BIG I | NEW YORK

DATE: August 18th, 2022

TO: Joanne Berman, Counsel to NYSDFS Cybersecurity Division

FROM: Scott Hobson, Assistant Vice President of Government Relations, Big I NY

RE: New York State Department of Financial Services Pre-Proposed Outreach
Potential Amendments to 23 NYCRR 500, *Cybersecurity Requirements for Financial Services Companies*

Joanne,

Thank you for the opportunity to provide comments on the proposed draft second amendment to 23 NYCRR 500. Our initial comments are as follows:

1. **RE: Changes to limited exemption:**
   a. The proposed increase in threshold of employee count and assets to qualify for the limited exemption is welcome and reasonable.
   b. We suggest the revenue threshold also be raised correspondingly, for example to $10 million in New York income.
   c. We recommend "Independent Contractors" include only those contractors who have access to the covered entity's NPI. For example, outside accounting firms, law firms, landscaping and maintenance contractors, etc. should be excluded from this count.
2. **RE: exemption for inactive licensees in subdivision (f):**
   a. We believe this is reasonable and will be a welcome relief for retired insurance producers who continue to maintain their license.
   b. This exemption should also include brokers in addition to agents.
3. **RE: Changes to risk assessments:**
   a. In 500.1(k): We believe "image, and reputation" risks to organizational operations should be removed from the risks a covered entity is *required* to identify in their risk assessments. While these are factors that many prudent covered entities will wish to consider, they should be voluntary.
   b. In 500.9(c), recommend "The risk assessment shall be updated at least annually, <u>unless there have been no material changes to the covered entity's cyber risk."</u>
4. **RE: Changes to third-party service providers:**
   a. The removal of "non-governmental" from the definition of "person" means that governmental entities would become "third party service providers" upon which covered entities will have to perform due diligence. This will prove extremely burdensome for independent insurance agencies and brokerages and create challenges if a governmental entity is not forthcoming about its cybersecurity practices. Realistically, insurance agents and brokers have no meaningful ability to cease doing business with or demand changes by the governmental entity (for example, FEMA or the

NYS Insurance Fund), nor is it clear how insurance agents and brokers conducting due diligence on government entities will meaningfully enhance cybersecurity.

b. We believe 23 NYCRR 500 should be amended to make clear that covered entities are not considered third party service providers, as is the case with the NAIC model cybersecurity law now adopted in 21 states. The current state of the regulation, in which agents and insurance carriers must effectively “cross police” each other’s data security standards is unduly burdensome and ineffective. We believe the rationale for this change is even stronger now in light of the widespread adoption of the NAIC model law and the currently proposed amendments to 23 NYCRR 500.

5. **RE: Certification of non-compliance by covered entities 500.17(b)(1)(ii)**

a. We believe this requirement should not be included as it will create a substantial cybersecurity risk. Requiring covered entities to document noncompliance and identify specific areas of vulnerability will put NYSDFS in possession of a list of prime targets for cyberattack or extortion, which bad actors will seek to access and exploit. Government entities are frequently the target of cyberattack, as underscored by recent cyberattacks against the NY Joint Commission on Public Ethics and also the New York City Law Department.

6. **RE: Prohibited Acts in 500.20**

a. 500.20 (a) (2) should be limited to “intentional” failure to comply and the time period increased to 72 hours.

7. **RE: Vulnerability processes**

a. The amendment refers to three distinct vulnerability-related processes: “vulnerability analyses” (500.9); vulnerability and patch management (500.3); and vulnerability assessment (500.5). Further clarification is needed as to how these various processes differ from each other.