sifma
Invested in America

FINANCIAL
SERVICES
ROUNDTABLE

American
Bankers
Association

FSSCC
Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

January 27, 2017

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-RP**

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"), and the Financial Services Sector Coordinating Council ("FSSCC") we appreciate the opportunity to comment on the New York State Department of Financial Services ("DFS") revised proposed rulemaking on Cybersecurity Requirements for Financial Services Companies (the "Proposal").[2] We thank DFS for considering our comments, submitted on November 14, 2016 (the "Letter")[3] as well as the comments of other associations and industry stakeholders regarding the initial proposed rule. We once again commend DFS in its efforts to strengthen and improve cybersecurity in the financial sector.

It is evident based on a reading of the Proposal that DFS seriously considered the numerous comments received. We believe the Proposal as revised now better represents a rule which

[1] SIFMA is the voice of the U.S. securities industry, representing the broker-dealers, banks and asset managers whose 889,000 employees provide access to the capital markets, raising over $2.4 trillion for businesses and municipalities in the U.S., serving clients with over $16 trillion in assets and managing more than $62 trillion in assets for individual and institutional clients including mutual funds and retirement plans. 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 "23 NYCRR 500. New York Department of Financial Services Proposed Cybersecurity Requirements For Financial Services Companies." (DFS Proposal) http://www.dfs.ny.gov/about/press/pr1612281.htm

[3] See "SIFMA Response to NY DFS Proposed Cyber Requirements," November 14, 2016. ("SIFMA Letter to DFS"). The SIFMA Letter to DFS was submitted in a joint effort with the American Bankers Association, the Financial Services Roundtable, the Financial Services Sector Coordinating Council, the Mortgage Bankers Association, the American Financial Services Association, the American Land Title Association, and the New York Mortgage Bankers Association.

satisfies DFS' regulatory mandate, and minimizes many of the unintentionally onerous requirements of the initial proposed rule. However, we respectfully request your consideration of the following essential revisions to: (1) application of the Proposal to foreign entities; (2) the Proposal's Risk Assessment requirements; and (3) implementation impracticalities and unintended consequences stemming from the Proposal, including the Proposal's current considerations regarding encryption. Our detailed recommendations follow.

*   *   *

## A. The New York Branch of Foreign Financial Services Companies

### 1. Covered Entity – Section 500.01(c)

Although we appreciate the candor of DFS personnel in adopting our recommendations, it appears that certain institutions, which we believe should not be subject to the remit of the Proposal, remain in scope. Specifically, the Proposal appears to apply to foreign banking organizations with branches located in New York. We do not believe it is the intent of DFS to place foreign institutions in scope. However, this is the effect of a plain reading of the Proposal. A Covered Entity is currently defined as "a Person operating under or required to operate under a license…under the Banking Law, the Insurance Law or the Financial Services Law."[4] Under New York's Banking Law, the foreign institution itself applies for, and operates under a license, not the New York branch of said foreign entity.[5] While the term "branch" was added to the term "Person" (so that "Person" means…any non-governmental entity, including but not limited to any…branch), this does not resolve the issue because, while the branch can be viewed as a "Person" operating under a license, the foreign banking organization (which is also a "Person") is also in scope under a plain reading of the regulation, as is the "Person" required to obtain the license to operate in New York through a branch. Thus, under a plain reading of the Proposal, the foreign home office of an institution is subject to the Proposal, rather than the New York branch only.

The result of such a construction would be that the foreign banking organization would not only be required to satisfy the regulation's requirements with respect to extra-territorial systems that are not used for the New York branch, but DFS would receive Cybersecurity Event notifications regarding Nonpublic Information that are irrelevant to the New York branch as well as annual certifications from the Foreign Banking Organization itself regarding systems beyond the scope of the New York branch.  We believe DFS intended the Proposal to apply solely to the New York branch in this circumstance, similar to DFS' intention with respect to the DFS' Banking Transaction Monitoring Rule, where the definition of "Bank Regulated Institutions" makes clear that the foreign banking organization is out of scope.

[4] *Id* at 2.

[5] *See* New York Banking Law Article V-B. License for a Foreign Banking Corporation to Maintain a Representative.

To resolve this issue, we propose that DFS revise the definition of the term Covered Entity, and add a new definition to the Proposal titled "Banking Law Regulated Entity,"[6] mapped to the definitions of "Bank Regulated Institutions" and "Nonbank Regulated Institutions" in DFS' Banking Transaction Monitoring Rule, and expanded to include non-bank entities which DFS desires to remain in-scope. We stress however that foreign institutions themselves should remain firmly outside of any final rules. We propose that Section 500.01 of the Proposal be revised as follows:

> **500.01(c)** *Banking Law Regulated Entities* means (a) all banks, trust companies, private bankers, savings banks, and savings and loan associations chartered pursuant to the Banking Law and all branches, and agencies of foreign banking corporations licensed pursuant to the Banking Law to conduct banking operations in New York; and (b) all check cashers, and money transmitters, [budget planners, licensed lenders, premium finance agencies, sales finance agencies, and mortgage companies] licensed pursuant to the Banking Law.
>
> **500.01(d)~~(c)~~** *Covered Entity* means any (a) Banking Law Regulated Entity; or (b) Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the ~~Banking Law,~~ Insurance Law or the Financial Services Law.

In addition to the changes outlined above, we strongly urge DFS to create explicit language ensuring that representative offices of foreign banking institutions shall not be subject to this Part. We do not believe DFS intended such institutions to be in scope, and we ask DFS to explicitly revise the Proposal accordingly. In addition, DFS should create clear citations in any final rule to the New York Banking Law, Insurance Law, and Financial Services Law, including website URL links to an official New York State webpage, to ensure entities are easily able to discern which portions of their enterprise are covered. Revising the definition of Covered Entity in the above manner, while adding the definition of Banking Law Regulated Entity from DFS' Transaction Monitoring Rule will have the effect of definitively stating that the New York branches of foreign institutions are subject to the Proposal, rather than foreign institutions at an enterprise-level, while mapping to existing DFS regulations. However, such a change still does not solve the issue of requiring New York entities to adopt cybersecurity programs and policies separate and distinct from their Affiliates. To remedy this disparity, we urge DFS additionally to alter Section 500.02(c) as outlined below.

### 2. Cybersecurity Program – Section 500.02

Section 500.02(c) of the Proposal states that a Covered Entity may meet the Proposal's requirements by "adopting a cybersecurity program maintained by an Affiliate, provided that the

[6] Under DFS' Transaction Monitoring Rule, "Bank Regulated Institutions" means "*all banks, trust companies, private bankers, savings banks, and savings and loan associations chartered pursuant to the New York Banking Law (the "Banking Law") and all branches and agencies of foreign banking corporations licensed pursuant to the Banking Law to conduct operations in New York*." "Nonbank Regulated Institutions" means "*all check cashers and money transmitters licensed pursuant to the Banking Law*." *See* "Department of Financial Services Superintendent's Regulations Part 504: Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications."

Affiliate's cybersecurity program covers the Covered Entity's Information Systems and Nonpublic Information and meets the requirements of this Part."[7] Permitting New York entities to adopt the cybersecurity programs of Affiliates is crucial to the success of enterprise-wide operations, as maintaining a rule that requires duplication of effort on this scale exacerbates cyber risks, rather than minimizing them, as it diverts resources that could have been focused on true cybersecurity risks into performing unnecessary "check the box" exercises, simply to comply with the regulation. We accordingly propose that Section 500.02 be revised to ensure that entities in New York are able to adopt an Affiliate's cybersecurity program, in whole or in part, and that, in such cases, the adopted portion(s) of the Affiliate's program only need to comply with the Proposal to the extent applicable to the Covered Entity's Nonpublic Information or Information Systems (as opposed to in the program's entirety). If this revision is not made, this Part will create unnecessary, and we believe unintended extraterritorial application of the final rules. We therefore urge DFS to revise Section 500.02 as follows:

**Section 500.02 Cybersecurity Program**

(a) Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of the Covered Entity's Information Systems.

(b) The cybersecurity program shall be ~~based on the Covered Entity's Risk Assessment and~~ designed to perform the following core cybersecurity functions as appropriate to the applicable risks identified pursuant to the Covered Entity's Risk Assessments.

(1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems;

(2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;

(3) detect Cybersecurity Events;

(4) respond to identified or detected Cybersecurity Events to mitigate any negative effects;

(5) recover from Cybersecurity Events and restore normal operations and services; and

(6) fulfill applicable regulatory reporting obligations.

(c) A Covered Entity may meet any of the requirements of this Part by adopting, in whole or in part, a cybersecurity program maintained by an Affiliate, provided that ~~the~~ any adopted Affiliate's cybersecurity program (or part thereof) cover~~s~~ the Covered Entity's Information Systems and Nonpublic Information and, to the extent an adopted portion applies to the Covered Entity's Information Systems and Nonpublic Information, meets the requirements of this Part in question.

(d) Policies, processes and other written material that ~~All~~ document~~ation~~ the required aspects of the Cybersecurity Program to be maintained pursuant to this Part ~~and information relevant to the Covered Entity's cybersecurity program~~ shall be made available to the superintendent upon request.

[7] DFS Proposal, at 4.

Section 500.02(b) as currently drafted in the Proposal does not provide sufficient flexibility for entities to focus their cybersecurity efforts using a risk-based approach. Section 500.02(d) should be narrowed to apply solely to the documentation and information required to be maintained pursuant to this Part, rather than "any" information relevant to the program. We believe these suggested revisions will ensure the cybersecurity needs of Covered Entities are met, while meeting DFS' regulatory goals.

### B. Clarify That a Risk Assessment is Satisfied by the Ongoing Risk-Based Approach Utilized by Financial Services Companies – Section 500.09 and Section 500.01(k)

In our Letter to DFS, we urged DFS to revise any final rules to adopt the same risk-based framework developed by federal requirements and prevailing industry standards, including the NIST (National Institute of Standards and Technology) Cybersecurity Framework, the International Organization for Standardization's ("ISO") and the Interagency Guidelines.[8] We encouraged DFS to affect this approach by permitting Covered Entities to: (1) carry out a risk assessment for the purpose of identifying relevant risks and categorizing such risks; (2) implement applicable measures or other superseding or compensating controls as appropriate in accordance with the level of risk; and (3) maintain supportive documentation of steps (1) and (2).[9] DFS responded by expanding the Proposal's Risk Assessment section, and stating through much of the Proposal that compliance with applicable sections of the Part shall be "based on" the Covered Entity's Risk Assessment. While we once again thank DFS for adopting changes based on our concerns, we do not believe Section 500.09 as written adequately describes risk mitigation processes as carried out by financial institutions.

Section 500.09 of the Proposal states that a Covered Entity shall conduct "a" periodic Risk Assessment, which Risk Assessment shall inform the design of an entity's cybersecurity program.[10] Generally, financial institutions may conduct a single, strategic enterprise-wide risk assessment to inform the overall cybersecurity strategy, with additional operational risk assessments carried out thereafter, on an as needed basis, such as when an institution is introducing major systems or technology changes into their infrastructure, or when new threat and vulnerability information relative to the institution is identified. A risk-based approach will entail conducting risk assessments as needed, in accordance with an entity's risk profile. As currently written, the Proposal's version of a risk assessment appears to be a single, enterprise-scale assessment, conducted periodically, and updated in a uniform way. Within the context of

[8] The Interagency Guidelines, jointly published by the Federal Deposit Insurance Corporation, Federal Reserve, National Credit Union Administration, and Office of the Comptroller of the Currency, 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." *See* 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 include 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).

[9] SIFMA Letter to DFS, at 6.

[10] DFS Proposal, at 6.

cyber and information security, a strategic risk assessment is generally one component of a risk management program, and its purpose is to identify: (1) threat scenarios applicable to the organization; (2) controls and control deficiencies, both internal and external to the organization; (3) the harm that may occur given the potential for threats exploiting controls and control deficiencies; and (4) the likelihood that harm will occur.[11] Once the risk level is determined, based on the organization's risk tolerance, an organization may respond accordingly, e.g., by adjusting its cybersecurity strategy and priorities.

In addition to the issues with Section 500.09 described above, this section as drafted is problematic in four other ways. First, by referring to "a periodic Risk Assessment of the Covered Entity's Information Systems", this section implies the assessment is solely of the Covered Entity's systems, though firms normally conduct their broader risk assessments in a more comprehensive way.  To avoid misallocation of resources by repeating risk assessments solely at the Covered Entity level, the language requires revision to clarify that a broader assessment is acceptable as long as it includes the Covered Entity's Information Systems. Second, by stating that the "Covered Entity shall conduct" the Risk Assessment, the provision implies that the Covered Entity must perform Risk Assessments itself, when many firms will have assessments conducted by an Affiliate (as stated above, on a broader scale). The proposed language should be revised to clarify that an Affiliate's risk assessment will satisfy the provision. Third, a major objective of performing risk assessments is to allow a firm to "assess" its risks by impact and probability and then apply the applicable controls as appropriate based on the assessed risk. The Proposal's current language ("based on its Risk Assessment") does not clarify that firms may apply the controls as appropriate based on the assessed risk (the approach implied in DFS's original stated intent of allowing firms to create cybersecurity programs that match relevant risks). Again, to avoid misallocation of resources, it is crucial to revise the regulation to make this clear. Finally, some of the Proposal's provisions (namely 500.05 (Pen Testing), 500.12(b) (Multifactor Authentication) and 500.15 (Encryption)), prescribe specific technological procedures or controls that may be superseded in the future, and the Proposal should be revised to allow firms to use superseding controls that are equally or more effective, as determined by the Covered Entity's CISO, or the CISO's qualified designee.

We accordingly recommend the below changes to Section 500.09(a) which will resolve the issues outlined above:

**Section 500.09 Risk Assessments**

(a) Each Covered Entity shall conduct ~~a~~ periodic ~~R~~risk ~~A~~assessments, or adopt those of an Affiliate, that include ~~of~~ the Covered Entity's Information Systems (any such assessment, the "Risk Assessment" or "Covered Entity's Risk Assessment") and are sufficient to inform the design of the cybersecurity program as required by this Part, including the appropriateness of the program's controls to the level and likelihood of the identified risk. Such Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations. The Covered Entity's Risk Assessment shall allow for revision of controls to respond to technological developments and evolving threats

[11] *See* NIST Special Publication 800-30: Guide for Conducting Risk Assessments, Joint Task Force Transformation Initiative, (September 2012).

> and shall consider the particular risks of the Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems. In the event a Covered Entity's CISO (or a qualified designee) has approved, in writing, the use of reasonably equivalent or more secure controls as compared to the default control set forth in Section 500.05, 500.12(b), and/or 500.15, the Covered Entity may comply with such Section(s) by applying the equivalent or more secure controls.

To conform with the revised language in Section 500.09, we recommend that the term Risk Assessment throughout the document be revised to state "Risk Assessments," and the definition of Risk Assessment in Section 500.01(k) be revised as follows:

> **Section 500.01(k)** *Risk Assessments* means the risk assessments that each Covered Entity carries out, as necessary, under section 500.09 of this Part.

Additionally, Section 500.08(a) regarding Application Security should be revised as follows to reflect the above changes to Section 500.09:

> **Section 500.08(a) Application Security**
> Each Covered Entity's cybersecurity program shall include written procedures, guidelines, and/or standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment, in each case developed and applied based on the Risk Assessments.

We believe that Section 500.09 of the Proposal is critical to the success of any final rules, as the Risk Assessment language has been placed throughout the document in lieu of our proposed language regarding a "risk-based approach."[12] To eliminate this confusion, we recommend revising the Proposal in this manner to be made consistent with current Federal regulations and industry-recognized best practices.

### C. Implementation Impracticalities and Unintended Consequences of the Proposed Technical Requirements

In this section, we specifically address the proposed requirements and offer detailed comments to improve their functionality. Some of the more impractical consequences of the Proposal, as currently drafted, relate to: (1) the requirement of Covered Entities to maintain an "audit trail" detailing five years of records; (2) encryption and multi-factor authentication requirements; (3) the superintendent notification requirement; (4) testing requirements; (5) the transition period for implementation regarding access privileges; and (6) the scope of the Proposal.

[12] *See* SIFMA Letter to DFS.

### 1. Audit Trail – Section 500.06

In our Letter to DFS, we urged DFS to utilize a risk-based approach when implementing an "audit trail" system, which would maintain necessary records for a period reasonably necessary to investigate anomalies. We once again thank DFS for considering our comments, as well as the comments of other organizations, and revising the original language, stating that the audit trail should be designed to "reconstruct material financial transactions," and "respond to Cybersecurity Events with a reasonable likelihood of materially harming any material part of normal operations." Further, the Proposal now requires Covered Entities to maintain such records for at least five years rather than six years.[13]

As written, the audit trail appears to be an attempt to satisfy the dual purpose of acting as an audit trail for financial transactions, and as an audit trail for cybersecurity events. On one hand, it appears that the purpose of this section is to act as a forensic-accounting requirement for financial transactions. On another, the objective of this section is to retain sufficient data to get to a hold-point, a known "good point." Moreover, although Section 500.06 is titled "Audit Trail," the audit trail requirement is only mentioned in Section 500.06(a)(2) in regards to cybersecurity events, and not in regards to the material financial transactions discussed in 500.06(a)(1).[14] Further, although Section 500.06(b) states that the "records" in Section 500.06 should be "maintained," a reading of Section 500.06(a) together with Section 500.06(a)(1) makes clear that (a)(1) only requires that Covered Entities have the ability to reconstruct material financial transactions.[15] There is no mention of an audit trail; the discussion of an audit trail appears to refer solely to cybersecurity matters, and is only discussed in the second half of the Section. It appears as if this is two sections in one.

As an initial matter, we recommend DFS clarify the exact purpose of this five-year requirement. Organizations need clarity in their obligations when determining how to structure and store data, which is complicated by these seemingly varied purposes. Moreover, the Audit Trail requirement does not sufficiently account for changes in an organization's information technology systems, as stored cybersecurity incident data will likely become irrelevant when an entity updates its infrastructure to a new operating platform. Financial institutions are at the forefront of in-house technology infrastructure advances, and updates to operating systems occur at a frequency much less than five years, making DFS' five-year record retention requirement of questionable utility for responding to cybersecurity events. Furthermore, the five-year requirement when applied to Section 500.06(a)(2) would require firms to store massive amounts of data that will not be useful to them. Accordingly, we propose that this section be revised as follows:

**Section 500.06 Audit Trail**

(a) Each Covered Entity shall securely ~~maintain systems~~ retain records that, to the extent applicable and based on its Risk Assessments:

  (1) are designed to retain evidence of ~~reconstruct~~ material financial transactions sufficient to support the rights and obligations of the Covered Entity with respect to such transactions; and

[13] DFS Proposal, at 6.

[14] *Id* at 6.

[15] *Id*.

(2) include audit trails reasonably designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming a~~ny~~ material part of the normal operations of the Covered Entity.

(b) Each Covered Entity shall maintain records required by Section 500.06(a)(1) ~~this Section~~ for not fewer than five years.

There are currently no existing requirements for financial institutions to maintain an "audit trail" of cybersecurity events, and it is unclear how the Proposal's requirements would minimize cybersecurity risks of Covered Entities, or provide the flexibility required in this dynamic space. Revising Section 500.06 in the manner proposed above will clarify the audit trail requirement, and optimize the data retention requirement in a manner consistent with the goals of both DFS and Covered Entities.

### 2. Multi-Factor Authentication – Section 500.12, and Encryption of Nonpublic Information – Section 500.15

In our Letter to DFS, we urged DFS to revise the stated requirements regarding multi-factor authentication, and encryption of nonpublic information. We recommended that any final rules concerning multi-factor authentication should be based on a risk-based assessment by financial firms, with compensating controls permitted where applicable.[16] Further, we highlighted the significant issues present within DFS' original proposed rule regarding mandatory encryption of all nonpublic information, recommending that any final rule on encryption be based on a risk-based analysis, and in light of compensating controls.[17] SIFMA again thanks DFS for considering our recommended changes, and revising the original proposed rule.

#### a. Multi-Factor Authentication

Section 500.12 has been revised in what we believe to be a largely positive manner, adopting a less prescriptive approach to multi-factor authentication. However, we believe Section 500.12(b), which currently mandates that a Covered Entity's CISO approve each and every mechanism by which internal networks are accessed does not accurately reflect best practices, nor operate as an effective cybersecurity measure. The purpose of Section 500.12(b) as written is not entirely clear. If in fact a Covered Entity's information security team determines that multi-factor authentication is not the best means by which to secure an entity's Information Systems, then such determination should not require approval by a CISO on every occasion. This provision specifically states that CISO approval is required even when "more secure controls" are used. We believe such approval is inherently unnecessary. We suggest that this section be revised as follows

**Section 500.12(b) Multi-Factor Authentication**
Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless based on the Covered Entity's Risk Assessments, ~~the Covered Entity's CISO has approved in writing the use of~~

[16] SIFMA Letter to DFS, at 14.
[17] *Id* at 14.

~~reasonably equivalent or more secure controls~~ other ~~utilizes reasonably equivalent or more secure access~~ controls are appropriately effective.

### b. Encryption of Nonpublic Information

As was stated in our Letter to DFS, a broad-spectrum encryption requirement is not only infeasible, but also detrimental to the ability of firms to maintain a fluid, evolving cybersecurity program.[18] Implementing mandatory encryption requirements will cause massive delays in data processing times and stretch critical in-house personnel with questionable security benefit.

DFS attempts to make a distinction between "external" and "internal" networks. Due to the complexity of current network environments, the line between external and internal networks has become increasingly blurred, to the point that seasoned information technology and information security professionals frequently have different definitions for each. Moreover, requiring data encryption across-the-board weakens security controls by: (a) blocking standard surveillance of such data to detect intruders; and (b) requiring the broad distribution of encryption keys to allow applications to access such data, increasing the number of vulnerability points.[19] In this way, although encryption is frequently thought of as a catch-all for cybersecurity, broadly mandating encryption of data increases cybersecurity challenges for Covered Entities, complicates in-house access to this data, and decreases in-house mobility toward a more advanced cybersecurity posture. We accordingly propose that this section be revised as follows:

**Section 500.15 Encryption of Nonpublic Information**

(a) As part of its cybersecurity program, based on its Risk Assessments, each Covered Entity shall implement controls~~, including encryption~~ to protect Nonpublic Information held or transmitted by the Covered Entity ~~both in transit over external networks and at rest~~, which shall include encryption for transit over external networks.

(1) To the extent a Covered Entity determines that encryption of Nonpublic Information in transit over external networks is not reasonably ~~in~~feasible or based on its Risk Assessments, that other controls are appropriately effective, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO (or a qualified designee).

~~(2) To the extent a Covered Entity determines that encryption of Nonpublic Information at rest is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.~~

(b) To the extent that a Covered Entity is utilizing compensating controls under (a) above, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO (or a qualified designee) at least annually.

Revising Section 500.15 in this manner will ensure that firms are able to adopt new technologies which supersede encryption, rather than unnecessarily locking Covered Entities into adoption of

[18] SIFMA Letter to DFS, at 14.
[19]*Id* at 14.

massive encryption efforts, and successfully maps to the language adopted by DFS in Section 500.12 of the Proposal. Moreover, DFS' Proposal retains the word "infeasible" as a requirement to illustrate why encryption has not been utilized. There is no discernible method by which CISOs could effectively demonstrate what is feasible, and what is not; as such we urge DFS to remove this language. Mass encryption of data, specifically data at rest, creates numerous information security challenges for financial organizations. Implementing encryption throughout existing programs and applications, thereby requiring encryption keys for basic system access, will dramatically impede normal business operations. Moreover, if encryption key(s) are lost, or compromised by bad actors, a Covered Entity's information systems will be placed in unnecessary risk, either due to being locked out of their own data, or giving a malicious actor access to sensitive Nonpublic Information.

Cybersecurity is a fluid area, and financial institutions require flexibility to ensure robust programs to meet the needs of a diverse industry. Although encryption is a useful and commonly used tool, it is neither the required or the preferred approach for the broad range of situations mandated in DFS' Proposal. DFS adopted what we believe to be a more correct approach in Section 500.12, where it recognized that while multi-factor authentication is currently one possible component of cybersecurity practice, new and better tools will be developed and adopted in the future. We suggest that DFS revise Section 500.15 in a similar fashion.

### 3. Notice to Superintendent – Section 500.17

In our Letter to DFS, we proposed revisions to Section 500.17 regarding the requirement for Covered Entities to provide notice to the superintendent within 72 hours (Notice Requirement) of a Cybersecurity Event.[20] We thank DFS for considering our comments, and limiting the scope of the Notice Requirement. However, we believe additional revisions are necessary, specifically regarding Section 500.17(a)(1) and Section 500.17(b).

#### a. Providing Notice to DFS When Notice is Required to Other Entities

A currently drafted, Section 500.17(a)(1) states that notice should be given to DFS when notice must be given to "any" government body, self-regulatory agency or "any" other supervisory body.[21] Based on a plain reading of this section as drafted, a global Covered Entity would be required to notify DFS when notice is required to any foreign, Federal, or non-New York state entity. We believe this falls strongly outside the remit of DFS, and the section should be revised as follows:

> **Section 500.17(a)(1)** Cybersecurity Events of which notice is required to be provided to any <u>New York</u> government body, <u>New York</u> self-regulatory agency or any other <u>New York</u> supervisory body<u>, excluding New York law enforcement agencies</u>.

Federal, foreign, and other state governments, agencies, and supervisory bodies do not require notice be given for occurrences outside their jurisdiction. As currently written, notice of every Cybersecurity Event must be forwarded to DFS regardless of the location of the event. Abiding

[20] SIFMA Letter to DFS, at 12.
[21] DFS Proposal, at 10.

by the Proposal as drafted, a Covered Entity with foreign operations, which becomes required to notify local foreign authorities of a cyber event occurring in that jurisdiction, will then be required to notify DFS of that foreign event, despite the fact that such international notice serves no apparent purpose for cyber resiliency.

Moreover, reading Section 500.17(a) as drafted together with the Proposal's current definition of Cybersecurity Event, it appears DFS desires to receive notice, regardless of whether an event is successful or unsuccessful, despite the fact that an unsuccessful attempt, by virtue of its plain meaning, cannot have a "reasonable likelihood of materially harming"[22] a Covered Entity. Indeed, DFS' commentary on the original proposed rules echoes this sentiment.[23] Although we agree that unsuccessful events could provide insight in some cases, we once again stress that, even with the aforementioned qualifying statements, providing notice to DFS of unsuccessful attempts provides very limited security or resiliency benefit.

### b. Statement to DFS Certifying Compliance

As currently drafted, Section 500.17(b) provides that each Covered Entity must submit an annual statement to DFS, "certifying that the Covered Entity is in compliance"[24] with the Proposal's requirements. However, situations may arise wherein a Covered Entity is not in full compliance with the final rules, and still has improvements to make to their cybersecurity program. A plain reading of this Section dictates that a Covered Entity must certify compliance with a rule with which it is not in fact in compliance. It appears the later parts of this Section contemplate noncompliance, but leave no safe harbor method of reporting said noncompliance. Section 500.17(b) manufactures potential criminal and/or civil liability for senior executives, as representatives of the Covered Entity. We accordingly recommend Section 500.17(b) be revised as follows:

> **Section 500.17(b)** Annually, each Covered Entity shall submit to the superintendent a written statement by February 15, in such form set forth as Appendix A, certifying that the Covered Entity is in compliance with the requirements set forth in this Part. To the extent a Covered Entity has identified areas, systems or processes that require material improvement, updating or redesign, the Covered Entity shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes; such voluntarily disclosed noncompliance and remediation efforts shall suffice as an exception to a certification of compliance. Each Covered Entity shall maintain for examination by the Department ~~all~~ records that ~~schedules, and data~~ support~~ing~~ the~~is~~ certification of compliance for a period of five years. ~~To the extent a Covered Entity has identified areas, systems or processes that require material~~

[22] *Id*.

[23] "Cybersecurity Event: Some commentators stated that this definition, and particularly its use of words like "unsuccessful" and "attempt" was overbroad and resulted in overbroad requirements. DFS has not revised this definition under the stated rationale that it is important for a comprehensive cybersecurity program to address attempts even where unsuccessful. However, the Department has revised several of the provisions of specific concern by requiring that certain provisions be based on the Risk Assessment and by including materiality qualifiers, such as the Notices to Superintendent section." *See* "Assessment of Public Comments for New Part 500 to 23 NYCRR," page 1. (2016).

[24] DFS Proposal at 10.

> ~~improvement, updating or redesign, the Covered Entity shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes.~~ Such documentation must be available for inspection by the superintendent.

As written, Section 500.17(b) creates a dilemma wherein Covered Entities may be faced with a choice of falsely certifying compliance on one hand, or facing regulatory sanction for noncompliance by having failed to provide the certification as to complete compliance. We propose DFS revise the language as drafted above, and clarify DFS' stance on how it believes Covered Entities should operate in this scenario, considering the evolving cybersecurity landscape, and the frequency with which firms must update their cybersecurity posture. In addition, we ask DFS to clarify the extent of confidential treatment given to Covered Entity certifications, whether in full, partial, or non-compliance. Any certification submitted pursuant to this Part will detail a Covered Entity's activities in relation to their active cybersecurity program; such summaries are valuable tools for malicious cyber actors, and we therefore stress that confidentiality is necessary when DFS handles any such certification documents.

### 4. Penetration Testing and Vulnerability Assessments – Section 500.05

In our Letter to DFS, we described why DFS' original language mandating annual penetration tests and vulnerability assessments were untenable, stating that due to DFS' broad definition of Information Systems, testing and assessment of each and every information system was not only unnecessary, but also infeasible.[25] We thank DFS for making certain modifications to the original proposed rule, recognizing that across-the-board testing of Information Systems is unnecessary, and shall instead be conducted in accordance with an entity's Risk Assessments. However, we believe Section 500.05 as drafted remains too broad, and does not adequately describe the processes by which systems and applications are tested. As such, we recommend that Section 500.05 be revised as follows:

> **Section 500.05 Penetration Testing and Vulnerability Assessments**
>
> (a) The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity's Risk Assessments, designed to assess the effectiveness of the Covered Entity's cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments~~, and shall be done periodically~~. Absent other reasonably effective means for ~~continuous~~ monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct the following, at a minimum, with respect to the Covered Entity's relevant Information Systems determined to be high risk pursuant to the Risk Assessments:
>
> (1) ~~annual~~ periodic penetration testing for relevant Internet-accessible systems ~~of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment~~; and
>
> (2) ~~bi-~~annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly

[25] SIFMA Letter to DFS, at 10.

known cybersecurity vulnerabilities in the Covered Entity's Information Systems ~~based on the Risk Assessment~~.

(b) To the extent a Covered Entity has identified areas, systems or processes that require material improvement, updating or redesign, the Covered Entity shall document the material deficiencies and the remedial efforts planned and underway to address such areas systems or processes; such voluntarily disclosed noncompliance and remediation efforts shall suffice as an exception to penetration testing and vulnerability requirements mandated in this Part.

The statement "based on the Covered Entity's Risk Assessment" does not adequately clarify that a firm should conduct penetration testing and vulnerability assessments as appropriate to the relevant risks. Moreover, pen testing is not appropriate for all systems, and a testing program should be implemented by a Covered Entity based on perceived risks; for example, a Covered Entity may conduct annual pen tests on critical systems and applications, with less frequent tests on new or updated systems and applications. Penetration testing resources are scarce, and industry best practices tailor such efforts on critical systems and applications for which they can have the greatest impact. DFS should include language stating the Section 500.05 requirements should only apply to high risk Internet-accessible systems; we believe the proposed revisions to this Section accomplish this. Further, the current language does not give firms license to utilize methods which supersede pen testing or vulnerability assessments, such as red teaming. DFS should revise the language as proposed, and further clarify that Covered Entities have the ability to utilize testing and assessments methods, as appropriate, in lieu of penetration testing or vulnerability assessments where appropriate, rather than adopting specific testing and assessment methodologies into the Proposal that are not universally applicable. Finally, financial institutions may not utilize tests or assessments when an entity is in the process of remediating issues within the infrastructure. The addition of Section 500.05(b), which mirrors our proposed language revisions in Section 500.17(b), will allow Covered Entities to safely remediate discovered weaknesses within their infrastructure.

Finally, we suggest DFS revise the definition of penetration testing in Section 500.01(i) to more accurately reflect real-life testing processes:

> **Section 500.01(i)** *Penetration Testing* means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by ~~attempting~~ simulating unauthorized penetration of databases or controls from outside or inside the Covered Entity's Information Systems.

### 5. Section 500.22 – Transition Periods

We thank DFS for recognizing that achieving each and every additional control and requirement in the Proposal would be infeasible, and implementing a staggered series of compliance times for each subsection in this Part. However, Section 500.07 as drafted mandates a potential overhaul of current access privilege practices by Covered Entities. We therefore ask DFS to revise Section 500.22(b)(2) as follows, extending the time to comply with the access privilege requirements of Section 500.07:

> **Section 500.22(b)(2)** Eighteen months from the effective date of this Part to comply with the requirements of sections 500.06, 500.07, 500.08, 500.13, 500.14(a)(1) and 500.15 of this Part.

### 6. Scope of the Proposal –Nonpublic Information, Cybersecurity Event, Third-Party Service Providers, and Exemptions

Finally, we suggest that any final rule will benefit from definitions that narrow the scope of application of the Proposal's substantive requirements. The definitions of "Nonpublic Information," and "Cybersecurity Event," the provision discussing third-party service providers, and DFS' proposed exemptions should be revised. Defined below are examples of how to narrow the Sections in this Part in a manner consistent with current information security best practices, and will ensure Covered Entities adhere to well defined standards of care, while meeting DFS' regulatory objectives.

#### a. Nonpublic Information – Section 500.01(g)

In our Letter to DFS, we stated that the definition of Nonpublic Information in DFS' original proposal was overly broad, and suggested the definition should be sufficiently narrowed to only include relevant information.[26] We thank DFS for considering the proposed revisions drafted in our Letter, as well as the proposed revisions from other associations, and industry stakeholders. However, we believe that the definition of Nonpublic Information in the Proposal remains overly inclusive, and does not accurately reflect current practices of financial institutions.

Nonpublic Information as currently defined in Section 500.01(g) should be revised to include an exemption for certain kinds of personal information, mirroring an exemption titled "information not included" in the Gramm-Leach-Bliley Act's (GLBA) section on personally identifiable financial information[27]. Additionally, we believe DFS should adopt the HIPAA (Health Insurance Portability and Accountability Act) exemption for health care provider information held by Covered Entities to exempt data held by those entities concerning their employees, which they may hold only in their capacity as an employer.[28] The basic requirement under the HIPAA Security Rule is that covered entities must secure electronic "protected health information," and exempts, among others, individually identifiable health information in employment records held by a HIPAA covered entity, in its role as employer.[29] We accordingly propose that Section 500.01 be revised as follows:

> **Section 500.01(g)** *Nonpublic Information* shall mean all electronic information that is not Publicly Available Information and is:

[26] Letter to DFS at 8.

[27] **Information not included**. Personally identifiable financial information does not include: (A) A list of names and addresses of customers of an entity that is not a financial institution; and (B) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses. *See* 16 C.F.R. § 313.3(o)

[28] Protected health information excludes individually identifiable health information: … (iii) In employment records held by a covered entity in its role as employer; and (iv) Regarding a person who has been deceased for more than 50 years. *See* C.F.R. 164.103.

[29] *See* 45 C.F.R. 164.103.

(1) 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.

(2) Any information concerning an individual ~~which because of name, number, personal mark or other identifier can be used to identify such individual, in combination with any one or more of the following data elements~~ that is any: (i) social security number, (ii) driver's license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) security code, access code or password that would permit access to an individual's financial account; or (v) biometric records.

(3) Any information or data, except age or gender, in any form or medium created or received by ~~or derived from~~ a health care provider ~~or an individual~~ and that is Protected Health Information as defined in the Health Insurance Portability and Accountability Act Privacy Rule ~~: relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual;~~.

(4) Nonpublic Information shall not include: (i) a list of names and addresses of individuals of an entity that is not a financial institution; (ii) information that does not identify an individual, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses; or (iii) information excluded from the definition of Protected Health Information as defined in the Health Insurance Portability and Accountability Act Privacy Rule, including individually identifiable health information in employment records held by a covered entity in its role as employer, or information regarding an individual who has been deceased for more than fifty years.

To affect an adequate tailoring of the definition of Nonpublic Information, we further recommend that the term HIPAA Covered Entity be added to Section 500.01, mapped to HIPAA's (Health Insurance Portability and Accountability Act) definition of Covered Entity[30], as follows:

> *HIPAA Covered Entity* means a (1) health plan, (2) health care clearinghouse, or (3) health care provider who electronically transmits any health information in connection with transactions for which the United States Department of Health and Human Services has adopted standards; or a Covered Entity, as defined in the Health Insurance Portability and Accountability Act.

As currently drafted, Section 500.01(g)(2)'s requirement is not effectively applied to most of the substantive provisions in which the term "Nonpublic Information" is used in this Part. Firms do not track the combination of identifying information together with more sensitive information such as social security numbers, driver's license numbers, and biometric records. Thus, making

[30] *Covered Entity* means: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter. *See* 45 C.F.R. 160.103 – Definitions.

the definition based on the combination of these two factors unhelpful. As it is equally protective to simply list the sensitive information in clause (g)(2), we recommend that the concept of "combination" be removed and that simply the presence of sensitive information be sufficient to make data Nonpublic Information. As drafted, Section 500.01(g)(3) is even broader than the HIPAA definition of individually identifiable health information, as it includes any information "provided by an individual" that covers the relevant topics, applies to entities that aren't covered entities under HIPAA and does not include the relevant HIPAA exclusions.

Covered Entities should not be required to extend compliance resources protecting this unnecessarily broadened category of data. We believe the above alterations align with standard best practices of Covered Entities and with the relevant HIPAA definitions, while meeting DFS' goals. Moreover, as we discussed in our recommendations regarding alterations to the definition of Banking Law Regulated Entities, we urge DFS to create clear citations in any final rule to the Health Insurance Portability and Accountability Act, including website URL links to ensure entities are easily able to determine which portions of their enterprise are covered.

Finally, we ask DFS to clarify the scope of an entity's cybersecurity program as it relates to Nonpublic Information. Where a Covered Entity performs both DFS-licensed and non-DFS-licensed activity (e.g., insurance services regulated by DFS and brokerage services), it does not appear that Nonpublic Information derived from the brokerage services would be in scope of the Proposal. However, based on the enterprise-wide scale of the Proposal as drafted, DFS appears to desire that Nonpublic Information include information derived even from non-DFS-licensed activities, which we believe falls outside of DFS' stated jurisdiction.

### b. Cybersecurity Event – Section 500.01(e)

In our Letter to DFS, we stated that the definition of the term Cybersecurity Event was overly broad.[31] We believe that by including the original definition of Cybersecurity Event, DFS sets a troubling and misguided precedent by stating that any attempt made on an entity's Information System qualifies as a Cybersecurity Event. This is not an approach taken by any other regulator, or standard-setting body, and we believe that a different approach should be adopted in any final rules.[32] As drafted, Section 500.01(e) defines a Cybersecurity Event as any act or attempt to access, disrupt or misuse any Information Systems or Information stored on those systems. All manner of information is stored on an organization's systems, more so due to DFS' broad definition of Information Systems. The focus of DFS' Proposal is on customer protection; therefore, we propose DFS alter the definition of Cybersecurity Event to both remove any reference to unsuccessful events, and limit any information targeted to Nonpublic Information. We therefore propose that the definition of Cybersecurity Event be revised as follows:

[31] SIFMA Letter to DFS, at 8.

[32] The National Institute of Standards and Technology (NIST) does not define "cybersecurity event." However, NIST defines "Incident" as *"[a]n occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies*." A "Cyber Incident" is defined as *"[a]ctions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein." See NIST, "Glossary of Key Information Security Terms*" (June, 2013). http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

> **Section 500.01(e)** *Cybersecurity Event* means any material compromise of ~~act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse~~ an Information System or Nonpublic ~~i~~Information stored on such Information System.

We believe there is very limited utility to a Covered Entity's cybersecurity program in focusing efforts on responding to unsuccessful attempts, or minor incidents that are otherwise mitigated. Financial institutions can face hundreds or even thousands of attempts to compromise their Information Systems every day, and a requirement to treat unsuccessful or immaterial actions as events for the purposes of a Cybersecurity Program will not improve an organization's security. We therefore urge DFS to revise their Proposal in the manner suggested above.

### c. Third-Party Service Provider Security Policy – Section 500.11

In our Letter to DFS, we suggested DFS revise the original proposal's requirements regarding oversight of third-parties, stating that any requirements for preferred contracts and associated provisions were untenable, and any third-party oversight requirements should be risk-based.[33] We thank DFS for revising Section 500.11, and extending the time-period for compliance with this provision, recognizing that any alteration in the relationship between financial institutions and their service providers will take a significant period of time. However, we believe that slight clarifications to Section 500.11 in the Proposal are necessary to carry out DFS' intent and enable the security of the sector. We therefore propose that Section 500.11 be revised as follows:

> **Section 500.11 Third Party Service Provider Security Policy**
>
> (a) Third Party Service Provider Policy. Each Covered Entity shall implement written policies and procedures designed to evaluate and review ~~ensure~~ the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessments of the Covered Entity and shall address to the extent applicable:
>
> (1) the identification and risk assessment of Third Party Service Providers;
>
> (2) minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to conduct ~~do~~ business with the Covered Entity, as may be appropriate based on the risks they present;
>
> (3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers, as may be appropriate based on the risks they present; and
>
> (4) periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices; or adequacy of compensating controls where literal compliance is not feasible or practical.
>
> (b) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers including to the extent applicable guidelines addressing¸ based on the risks presented by a given Third Party Service Provider:
>
> (1) the Third Party Service Provider's policies and procedures for access controls ~~including its use of~~ which may include Multi-Factor Authentication or Risk-

[33] SIFMA Letter to DFS, at 11.

Based Authentication, to protect against unauthorized access to Nonpublic Information (in connection with services provided to Covered Entities) in accordance with ~~as defined by~~ section 500.12 of this Part ~~to limit access to sensitive systems and Nonpublic Information~~;

(2) the Third Party Service Provider's policies and procedures ~~for use of encryption as defined by section 500.15~~ to protect Nonpublic Information held or transmitted by the Third Party Service Provider in connection with its services provided to Covered Entities, which shall include encryption for transit over external networks or effective alternative compensating controls that are approved by the Covered Entity ~~in transit and at rest~~;

(3) notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or Non-public Information being held by the Third-Party Service Provider; and

(4) representations and warranties addressing the Third Party Service Provider's cybersecurity policies and procedures that relate to the security of the Covered Entity's Information Systems or Nonpublic Information.

(c) Limited Exceptions

(1) An agent, employee, representative or designee of a Covered Entity who is itself a Covered Entity need not develop its own Third Party Information Security Policy pursuant to this section if the agent, employee, representative or designee follows the policy of the Covered Entity that is required to comply with this Part.

(2) A Covered Entity need not implement a Third Party Information Security Policy with a Third Party Service Provider if a contact between the Covered Entity and the Third Party Service Provider was in force prior to the effective date of this Part. Such exception shall last in perpetuity until the expiration of such contract.

As drafted, Section 500.11 of the Proposal dictates specific requirements for Covered Entities based on their Risk Assessments. However, the Proposal as written treats all third parties in a similar manner, stating only that certain provisions shall apply "to the extent applicable." However, we believe DFS should more specifically state that the interaction between Covered Entities and service providers shall not only be based on risks presented by the Covered Entity, but also on the risks presented by said service providers. A one-size-fits-all provision mandating certain requirements in dealings with service providers, differentiated only by language stating "to the extent applicable" does not adequately consider the spectrum of third parties with which Covered Entities contract. Financial institutions currently employ robust protocols regarding third party technology services, derived from risk-based private and public-sector recognized standards.[34] Moreover, we believe DFS should include a temporary exception for contractual relationships already in existence at the time of the effective date as to not infringe on existing contractual rights of Covered Entities and Third Party Service Providers. We believe the

[34] *See* FFIEC IT Examination Handbook, "Business Continuity Planning, Appendix J: Strengthening the Resilience of Outsourced Technology Services." (February 6, 2015). http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-j-strengthening-the-resilience-of-outsourced-technology-services.aspx.
*See* NIST, "Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1" (January 10, 2017). https://www.nist.gov/sites/default/files/documents/2017/01/17/draft-cybersecurity-framework-v1.1.pdf

revisions suggested above effectively meet DFS' regulatory goals, while ensuring Covered Entities are not required to treat each third party in the same manner irrespective of said third party's presented risks.

### d. Exemption for De Minimis New York Operations – Section 500.19

In our Letter to DFS, and as described above, we ask DFS to consider limiting the definition of Covered Entity, and limit the scope of entities potentially covered by the Proposal. As noted, DFS has made significant positive alterations to the original proposal. However, we believe that DFS has placed a number of organizations unnecessarily in-scope through the proposed language in Section 500.19. As drafted, DFS exempts only entities with "fewer than 10 employees…less than $5,000,000 in gross annual revenue in each of the last three fiscal years, or less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates."[35] This Section appears to calculate assets and revenue at an enterprise level, considering only the entire size of an entity, rather than its impact on the New York State financial ecosystem. Although it may in fact have been DFS' intent to stretch the Proposal to all institutions earning more than $5,000,000 annually, we believe this is far beyond DFS' remit. Numerous regional financial institutions with de minimis financial ties to New York State will be unnecessarily brought within the reach of this Proposal. We recommend DFS revised Section 19(a) as follows:

**Section 500.19(a) Exemptions**

(a) Limited Exemption. Each Covered Entity with:
  (1) fewer than 10 employees including any independent contractors, or
  (2) less than $5,000,000 in ~~gross~~ annual revenue in each of the last three fiscal years earned in New York State, or
  (3) less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates.

Consider for example, an institution which earns $100,000 in New York annually, but $5,000,000 annually nationwide; based on the Proposal as written, said institution cannot utilize this exemption. Such a provision unnecessarily places nearly every regional financial institution doing even minute business in New York in scope. A requirement anchoring regional institutions to New York in this manner may deter financial institutions with smaller New York business portfolios from being involved in the state. We believe institutions with a de minimis impact on the financial dealings of New York residents, and on the New York State financial system should not come within the purview of any final rule, and recommend this section is altered accordingly.

*    *    *

We welcome further engagement and discussion with DFS concerning 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 Tom Wagner at 212-313-1161 or twagner@sifma.org.

[35] DFS Proposal, at 10-11.

Sincerely,

*/s/ Rich Baich*
Rich Baich
Chair
FSSCC

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

*/s/ Richard Foster*
Richard Foster
Senior Vice President & Senior Counsel
FSR/BITS

*/s/ Doug Johnson*
Doug Johnson
Senior Vice President
ABA

cc: Tom Price, SIFMA
Grant Levine, SIFMA