ELANY
EXCESS LINE ASSOCIATION OF NEW YORK
One Exchange Plaza / 55 Broadway (29th Floor)
New York, New York 10006-3728
Daniel F. Maher
Executive Director

VIA EMAIL AND REGULAR MAIL

October 31, 2016

Cassandra Lentchner
Deputy Superintendent for Compliance
NYS Department of Financial Services
One State Street
New York, New York 10004

Re: Proposed Regulation 23 NYCRR 500 – Cybersecurity Requirements For Financial Services Companies

Dear Ms. Lentchner:

The Excess Line Association of New York ("ELANY") appreciates the opportunity to comment on the Proposed Regulation titled "Cybersecurity Requirements For Financial Services Companies" (23 NYCRR 500) specifically, as it relates to New York licensed insurance producers both resident and non-resident.

I. PRODUCERS ARE BOTH "COVERED ENTITIES" AND "THIRD PARTIES DOING BUSINESS WITH A COVERED ENTITY."

Each New York Insurance Producer is a "Covered Entity" as defined in Section 500.01(c). Section 500.11 requires each covered entity to ensure the security of Information Systems of "third parties doing business with a Covered Entity."

Small to medium size insurance producers doing business with 10 to 20 insurance companies will be required to implement separate and varying cybersecurity requirements adopted by each insurer subject to this regulation. Indisputably, this will be a very heavy burden for each insurance producer separate and apart from the producer's own obligations as a "Covered Entity."

The limited exemption in Section 500.18 offers no relief to insurance producers as "Third Parties," who will be required to meet insurer imposed cybersecurity policies.

A Covered Entity has 180 days from the regulation effective date to comply. If insurers use 175 days to develop and initiate a plan, how can insurance producers possibly comply? The answer is it is highly unlikely insurance producers will be in a reasonable position to comply with last minute dictates by multiple insurers implementing procedures that will vary from insurer to

dmaher@elany.org
www.elany.org
phone 646-292-5500
direct line 646-292-5555

insurer. Insurance producers which simultaneously attempt to meet these requirements as a "Covered Entity" will find it incredibly difficult to reconcile insurer mandates with the producer's own cybersecurity plan.

Recommendation #1 – Amend the Proposed Regulation to provide that New York licensed insurance producers, who meet the cybersecurity policies of each insurance company, "Covered Entity" with whom it does business, are deemed to have met the requirements of the cybersecurity regulation. Additionally, at the very minimum, the Section 500.18 exemption standard should be much broader and apply to entities larger than those currently proposed that have a significant volume of New York business given the cost and scope of the Proposed Regulation.

Recommendation #2 – New York licensed insurance producers should be provided significant additional time to comply, at least 180 days beyond the compliance deadline for insurers subject to the Proposed Regulation.

II. ALL REGULATION, INCLUDING CYBERSECURITY REGULATION, NEEDS TO BE COORDINATED FOR CONVERGENCE AND UNIFORMITY ULTIMATELY.

While there is no doubt that cybersecurity is absolutely necessary in today's technical business world, as noted below, the costs to a "Covered Entity" to comply with this one single regulation will be unprecedented.

This single regulation with mandates requiring penetration testing, encryption, hiring of "sufficient" personnel, "regular" training, "periodic assessment" and "annual" and other mandatory reporting is just one additional layer of cybersecurity law or regulation for many of these covered entities.

Beginning in 1974, Congress first addressed data security with the 1974 Privacy Act. Since then, privacy and/or cybersecurity has been addressed in GLBA, HIPAA, FCRA, CAN-SPAM and the Cybersecurity Act of 2015 by the federal government just to name some. At least seven federal agencies maintain some level of jurisdiction and enforcement over privacy and cybersecurity; at least forty-seven states have enacted breach notification statutes. New York has Insurance Regulation 173, which also applies. In the meantime, the NAIC and various international bodies are taking action and making recommendations regarding data privacy and cybersecurity.

The trouble for covered entities is that compliance is expensive to begin with and nearly impossible to achieve when one authority chooses to add another layer of regulation without considering the need for coordination and convergence with an ultimate goal of uniformity or near uniformity in compliance standards. Using existing definitions from existing law, rather than new definitions such as 500.01 Nonpublic Information, would be a good start.

Recommendation #3 – **Consider adopting safe harbors recognizing compliance with other existing standards are sufficient to meet some or all of the requirements of this new Proposed Regulation.**

Recommendation #4 – **Coordinate New York efforts with other regulatory bodies to prevent new regulations from overlaying existing regulations or other proposed requirements on the cusp of being adopted.**

III. IMPROVE DEFINITIONS AND SCOPE OF REGULATION

In some cases, the definitions or scope of the Proposed Regulation make it quite difficult to determine what actions will constitute compliance. For example:

500.10 – a Covered Entity must...

... employ sufficient personnel

... provide...regular cybersecurity update and training sessions

... stay abreast of changing cybersecurity threats and

500.14 (a) (2) ... provide for and require all personnel to attend regular cybersecurity awareness training sessions...

These requirements are both prescriptive and vague at the same time. They are prescriptive in that they mandate levels of training and assume that there are parties, courses or a volume of professional trainers with off-the-shelf courses that will truly meet the intended goal of improving cybersecurity. These same standards are unduly vague containing subjective standards such as "sufficient" and "regular" and "staying abreast of changing threats." It would appear those that suffer a cybersecurity breach, based upon these definitions, may automatically be deemed to have not complied with the Proposed Regulation by virtue of the breach. By way of example, if you suffered a breach, you did not employ "sufficient" personnel. Moreover, the insurance industry recognizes the threats of cyber attacks and has certainly moved to establish security by investing in systems and personnel to protect itself. Standards of this nature to address a quickly evolving threat may do more harm than good. The industry may be in a better position to recognize the threats to which they, as individual entities, are most susceptible and allocate resources accordingly as opposed to the mandatory allocation of resources dictated by this Proposed Regulation.

Recommendation #5 – **Consider adopting definitions and protocols that already exist in other laws rather than 1) adopting additional protocols and 2) redefining existing terms and standards.**

Recommendation #6 – **Add a provision at 500.03 (a) (15) requiring the Cybersecurity Plan to address staffing, training and education and delete the definitions and requirements noted above.**

IV. CONSIDER THE NEGATIVE IMPACT ON THE INSURANCE MARKETPLACE CAUSED BY THE COST TO COMPLY

There are insurance producers, who will not meet the proposed 500.18 Exemption standard who are nevertheless small family owned businesses that are currently not profitable or marginally profitable. The cost to a small business to comply with the hiring, training, intrusion testing, encrypting and other prescriptive requirements of the proposed regulation are reasonably estimated to be $500,000 in the first year and $250,000 annually thereafter. For a small business with just over $5,000,000 in annual revenues, this could exhaust the profits that would have otherwise been earned. These costs are likely to recur annually.

Implementing encryption at this time will be extremely costly and seriously challenging, even with the most advanced technological support.

Recommendation #7 – Delete or significantly delay the requirements to encrypt data.

Thank you for the opportunity to comment.

Excess Line Association of New York

By

Daniel F. Maher
Executive Director