NEW YORK

PROFESSIONAL INSURANCE AGENTS

25 CHAMBERLAIN ST.
P. O. BOX 997
GLENMONT, NY 12077-0997
(800) 424-4244
FAX: (888) 225-6935
WEB: www.pia.org
E-MAIL: pia@pia.org

Memorandum re: Proposed Second Amendment to 23 NYCRR

PIANY respectively submits the following comments on the Department of Financial Services' proposed Second Amendment to 23 NYCRR

The Professional Insurance Agents of New York State Inc., an association of independent insurance agents throughout the state and their employees, would like to thank the New York State Department of Financial Services for the opportunity to submit comments on the department's proposed second amendment to 23 NYCRR 500. Since the enactment of the 23 NYCRR 500 in 2017, it has been a mission of PIANY to educate insurance producers about the importance of sound cyber security practices. In the five years since the implementation of 23 NYCRR 500, PIANY has provided insurance producers in New York and neighboring states with resources and education on the topic. PIANY legal staff have fielded hundreds of questions about the regulation and assisted numerous producers with compliance. Based on feedback from PIANY's Government Affairs Committee and PIANY members-at-large, as well as the association's experience with 23 NYCRR 500, PIANY respectively submits the following comments on the Department of Financial Services' proposed Second Amendment to 23 NYCRR 500:

Provide one-year compliance window for data retention and creation of business continuity and disaster recovery plans.
The second amendment to 23 NYCRR 500 includes several new requirements that while furthering the goal of sound cyber security protections, could present challenges to covered entities in trying to timely comply with these new requirements.

Amendments to 500.13, which relate to data retention, would now require all covered entities to develop written policies and procedures designed to ensure that covered entities maintain a complete asset inventory of their information systems and components.

500.16(a)(2) would require the development of a business continuity and disaster recovery plan. Creation of that plan includes several time-intensive steps including the identification of documents, data, facilities, infrastructure, personnel and competencies essential to the continued operations of the covered entity's business and the supervisory personnel responsible for implementing each aspect of the business continuity and disaster recovery plan.

PIANY is supportive of both changes but requests that covered entities be given additional time to comply with both Subsubsections 500.13(a) and 500.16(a)(2).

Currently, covered entities would be required to comply with both of those subsections within 180 days of the finalization of the regulation. PIANY is concerned that this would not provide covered entities with enough time to comply. Covered entities will need time to be educated on the changes to the regulation, to prepare

- continued -

and adopt the appropriate policies and procedures, to implement an asset inventory and BCDR and time to complete the asset inventory and BCDR.

The amount of time that is needed to fully educate producers on even the smallest changes to the Insurance Law cannot be understated. PIANY is still educating members on the requirements of the original regulation. It will take time to educate and prepare covered entities to comply with these new requirements. PIANY recommends adding both 500.13(a) and 500.16(a)(2) to proposed subdivision 500.22(d)(2), which provides a one-year implementation date for certain sections of the regulation. Providing an additional 180 days will help increase compliance with these very important requirements.

Exempt "inactive brokers"
PIANY would like to thank the department for adding language to 500.19(f) that exempts insurance agents who are deemed inactive under Banking Law Section 599-1 from the requirements of 23 NYCRR 500. PIANY has long advocated for inactive producers to be excluded from the requirements of this regulation. Inactive producers, while holding a license, do not handle any personally identifiable information. As such, many of the requirements of 23 NYCRR 500 are not applicable to them and would be impossible to comply with. To ensure all inactive producers may qualify for this exemption, PIANY would ask that this exemption be expanded to include insurance brokers. While there is no "inactive broker" statute as there is for insurance agents, PIANY supports adding language to allow inactive brokers to apply for exempt status but prevents an inactive broker who becomes active from applying for another exemption for a period of at least 12 months from the date the broker files a new exemption status. Adding such language would allow authentic inactive brokers to take advantage of the exemption, while minimizing the ability of covered entities to abuse the exemption by opting in and out multiple times over the year.

Remove written acknowledgement of non-compliance
PIANY has concerns over new requirements added to Section 500.17 addressing notices to the superintendent. The second amendment adds a new Subsection 500.17(b)(1)(ii) that requires covered entities who cannot demonstrate compliance with the regulation to file a written acknowledgement with the department of that fact, and identifies all the areas, systems and processes that require improvement. PIANY is concerned that this requirement could present an unnecessary security risk. If cyber criminals were to successfully breach the department's information system, they could get access to information that would highlight all the cyber security weak points of covered entities. PIANY asks that 500.17(b)(1)(ii) be removed to avoid this potential threat.

Clarification on removal of employee third-party exemption
PIANY seeks clarification on one change to the regulation. Section 500.11(c) was removed in the amendment. That subsection exempted employees of covered entities, who themselves are covered entities, from developing their own third-party information security policy. This was a common-sense exemption that recognized that employees of covered entities would be covered by their employer's policies. Requiring employees to create their own plans would be redundant and inefficient. Employers would either replicate their employer's plan or create their own unique plan,

- continued -

which would prove challenging to implement and enforce. Section 500.19(b), which was unchanged in the proposed second amendment, already exempts employees of covered entities from the requirements of 23 NYCRR 500, which would include the third-party information security policy. Given the logistical issues associated with the removal of the 500.11(c) exemption, PIANY would like to confirm that employees of covered entities would still be excluded from the requirements of 500.11 by virtue of their exempt status under 500.19(b).

Once again, PIANY would like to thank the department for the opportunity to comment on the proposed second amendment to 23 NYCRR 500. PIANY looks forward to working with the department on this critical regulation.

8/22