEC, *2015 Cybersecurity Initiative*, at 2; *see also* CFTC, Staff Advisory No. 14-21 (stating that firms should "[d]esignate a specific employee with privacy and security management oversight responsibilities, who develops strategic organizational plans for implementing the required controls, is part of or reports directly to senior management or the Board of Directors, and designates employee(s) to coordinate, implement and regularly assess the effectiveness of the program."); *see also* 17 C.F.R. § 242.1001(c) (requiring designation of "responsible SCI personnel").

[25] 17 C.F.R. § 248.30(a)(3); *see also* 16 C.F.R. § 314.3(b)(3).

[26] FFIEC, *Cybersecurity Assessment Tool*, at 36.

[27] 17 C.F.R. § 242.1001(a)(2)(ii).

[28] Interagency Guidelines, 12 C.F.R. pt. 364, App. B, at II.A; *see also* SEC, Regulation SCI, 17 C.F.R. § 242.1001(b)(1); Red Flags Rule, 7 C.F.R. § 162.30(d)(1) (CFTC), 12 C.F.R. § 717.90(d)(1) (NCUA); 16 C.F.R. § 681.1(d)(1) (FTC); 12 C.F.R. § 571.90(d)(1) (FDIC); 12 C.F.R. § 222.90(d)(1) (FRB); 12 C.F.R. § 41.90(d)(1) (OCC). Firms are required to develop a "comprehensive information security program" to address such identified risks "that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities." 12 C.F.R. pt. 364, App. B, at III.B; *see also* SEC, Regulation SCI, 17 C.F.R. § 242.1001(a)(1).

[29] Interagency Guidelines, 12 C.F.R. pt. 364, App. B, at III.C; *see also* SEC, Regulation S-P, 17 C.F.R. § 248.30(b)(2)(i).

[30] NIST, Cybersecurity Framework, at 5.

[31] *Id.*

[32] They are designed "to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture." ISO 31000:2009, https://www.iso.org/obp/ui/.

[33] The Introduction states that each firm is required to "*assess its specific risk profile* and *design a program that addresses its risks in a robust fashion*" and that the standards need not "be overly prescriptive so . . . cybersecurity programs can match . . . relevant risks." (emphasis added).

[34] NY DFS Final Bitlicense Regulatory Framework For Virtual Currency Firms. The regulation incorporates a requirement of risk-based policies, procedures, and practices to ensure compliance with applicable regulations.

[35] N.Y. Gen. Bus. Law § 899-AA(1)(b).

[36] Firms are already required to conduct periodic testing and audits of their cybersecurity controls pursuant to interagency guidelines, which state that "[t]he frequency or nature of such tests should be determined by the institution's risk assessment." 12 C.F.R. pt. 364, App. B, at III.C.3.

[37] For example, a customer application is not "necessary" for the provision of relevant financial services, but is necessary as evidence of authorization.

[38] 12 C.F.R. pt. 364, Supp. A, App. B, at II.A.1(b). New York requires notification for any individual whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. N.Y. Gen Bus. § 899-aa(1)(b).

[39] N.Y. Gen. Bus. Law § 899-AA(2).

[40] N.Y. Gen. Bus. Law § 899-AA(2); Iowa Code § 715C.2(3), (8); La. Rev. Stat. Ann. 51 § 3073(C)-(D) and L.A.C. 16:III.701(B); Md. Code. Ann. Comm. Law. § 14-3504(h); 9 Vt. Stat. Ann. § 2435(b)(3)(B)(i); Wash. Rev. Code § 19.255.010(16).