November 14, 2016

The Honorable Maria T. Vullo
Superintendent
New York Department of Financial Services
One State Street
New York, NY 10004-1511

Attention: Ms. Cassandra Lentchner
Executive Deputy Superintendent for Compliance

Re: **New York State Department of Financial Services Proposed 23 NYCRR 500 – Cybersecurity Requirements for Financial Services Companies**

Dear Superintendent Vullo:

The undersigned trade associations are writing to the New York State Department of Financial Services (DFS) on behalf of their member financial services companies regarding proposed 23 NYCRR 500 - Cybersecurity Requirements for Financial Services Companies ("proposed regulation"). We thank you for the opportunity to submit these comments. We strongly support the underlying goal of the proposed regulation "to promote the protection of customer information as well as information technology systems of regulated entities…" to respond to the acknowledged "… ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors."[1]

Financial services companies believe the most effective way to protect their New York customers' personal information and information technology ("IT") systems is to employ cybersecurity frameworks that are risk-based, flexible, and workable. Accordingly, the undersigned support the following statements in the Introduction to the proposed regulation: "Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances … This regulation requires each company to access its specific risk profile and design a program that addresses risks in a robust fashion…"[2] These statements are in line with the approach reflected in other key existing security frameworks, including the recently published "G7 Fundamental Elements of Cybersecurity for the Financial Sector" and the National Institute of Standards and Technology (NIST), the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification security frameworks.

The key security frameworks listed above are similarly focused on active risk management rather than on rigid, prescriptive security requirements. By contrast, we respectfully submit that the proposed regulation as a whole does not appear to reflect this approach and, consequently, poses the following fundamental, overarching concerns:

(1) Absence of Risk-Based Approach

Notwithstanding the statements in the Introduction, quoted above, the actual requirements of the proposed regulation appear to be prescriptive, not to be risk-based, and generally not to include a materiality standard or harm trigger. The one-size-fits-all nature of these requirements does not account for different financial services companies' unique business models, differences in their IT systems and their widely varying risk profiles. More specifically, Sections 500.02 and 500.03 do

[1] Proposed 23 NYCRR 500 - Cybersecurity Requirements for Financial Services Companies Section 500.0 - Introduction
[2] id.

not provide for the required cybersecurity program, policies and procedures to "… match the relevant risks and keep pace with technological advances …" The requirements and controls, in Sections 500.04 - 500.17, appear similarly prescriptive and to reflect the absence of a risk management focus.

Accordingly, we respectfully urge modification to the proposed regulation to make all of its requirements risk-based, and appropriate to each Covered Entity's risk profile; its nature, size, and complexity; the scope of its activities; and the sensitivity and amount of personal customer information the Covered Entity maintains. Allowing such tailoring of Covered Entities' programs, policies and security measures will provide them the flexibility to best protect their New York customers' personal information and the IT systems on which such information is maintained.

(2) Unworkable Requirements

Some particularly troublesome provisions of the proposed regulation would impose requirements that appear unclear, inappropriately applied to all financial institutions, practically unworkable, or technically infeasible. Concern with these provisions is exacerbated by the apparent prescriptive nature of the requirements and the breadth of the underlying definitions of key terms.

Examples include the requirements for: (i) audit trails that allow for "complete and accurate reconstruction of all financial transactions …" and maintenance of audit trail records for at least six years in Sections 500.06(1) and (6); (ii) annual assessments of all third party vendors or service providers in Section 500.11(a)(4); (iii) "support for Multi-Factor Authentication for any individual accessing web applications that capture, display or interface with Nonpublic Information" in Section 500.12(d); (iv) encryption of all Nonpublic Information at rest no later than five years after the effective date of the regulation in Section 500.15; (v) timely destruction of all Nonpublic Information "that is no longer necessary for the provision of products and services for which such information was provided …" in Section 500.13; and (vi) notice to the superintendent within 72 hours after becoming aware of a Cybersecurity Event in Section 500.17.

Concern with a number of these provisions may be addressed by making their requirements risk-based and limiting their applicability to sensitive information systems or sensitive nonpublic information. Other provisions may require additional specific modifications and some requirements that are technically infeasible may need to be eliminated altogether. More specific suggestions to address these concerns are provided in some of the undersigned's individual letters and others' letters to the DFS relating to the proposed regulation.

(3) Overly Broad Definitions

The definitions of key terms, particularly the definitions of "Cybersecurity Event," "Information System," and "Nonpublic Information" are overly broad.

The definition of "Cybersecurity Event" would include thousands of unsuccessful attempts to access Cover Entities' Information Systems and daily occurrences of routine network activity and human errors, which are unlikely to result in material harm to either a Covered Entity or an individual subject of Nonpublic Information. The inclusion of unsuccessful attempts within the scope of the definition of "Cybersecurity Event," without a clear harm trigger, would result in multiple daily triggering of the notice and reporting requirements in Section 500.17. In fact, compliance with the requirements in Section 500.17 to report any "Cybersecurity Event" that has a "reasonable *likelihood* of materially affecting normal operations …" *(Italics added.),* that affects Nonpublic Information, or that involves "actual *or potential* unauthorized tampering…" *(Italics* *added.)* is likely to be practically impossible and to unnecessarily overburden resources of Covered Entities and the DFS without providing commensurate benefit.

A number of the requirements and controls prescribed by the proposed regulation are appropriate only for sensitive information systems and sensitive nonpublic information. However, the definitions of the terms "Information System" and "Nonpublic Information" include systems and much information that are not sensitive.

The definition of "Nonpublic Information" could be construed to include essentially any business information of a Covered Entity or any information about a customer obtained by a Covered Entity in connection with the provision of a financial product or service. Much of the concern with the prescriptive nature and absence of a risk-based approach in the proposed regulation flows from this overly broad definition. To apply all of the proposed regulation's requirements and controls to all the IT systems and information encompassed within the scope of the definitions of "Information System" and "Nonpublic Information" would be unnecessarily burdensome and costly, again without commensurate benefit.

Accordingly, we respectfully urge modification to the definition of "Cybersecurity Event" to ensure that it includes a materiality standard and harm trigger. We also urge modification to the proposed regulation to add two new terms: "Sensitive Information System" and "Sensitive Nonpublic Information," and to make certain requirements and controls only applicable to "Sensitive Information Systems" and/or "Sensitive Nonpublic Information," as appropriate to the likelihood of material harm to a Covered Entity or New York customer in the event of unauthorized access, disruption or misuse of an IT system or customer information.

(4) Extraterritorial Effects

Several provisions would cause the proposed regulation to be extraterritorial. These provisions would: (i) impose security requirements applicable to Nonpublic Information of individuals who reside outside New York; and (ii) subject Covered Entities to reporting obligations relating to Cybersecurity Events that may occur outside New York and not involve the Nonpublic Information of New York residents. These provisions are unnecessarily duplicative of requirements imposed under other state, federal and international laws.

Of most concern: (i) the definition of "Nonpublic Information," in Section 500.01(g) is not limited to information of New York residents; (ii) the reference to "customers" in Section 5000.18(a)(1) is not limited to New York residents; and (iii) the trigger for notice to the superintendent in Section 500.17(a)(1) is "any Cybersecurity Event of which notice is provided to *any* government or self regulatory agency …"*(Italics added.)* which extends to notices required of Covered Entities in connection with Cybersecurity Events that may occur outside New York and not involve the Nonpublic Information of New York residents.

We respectfully urge modification to the definition of "Nonpublic Information" and to the proposed regulation as otherwise necessary to ensure that its security requirements are only applicable to the Nonpublic Information or Sensitive Nonpublic Information of New York residents and that Covered Entities' reporting requirements only apply to Cybersecurity Events that occur in New York and involve the Sensitive Nonpublic Information of New York residents.

(5) Uniform National Security Standards

In departing from the risk-based approach of key existing security frameworks, we believe that the proposed regulation is likely to operate counter to, rather than to further, the goal of uniform, risk-based and flexible security standards from state to state. Uniform standards are essential because security policies and procedures of financial services companies generally are the same across an institution's enterprise and do not vary from state to state.

In addition to the above, we also respectfully submit the following with respect to the proposed regulation:

Transitional Period

Given the many new requirements to which financial services companies will be subject under the proposed regulation, we respectfully submit that the transition period of 180 days from the effective date, provided in Section 500.21, will not allow enough time for Covered Entities to come into compliance. Accordingly, we urge modification to Section 500.21 to allow twenty-four months from the effective date to come into compliance except as otherwise specified.

Confidentiality

Given the sensitivity and proprietary nature of information a Covered Entity may be required to submit to the superintendent and the possibility that disclosure of such information could cause the Covered Entity substantial injury, we urge modification: (i) to provide that any Nonpublic Information or Sensitive Nonpublic Information provided to the Commissioner pursuant to the proposed regulation shall be maintained as confidential; and (ii) to permit a Covered Entity to request that such information be protected from disclosure under the New York open records laws.

Satisfaction of Requirements by Parent or Affiliate

For financial services companies that are part of a group, sometimes security measures and protocols may be most effectively implemented across the enterprise or by the parent or a particular affiliate of the Covered Entity. Accordingly, we also urge modification to permit the requirements of the proposed regulation to be met on an enterprise basis for Covered Entities that are part of a group and to allow use of the personnel and/or resources of a parent or affiliate to satisfy the requirements of the proposed regulation.

In conclusion, as noted several times above, financial services companies believe security standards that are risk based, flexible and appropriate to each company's risk profile are necessary for each institution to most effectively protect its customers' personal information and the IT systems on which such information is stored.

We hope to have the opportunity to engage in continued dialogue with the DFS regarding the proposed regulation and are committed to working with the DFS to craft a flexible, risk-based, and workable cybersecurity regulation that meets our mutual goal of protecting customer information in light of ever growing threats.

Thank you for your consideration of these comments, and please contact us if you have any questions.

Sincerely,

Organization	Name	Phone Number	E-mail Address
American Bankers Association	Sarah Ferman	202-663-5510	sferman@aba.com
American Council of Life Insurers	Robbie Meyer	202-624-2184	robbiemeyer@acli.com
America's Health Insurance Plans	Bob Ridgeway	501-333-2621	bridgeway@ahip.org
American Land Title Association	Justin Ailes	202-261-2937	justin@alta.org
Blue Cross Blue Shield Association	Paul Brown	202-626-4802	paul.brown@bcbsa.com
Council of Insurance Agents and Brokers	John Fielding	202-350-5864	john.fielding@ciab.com
Independent Insurance Agents & Brokers of America	Wes Bisset	202-302-1607	wes.bissett@iiaba.net
Insured Retirement Institute	Chelsea Crucitti	202-469-3032	CCrucitti@irionline.org
National Association of Insurance and Financial Advisors	Gary Sanders	703-770-8192	gsanders@naifa.org
National Association of Mutual Insurance Companies	Paul Tetrault	978-969-1046	ptetrault@namic.org
National Association of Professional Insurance Agents	Lauren Pachman	703-518-1344	laurenpa@pianet.org
Property Casualty Insurers	Dierdre Manna	847-553-3613	deirdre.manna@pciaa.net

Association of America			
Reinsurance Association of America	Matthew T. Wulf	202-783-8381	wulf@reinsurance.org