December 5, 2016

Maria T. Vullo, Superintendent
New York Department of Financial Services
One State Street
New York, N.Y. 10004-1511

Re: Joint Industry Letter on Proposed 23NYCRR Part 500 – *Cybersecurity Requirements for Financial Services Companies*

Dear Superintendent Vullo:

Businesses operating in New York State are and will remain focused on matters of cybersecurity risk. We recognize that our ability to prevent and address cyber attacks is critical; to not do so is to risk the compromise of sensitive customer data. Breaches in cybersecurity result not only in adverse legal and regulatory consequences for businesses but also create reputational damage to financial services providers and business as a whole.

All that said, the implications of Proposed 23 NYCRR Part 500 – *Cybersecurity Requirements for Financial Services Companies* – must be carefully reviewed for unintended consequences that could cost the business community many millions of dollars in compliance cost, for very little value, resulting in Covered Entities' expending resources on less beneficial security protection strategies. Importantly, the approach we recommend below would promote harmonization with existing federal cybersecurity requirements. Cybersecurity regulations issued without coordination with current requirements will lead to massive confusion, given the many federal entities with overlapping jurisdiction in this area. As discussed below, the Proposed Regulation contains a number of rigid requirements that extend well beyond those embodied in existing federal and state regulations, and both DFS guidance and the Proposed Regulation should be amended to reduce the risk of unintended consequences. At a minimum, we urge the Department to delay the promulgation of any final Regulation in order to facilitate a comprehensive deliberative process between the Department and Covered Entities.

We strongly believe that the final Regulation must be risk-based, so any Covered Entity (and the third parties with which they contract) may take into account the broad security environment in which they operate, the particular risks to which they are or may be subject, the size and complexity of such risks, the nature and scope of their activities, and the sensitivity of the customer information they maintain. It must also not be overly-prescriptive as to specific security technologies, so that businesses are forced into spending resources on a particular technology that may become quickly obsolete and at the expense of certain other technologies that may be better suited as a defense for that Entities' particular risks.

One example of where we believe that the Proposed Regulation misses the risk-based, not-prescriptive mark is the provision that will require financial services companies to encrypt all of their at-rest, non-computerized data (Part 500.15). This provision will cost companies many millions of dollars to implement over a long period of time, for what we believe to be of very little value. The risk of a breach to at-rest data is very small, since it is not resting on a computer and is, therefore, not a prime candidate for a cyberattack. The proposed five year implementation timetable for this provision included in the Proposal demonstrates that the Department of Financial Services recognizes that this will be a difficult provision with which to comply. We would be remiss, however, if we did not point out that the rapid-fire pace of changing technology could very well make this type of security measure obsolete in five years and companies would have expended many millions of dollars for compliance for no significant benefit. This is also precisely the reason why business cybersecurity processes employ "defense in depth" strategies that include multiple layers of cybersecurity, rather than just reliance

on one or two defenses at the expense of others, and those layers may differ, depending on the risks to the particular Covered Entity.

The Proposal applies 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 of the Insurance Law 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 governed by the Proposal, then any final rule resulting from the Proposal 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.

Another example of where this Proposal misses the mark are the provisions that seek to impose significant new, likely unachievable, compliance requirements – the third-party information security policy provisions (Part 500.11). Although we agree that oversight of the use of sensitive information by any third party vendor of a Covered Entity needs to be a critical component of a robust cybersecurity policy, we have heard from numerous businesses that these Proposed provisions go well beyond what can reasonably be expected by mandating "representations and warranties" that the third party is "*free of viruses, trap doors, time bombs and other mechanisms that would impair the security of the Covered Entity's Information Systems or Nonpublic Information.*" A third party service provider is likely not going to make this representation, because such a representation would be difficult, if not impossible, to make. No information system will ever truly be "free of" cyber threats, since no organization – commercial or government – can represent that there are no flaws or vulnerabilities on its systems.

This provision is also not limited to just vendors that have access to sensitive customer information and would, therefore, appear to apply to any vendor with which a financial service company is doing business (such as a printer or dry cleaner), which would place Covered Entities in the position of spending millions of dollars to review every single vendor contract (perhaps numbering in the several thousand for larger entities), whether such vendor has access to sensitive customer information, or not.

Therefore, we believe that this provision, in particular, must be amended to avoid mandating contract provisions and representations with third parties. For covered entities using a large number of service providers, assessing every one of them annually is just not reasonable. These provisions should be risk-based and certainly limited to vendors with access to sensitive information systems or sensitive customer information.

Given the significant compliance costs to business that could be associated with this Proposal if it is promulgated as currently proposed, we believe that it is not unreasonable to request more time to implement a deliberative process that will ensure that both the financial services community, and the third party vendors with which they contract, to provide input as to the appropriate outcome. By doing so, the Department will ensure that the proposed regulatory regime implemented will effectively assist the regulated entities in their management of cybersecurity risks.

A longer review period will also facilitate the ability of the Department to achieve a seamless regulatory framework with international and federal regulators that have also proposed or implemented regulations or standards for enhanced cyber risk management. It would certainly seem to be counterproductive to the goal of an effective financial services cybersecurity framework to have conflicting or duplicative regulations or standards with which to comply.

To this end, the undersigned on this letter believe that they can most effectively protect their customers' information and their information technology (IT) systems via cybersecurity frameworks: (i) that are risk-based, flexible, and scalable; and (ii) that permit each Covered Entity to take into account the broad security environment in which it operates, the particular risks to which it is or may be subject, its size and complexity, the nature and scope of its activities, the sensitivity of the customer information it maintains, and the security laws and regulations to which the insurer and independent agent already is subject, among other things. We would be pleased to work with you on addressing revisions to the Proposal that would bring it into conformance with these frameworks.

Sincerely,

Heather C. Briccetti, Esq., President and CEO
The Business Council of New York State, Inc.

Cate Paolino, Director, State Affairs, Northeast Region
National Association of Mutual Insurance Companies

Kristina Baldwin, Vice President
Property Casualty Insurers Association of America

Mary A. Griffin, President & CEO
Life Insurance Council of New York, Inc.

John J. Witkowski, President & CEO
Independent Bankers Association of NYS

John C. Parsons, II, President
Professional Insurance Agents of NY

Lisa Lounsbury, Interim President & CEO
Independent Insurance Agents & Brokers of NY

Ellen Melchionni, President
New York Insurance Association

Lawrence Holzberg, President
NAIFA-NYS

Paul Macielak, President & CEO
New York Health Plan Association

Cc: William Mulrow
Secretary to the Governor
Alphonso B. David, Esq.
Counsel to the Governor