AAMGA
American Association of Managing General Agents

610 Freedom Business Center | Suite 110
King of Prussia, PA 19406
ph 610.992.0022 | fax 610.992.0021
www.aamga.org

October 27, 2016

Sent via email to: CyberRegComments@dfs.ny.gov

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

Attention: Honorable Maria T. Vullo, Superintendent of Financial Services

Re: *Comments to 23 NYCRR 500*: *Cybersecurity Requirements for Financial Services Companies*

Dear Superintendent Vullo:

The American Association of Managing General Agents (hereinafter also referred to as "AAMGA"), represents the wholesale agents, brokers, aggregators, program managers and administrators in the United States invested with trusted delegated binding authority from domestic and international insurance markets.[1] The membership is comprised of many small to medium entrepreneurial businesses throughout the United States, as well as the larger brokers and MGA operations.

In underwriting year 2015, the wholesale agent, broker and program members wrote a combined $31.6 billion of annual written premium. AAMGA members write both admitted and excess and surplus (E&S) lines business in New York State, of which a total of $3.56 billion in E&S premium was written in 2015.[2] Our agent and company members are very engaged in New York in securing the risks of policyholders, and appreciate all the efforts the Department makes on behalf of its citizens every year.

We write to thank you for the opportunity to provide comments in respect of the proposed regulation pertaining to cybersecurity requirements for financial service companies. We are in concurrence with the introductory comments of the proposed regulation that the threat of cybercriminals in commerce is on the rise and measures must

[1] The Association also represents members who are the domestic and international insurance companies who have afforded the delegated binding authority to the wholesalers, as well as reinsurers, captive insurers and other risk-bearing entities and business service providers. Other members also include the Excess Lines Association on New York ("ELANY") and their state stamping and surplus lines offices colleagues in the 14 other states maintaining those operations.

[2] *See*, ELANY Annual Statistics: http://www.elany.org/statistics.aspx?d=1914.

be taken to combat their rising threat. Events of the past week alone at Dyn's Domain Name System operations involving the distributed denial of service (DDoS) attack involving the Mirai botnet are emblematic of the threat occasioned by outside attackers. The proactive move by the Department of Financial Services is to be applauded. However, we are providing these comments as we respectfully disagree with the regulatory framework being proposed, and the manner of its proposed implementation.

The broad language of the proposed regulation would appear to include our wholesale agent and broker members in its compliance requirements. As also noted in Bulletin No. 2016-23 issued by ELANY, "[w]hile initial indications suggested the proposed regulation is addressed to banks and insurers, it appears from the plain language proposed that it will apply to insurance brokers and excess line brokers in both a direct and indirect manner in most instances."

The terms used in the regulations for "financial services" and "regulated entities" cast a very wide net. Similarly, the services provided under these umbrella terms can vary widely in their scope and the sensitivity of information that is involved in their day-to-day functions. For some industries, care should be given that losses of efficiency and increased cost of operation does not overwhelm the gains of security if these regulations are adopted as proposed. AAMGA members, as wholesale members of the excess and surplus lines insurance distribution network are concerned that gains will not measure up to the costs as a result of this proposed regulation and will have a chilling effect on the industry in New York.

For example, in speaking with many of our members in New York State, as well as others also writing insurance business in the state, we can confirm that the compliance costs of the proposed regulations would be extraordinary and, for some, not able to be absorbed. Most small to medium sized wholesalers do not have an internal information technology (IT) department or staff and, therefore, would need to outsource the implementation and compliance requirements. Given the comprehensiveness of the proposed regulations, IT consultants advise the cost associated with compliance may be in excess of $80,000 annually. Given the commission based nature of the insurance transaction, these added costs would either have to be absorbed by the wholesaler or, more likely, passed on to the consumer.

A wholesale insurance office by its very makeup is an aggregator of many insurance policies for insurance companies. It is doubtful any managing general agent would qualify for the small entity exemption as written because of the "and" statement at the end of the qualifiers rather than "or". Many managing general agencies do not have $5,000,000 in gross annual revenue or $10,000,000 in year-end total assets, but almost all have more than 1,000 individual policies in force. The commission retention by these offices is generally 10% on average. An average E&S policy has a $2,500 premium, which means this regulation will potentially affect an office with a gross revenue of only $250,000.

As noted, the estimated cost of implementation of the full set of regulatory requirements is exorbitant for an individual office due to technical duties such as penetration testing (*See* §500.05), and other requirements no small business owner is qualified to implement. As previously stated, it will become a decision for many businesses on whether they can simply stay in business with compliance requirements as presently written. It will also be the smaller, local New York businesses in our segment who will be more adversely impacted versus the non-domiciled national firms. This will have the unintended consequence of giving policyholders and commercial entities less options to choose from in working with wholesalers to secure their risk exposures.

Even if the small entity exemption were revised so a business that satisfied any of the three qualifications could take advantage of the exemption, wholesale managing general agencies are too tied in with their insurance companies to be able to separate themselves from the additional regulatory requirements. Under the plain language of the regulations, wholesale offices would still fall under the third-party provider of services definition, given the insurance companies they represent. This third-party relationship with a non-exempt business would subject them to compliance under §500.11, which reasserts many of the regulatory requirements that were exempted under the small entity exemption of §500.18.

In light of the impossible prospect of the cost of implementation for these businesses, our criticism of the regulations is best summarized as follows:

1. <u>The Need to Segment the Regulation</u>

The regulation should not have a blanket application to all businesses in the financial services sector. Having reviewed the proposed regulation in its entirety, we recommend the regulations be segmented by the types of businesses that are truly required to be regulated in this manner. Moreover, different financial services businesses have different exposure levels. Banks and other financial institutions have a high level of sensitive data. Managing general agent offices are on the other end of the spectrum, with most of the data internally generated for rating, and much of the other data being publicly available. However the regulations completely ignore this spectrum.

On their face the regulations, understandably, appear to be drafted for the financial services entities with the most sensitive data, creating an unrealistically high standard for compliance for the remainder of businesses. Banks and other institutions with regular access to social security numbers and health information certainly should be regulated differently than business entities that transact only with name and address information and policy numbers.

Therefore, we respectfully recommend that the regulations be segmented by industry type to better recognize the vast differences in business operations and the very need to avoid subjecting small and medium businesses – and those with little to no sensitive data – to the onerous imposition of these regulatory constraints and compliance costs.

2. **The Cost of Compliance**

It appears that the regulations have been initially drafted without an objective consideration as to the cost of implementation. We trust these comments will be able to put the grave financial impact into better perspective, and drive another examination into the overall efficacy and propriety of the regulations as presently drafted.

We note the Regulatory Impact Statement makes unsupported assumptions that there will be "some costs" to small businesses and that "a small business will not necessarily need any professional services to comply". Both of these declarations are wholly inaccurate. Speaking on behalf of those wholesale insurance entities immediately affected by these regulations, it is unrealistic to assume – or require – that a small or medium sized business owner will be qualified or able to, among other things:

- do penetration testing as delineated in §500.05;
- develop, implement and maintain a cybersecurity policy;
- manage a cybersecurity policy that requires "at a minimum" to address the 14 individual requirements as delineated in §500.03;
- manage all of the 6 various requirements comprising the audit trail as delineated in §500.06;
- perform annual risk assessments and the detailed analysis of their own network as delineated in §500.09; and
- employ additional cybersecurity personnel as delineated in §500.10

All of these services will necessarily require the cost of hiring IT and/or cybersecurity professionals to accomplish; and the costs will be not be insignificant. IT costs are some of the highest levied against small businesses and compliance with the full set of regulations will be severe.

We are also observant of the fact that the Errors & Omissions and related insurance policies of wholesale agents and brokers will need to be amended to include the various affirmative additional compliance efforts noted in the proposed regulation. In the event a breach were to occur despite these efforts having been performed, these policies would certainly be triggered. This will impose even more additional costs on wholesale agents and brokers, assuming the expanded coverages could be secured.

3. **Nonpublic Information**

The definition of "Nonpublic Information" is extremely overly broad and unduly vague. As drafted, the provision covers all information that is not Publicly Available Information, despite the four paragraphs of clarification provided. *See* §500.01 Definitions. (g)(1-4). All data stored by a business is business related, and any business related data that has been tampered with, no matter the least sensitive, will have a financial impact on that business. At minimum, the business will incur the additional cost to fix the data.

In reality, we can foresee no situation where a financial impact, however small, will not have a "material adverse impact". This broad and vague definition generally renders the subsequent paragraphs moot, because no data stored by a business will escape capture by the first paragraph. Moreover, the definition leaves no room for any data stored, received, or transmitted by any entity to fall outside the regulations requiring cybersecurity protection. As a consequence, the sweeping application of the regulations, as presently worded, serves to further increase the cost of compliance for businesses, deepening the financial impact on the industry.

Further, the seminal problem with the definition of "Nonpublic Information" is that this term is used at all in the regulations. It is too broad in its plain meaning and will subject the definition to rounds of potentially varying interpretation in legal proceedings, where the need for consistent and uniform interpretation are required.

We recommend the regulation be limited to addressing "nonpublic personal information" according to the definition supplied under the Gramm-Leach-Bliley Act, 15 USC 6801– 6827 (1999)[3], and "individually identifiable health information" as defined under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regulations[4]. These definitions are well-established and have already neem vetted by case law. Taking the definition to such an extreme as proposed in the regulations is damaging to business and will adversely impact New York businesses disproportionally.

[3] The personal information covered by the GLBA is termed "nonpublic personal information," which means "personally identifiable financial information - provided by a consumer to a financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution." The term does not include publicly available information. Regulations issued under the statute define "personally identifiable financial information" as any information: "a consumer provides to you to obtain a financial product or service from you; about a consumer resulting from any transaction involving a financial product or service between you and a consumer; or you otherwise obtain about a consumer in connection with providing a financial product or service to that consumer." Id. Those definitions are important, because the way "nonpublic personal information" is defined includes just about all information provided by a consumer or customer that is nonpublic, whether or not it appears to be particularly sensitive or confidential.

[4] "Individually identifiable health information" is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
(i) That identifies the individual; or
(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual."

See, 45 CFR 160.103.

4. **Confirmation that Non-Admitted/Alien Insurers Are Not Subject to the Regulation**

We are advised and agree that, as written, the proposed regulations are not intended to apply to Excess Line/Non-Admitted/Alien Insurers whose coverages are sold in New York through licensed excess line brokers. As our members include these insurers writing insurance policies in New York State, we will appreciate confirmation of this interpretation.

5. **Imposition of Regulation Compliance by Retail Producers**

Notwithstanding the foregoing, in respect of Excess Line/Non-Admitted/Alien Insurers presumably not being subject to the regulation, our agent and broker members also conduct business with admitted insurers who, are presumably subjected to the provisions.

Agents and brokers need to access the portals and systems of the admitted to market insurers primarily for the purposes of rating, quoting and binding risk exposures. Pursuant to the regulatory conscripts as presently drafted, admitted insurers would presumably also require agents and brokers to prove they are in compliance with the proposed regulations.

In addition, as the flow of business in the insurance transaction flows from the private consumer/commercial policyholder through a retail producer/broker and then to the wholesaler. Therefore, regardless of whether retail brokers might be expressly exempt from the regulations, wholesalers would still be required to ensure their retail producers are in compliance with the regulations as presently drafted, thereby, no longer effecting the intent of the regulations to make those retail brokers exempt. As presently written, it would be nearly impossible for wholesale agents and brokers to assess and evaluate the Cybersecurity practices of their retail customers without hiring a full time staff to do so. We do not believe the Department intended wholesale agents and brokers to undertake an investigatory or policing aspect of their retail customers.

6. **Multi-State & Out of State Operations**

Similar to the foregoing, most, if not all of the agents and brokers having operations in New York State also have operations in neighboring and other states. As noted, utilizing the retail producer distribution network, many of the retailers also exist in neighboring and other states. Under the regulations, as presently written, the wholesale agent or broker would need to insure that the out-of-state retail producer is also in compliance with the New York state regulations, whether or not they are intended to be exempted.

Further, due to the national scope of many wholesale agents and brokers with home state operations outside of New York, they also provide services and benefits to New York residents and businesses. As presently drafted, the regulations would appear to also include these non-New York state based wholesale agents and brokers under their purview. In essence, the enforcement mechanism of the Department of Financial Services would

extend to out-of-state wholesale agents, brokers and retail producers writing business in New York State for those policyholders within the state. We do not believe that was an intent of the proposed regulations and, therefore, recommend this be clarified.

7. Timing of compliance standards

In order to assure the consistency in application and enforcement, we recommend the temporal elements of various compliance provisions be amended in order to be uniform. While most of the compliance provisions in the regulations, as presently drafted, call for annual certifications, others call for compliance on less than an annual basis. These include, but are not limited to:

- the Chief Information Security Officer's (CISO) report is to be provided bi-annually, as set forth in §500.04(b); and
- vulnerability assessments of the Covered Entity's Information System is to be undertaken on a quarterly basis as set forth in §500.05(2)

In the event the proposed regulation is formally adopted, the timing of compliance requirements should be made uniform throughout the regulation, and undertaken on an annual basis.

8. Protection of Proprietary Marketing and Confidential Information

Section 500.04(b) delineates the Report to be prepared by the CISO of each Covered Entity on at least a bi-annual basis. As presently drafted, the proposed regulation requires the Report to have:

1. assessed the confidentiality, integrity and availability of the Covered Entity's Information Systems;
2. detail exceptions to the Covered Entity's cyber security policies and procedures;
3. identification of cyber risks to the Covered Entity;
4. assessment of the effectiveness of the Covered Entity's cyber security program;
5. the proposal of steps to remediate any inadequacies identified as a result of the assessment as set forth in the Report; and
6. to include a summary of all material Cyber security Events that affected the Covered Entity during the time period addressed by the report.

The section of the proposed regulation also notes that the report "shall be made available to the superintendent upon request." As most if not all of these six enumerated provisions to be included in the report are proprietary and would include information of a confidential nature, no provisions are set forth in the proposed regulations to ensure the

confidentiality of this information should a request be made by the superintendent for the Report.

Further, we are concerned as to the discoverability of and public access to such a Report by third-parties and competitors of the wholesale agent or broker in the event a cyber-security, errors or omission, directors and officers, or any other occurrence would result in litigation. Due to the broad nature of discovery rules under the Federal Rules of Civil Procedure (particularly, Rules 26 and 34), as well as those in effect in New York State (*See, e.g.*, NY Civil Practice Law and Rules §3101 Scope of Disclosure, and §3120 Discovery and production of documents and things for inspection, testing, copying or photocopying), in the event this provision of the proposed regulations should remain as stated, additional protections will need to be drafted and included in the regulations in order to ensure the confidential nature of these important and proprietary details which may come to light in any assessment undertaken by the CISO of the Covered Entity on a bi-annual basis, whether or not they are provided to the superintendent if requested.

9. **Duplicity of Compliance Requirements**

We further question the advisability of the proposed regulations in light of the fact that many wholesalers now already have in force and effect, and maintain Cybersecurity insurance for their operations. Some of the insurance markets underwriting this coverage also require some of the internal protections of the insured entity, which are also being imposed by the proposed regulations. This would appear to render the proposed regulations as duplicative in scope and nature and impose another burdensome compliance requirement upon the wholesale agent and broker, which may already have been undertaken.

In the event the proposed regulations proceed as written, we recommend the Department of Financial Services consider exempting from compliance those wholesale agents and brokers with appropriate defense and indemnification limits of liability as set forth in their Cybersecurity insurance policies. This can be accomplished by annually providing the Department with Acord 25 and 27 (if required) - Certificates of Insurance reflecting the market and limits of liability during the noted incepting and expiry dates of the policy period.

10. **Prospective Overlap with National and State Model Laws and Regulations**

As the Department of Financial Services is undoubtedly aware, the National Association of Insurance Commissioners ("NAIC") is also actively reviewing the nature and extent of Cybersecurity risks and exposures and the appropriate measures to take to circumvent potential occurrences. The Superintendent is a member of NAIC's Cybersecurity (EX) Task Force. As such, the Superintendent is also aware of the various activities of the Task Force and work being done by the NAIC staff pertaining to the data collected from the Cybersecurity Insurance Coverage Supplement of the NAIC 2015 Property/Casualty annual statement and the ongoing drafting taking place under the

leadership of Commissioner Adam Hamm of North Dakota of a NAIC Insurance Data Security Model Law.

We also attend all the meetings and conference calls of the Task Force as an industry interested party. Since the Superintendent is also a member of the Task Force, there is no need to review the various developments taking place to establish a national model act, other than to comment upon the prospective duplicative nature of the proposed regulation and any national standards which are adopted by the NAIC and then moved to the states for formal adoption by the respective legislatures.

We recommend consideration be given to delaying the adoption and implementation of any potential proposed regulatory efforts in New York State, until such time as the ongoing process of a national model act has been completed. Once the model act has been brought through the formal adoption process and moved to the respective states, the current New York proposed regulation, or various sections thereof, might well become superseded or otherwise rendered moot.

Moreover, and as stated previously, since wholesale agents and brokers operate on a multistate if not nationwide basis today, we are concerned with the prospect of various other state regulations being imposed as they may well be inconsistent with those sought to be offered in the proposed regulation here. The increased burden and expense imposed upon wholesale professionals in complying with various state standards and regulations would be exacerbated under this very probably scenario.

Conclusion and Recommendations

We respectfully believe the Department's efforts in respect of imposing Cybersecurity compliance requirements on financial services companies as presently defined while, well-intentioned, are presently premature, cost prohibitive, and overbroad in the net being cast to include entities like wholesale agents and brokers, retail producers and other non-risk-bearing entities.

Unlike banks and other financial institutions, we are unaware of any wholesale agents or brokers storing the type of personal financial data of policyholders whose risk exposures are secured through the process of the insurance transaction, and which seem to lie at the foundation of the Department's proposed regulation. Moreover, while many offer online premium payment opportunities, most of these services utilize 3rd party vendors who have trust certificates already in place.

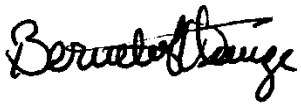
As presently written, the proposed regulations would not only seriously impact the ability of wholesale agents and brokers to provide the trusted services to their customers as well as policyholders, but also impose financial hardships which will dramatically impact their operations. At a time when private and commercial policyholders continue to rely upon the trusted services of wholesale agents and brokers to ensure their risk exposures are properly being secured with proper markets, this proposed regulation will have substantial

adverse consequences which, unfortunately, may cause some wholesale professionals to no longer be able to competitively conduct business within New York State.

Given the Superintendent's and Governor's public statements and commitments to make the Empire State a friendly one within which to do business, as well as the emphasis that has been placed on improving the small business climate, we respectfully suggest the proposed regulation be re-examined in regard to its necessity at this time given the matters outlined above, as well as its broad and over encompassing impact on wholesale agents and brokers.

We will be pleased to provide any further details or information on the matters advised above, or respond to any questions the Department may have. We will also be pleased to work with the Department on any opportunities to make the regulation more appropriate in achieving its intended purpose. In the meantime, we sincerely appreciate the courtesy of being given the opportunity to provide comments on the manner in which the proposed regulation will impact the wholesale agent and broker community.

Respectfully yours,



Bernd G. Heinze
Executive Director

cc: Dan Maher - Excess Lines Association of New York