NATIONAL ASSOCIATION OF PROFESSIONAL INSURANCE AGENTS

Local Agents Serving Main Street America℠

May 16, 2017

The Honorable Raymond G. Farmer
Chair, NAIC Cybersecurity (EX) Working Group

The Honorable Elizabeth Dwyer
Vice Chair, NAIC Cybersecurity (EX) Working Group

National Association of Insurance Commissioners
444 N. Capitol Street, NW, Suite 700
Washington, DC 20001

Submitted via email: Eric Nordman enordman@naic.org
Sara Robben srobben@naic.org

Re: Proposed Version 4 of Insurance Data Security Model Law

Dear Director Farmer and Superintendent Dwyer:

On behalf of the National Association of Professional Insurance Agents (PIA)[1], I want to again express our thanks for your patience as we have worked together to identify common ground on the aforementioned draft model law. We appreciate having been included in the Drafting Group and regulators' engagement with members of industry throughout this process. We appreciate the spirit of cooperation exhibited by the Drafting Group's regulatory members and by the National Association of Insurance Commissioners (NAIC) staff who have worked so hard to produce a model that stakeholders with a variety of perspectives and competing interests may support.

I hereby submit the following comments in response to the NAIC Cybersecurity Working Group's April 26, 2017 Draft of the Insurance Data Security Model Law (Draft #4) (herein referred to as "Draft #4").

First, we are particularly gratified to see the scope of the model has been substantially narrowed in Draft #4 and that Section 9 of the draft exempts licensees with under 10 employees from compliance with Section 4; this exemption acknowledges the limited resources available to the smallest of small insurance businesses. However, we remain concerned about the definition of "Cybersecurity Event," the licensees' obligations as they

[1] PIA is a national trade association founded in 1931 that represents member insurance agents in all 50 states, Puerto Rico, Guam, and the District of Columbia. PIA members are small business owners and insurance professionals who can be found across America.

pertain to the activities and potential liabilities of third-party service providers, the timeframe given in which to provide notification to the relevant commissioner of a "Cybersecurity Event," the limited scope of the aforementioned exemption, the effect of compliance with the recently-issued New York State Department of Financial Services (NYSDFS) Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York (23 NYCRR 500) on compliance with this model, and the scope of commissioner authority granted by Draft #4.

PIA is pleased to be continuing our work with the NAIC on this important issue. However, Draft #4 is not an improvement over the existing patchwork of state laws, and, as such, without substantial revision, we will be unable to support Draft #4 within the NAIC process or at the state legislative level. Having said that, if passage by the Working Group of Draft #4 or similar will be the inevitable conclusion of this process, we encourage the Working Group to engage in a comprehensive evaluation of the specific provisions of Draft #4. In furtherance of that effort, we offer the following comments and recommendations.

1. **Definition of a "Cybersecurity Event"**

The definition of "Cybersecurity Event" as set forth in Section 3C is overly broad and therefore unworkable. It defines a "Cybersecurity Event" as "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System."

On its face, this definition would include receipt of communications like phishing emails, irrespective of whether the recipient is taken in or any information is garnered by such emails. Any licensee would be challenged by the logistics of reporting to commissioners every time an employee receives a phishing email, and commissioners of insurance departments around the country would be overwhelmed by the sheer volume of reports they would receive from licensees if this broad a definition is approved. If the goal of the model is to provide commissioners with notice when the information systems of licensees are or may be about to be breached so that commissioners can react swiftly and effectively, that goal will be completely unachievable using this definition.

This language has its origins in 23 NYCRR 500, and we have heard Superintendent Vullo of the NYSDFS state verbally that her intent was not to require licensees to report receipt of phishing emails or similar inconsequential events. However, the language of both the New York law and Draft #4 imparts a requirement on licensees to do just that. To avoid further confusion on this issue, we recommend that the definition of "Cybersecurity Event" be modified to accurately require commissioner notification of the types of "Cybersecurity Events" commissioners expect the law to cover.

2. Licensees' Obligations Regarding Activities and Potential Liabilities of Third-Party Service Providers

Our biggest concern relates to the treatment of licensee relationships with third-party service providers. This issue arises in a few different areas, beginning, most notably, with Section 4F, Oversight of Third-Party Service Provider Arrangements.

To begin, it is unclear which Licensee will be responsible when a third-party provider experiences a "Cybersecurity Event." If an agent and a carrier pass consumer information back and forth through a third-party agency management system, and that third-party system is subjected to a "Cybersecurity Event," it is unclear whether the agent, the carrier, or some combination thereof will be responsible for communicating with the third-party service provider in the aftermath of that event. This ambiguity could be resolved with a change to the definition of "Licensee" and "third-party service provider" (found in Sections 3G and 3K, respectively).

According to Section 4F, Licensees are required to exert extraordinary authority over third-party service providers. For example, Section 4F(1)(b) requires Licensees to "[address] [m]inimum cybersecurity practices required to be met by such Third-Party Service Providers in order for them to do business with the Licensee." We have a number of concerns about this provision.

First, small-business Licensees in particular out of necessity frequently enter into what are known as "contracts of adhesion." Large companies serving as third-party service providers are going to be reticent to change their cybersecurity practices to reflect compliance with laws that only apply to Licensees. Small-business Licensees rarely have the opportunity to negotiate the details of their relationships with relatively large third-party service providers. Therefore, many Licensees will be subjected to whatever cybersecurity practices the third-party service provider already offers, whether or not those practices meet the standards set forth in Draft #4 applicable to Licensees.

Sections 4F(1)(c) and (d) are ambiguous and unnecessarily burdensome; Licensees do not have a clear means by which to "evaluate the adequacy of cybersecurity practices of such Third-Party Service Providers," nor is it clear how they would carry out "[p]eriodic assessment[s] of such Third-Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices."

Additionally, Section 5C requires Licensees to enforce the provisions of Section 5B against third-party service providers. This provision would be difficult to enforce because it requires Licensees to ensure that a third-party service provider with which it does business not contractually shift its obligations pursuant to Section 5B back to the Licensee. Again, our concerns arise out of the likelihood that many such arrangements constitute contracts of adhesion between small-business Licensees and large third-party service providers. One alternative might be to require the Licensee to simply "document," rather than "confirm and document" that the third-party service provider has adhered to Section 5B.

Finally, Section 6D(1) requires Licensees to treat "Cybersecurity Events" that occur in third-party service provider systems the same way it would treat a "Cybersecurity Event" in its own system, in accordance with Section 6A. This directive poses several problems, not least of which is the fact that Section 6A requires the Licensee to notify the commissioner within 72 hours of determining that a "Cybersecurity Event" has occurred. It would also require a Licensee to hazard what would, at best, be a guess of the number of consumers in the state affected by the "Cybersecurity Event" that has occurred in a third-party service provider system. That initial guess, likely to be inaccurate even if the "Cybersecurity Event" occurred within the Licensee's own system, would be due within 72 hours, as previously noted.

3. Timeframe in Which to Notify Relevant Commissioner

Pursuant to Section 6A, if a small-business Licensee experiences a "Cybersecurity Event," it must notify its commissioner within "72 hours from a determination that a Cybersecurity Event has occurred…", regardless of the resources available to the Licensee to do so. This timeframe is even shorter than the three (3) business days provided for in the previous draft, with which we also disagreed. Seventy-two hours, particularly without regard for when during a seven-day week those hours occur, would pose an extreme hardship to a Licensee. The level of detail sought to be provided to the commissioner in those 72 hours, as outlined in Section 6B(1)-(13), is burdensome and gives rise to substantial concerns about the practical workability of these provisions.

Section 6B(9) is particularly burdensome; it requires the Licensee to provide the Commissioner with "[t]he number of total Consumers in this state affected by the Cybersecurity Event." While generally Section 6B acknowledges that the provision of the listed information will be an ongoing process as information becomes available, with regard to Section 6B(9) specifically, the Licensee is directed to "provide the best estimate in the initial report to the commissioner and update this estimate with each subsequent report to the Commissioner pursuant to this section." Requiring Licensees to hazard a guess as to how many consumers are affected in a state within 72 hours of a "Cybersecurity Event" will prove unworkable for small Licensees.

Many small insurance agencies do not have a full-time IT staff member. It could take substantially longer than 72 hours for a part-time IT staff member to acquire sufficient information about a "Cybersecurity Event" to provide a commissioner with even the most minimal details (date, description, and means of discovery) of the "Cybersecurity Event."

We urge the Working Group to adopt a timeframe of at least 60 days in which to notify the commissioner and would welcome additional language that specifies that the Licensee must act "as expeditiously as possible and without unreasonable delay."

4. Scope of Small-Business Exemption

As noted above, we recognize and appreciate that Section 9 of Draft #4 exempts licensees with under 10 employees from compliance with Section 4; this exemption acknowledges the

limited resources available to small businesses. Having said that, we remain gravely concerned about the burden our small member agencies will face pursuant to Draft #4, even with the new language. We continue to be concerned about the overly broad definition of "Licensee," the potentially competing interests of licensees of different sizes and with different business objectives, and the practicalities associated with such scalability issues.

Additionally, the definition of "Licensee" (Section 3G) groups into one category insurance businesses of all sizes and purposes; a 10-person insurance agency would be treated the same way as a multibillion dollar insurance carrier with an employee roster in the thousands. PIA's membership is largely made up of small agencies, which will be unfairly burdened by the requirements of Draft #4. This encumbrance is exacerbated by the manner in which small entities are grouped together with large ones, with the same draconian requirements imposed on all. Insurance agencies, like carriers and other types of Licensees, come in all shapes and sizes, with all levels of sophistication and resources, financial and otherwise.

A small business would be unduly burdened by the requirements set forth in Section 5. A small-business insurance agency may not have sufficient resources to discover even that a "Cybersecurity Event" *may have* occurred until months or years after its occurrence. It may not have the resources to assess the scope of the incident, let alone identify the information that may have been compromised or determine whether the information was taken without authorization.

Section 4C, Risk Assessment, instructs Licensees to "[d]esignate one or more employees or an outside vendor and/or service provider designated to act on behalf of the Licensee who is responsible for the Information Security Program." (See Section 4C[1].) Many Licensees may have scarce resources to hire outside help to execute these directives. This problem also exists with regard to Section 4D(3), which requires Licensees to "include cybersecurity risks" in their enterprise risk management processes.

To help ease the burden on small insurance agencies, we urge the Working Group to enlarge the exemption to include Licensees with fewer than 25 employees, those with less than $5m in gross annual revenue, or those with less than $10m in year-end total assets.

5. Effect of Compliance with 23 NYCRR 500 on Compliance with Draft #4

The Drafting Group call on May 9 left us with the impression that the intent of the drafters is for Licensees who are already subject to 23 NYCRR 500 to be compliant with the model law without the need for additional steps to be taken. We encourage the Working Group to include a drafting note to that end to alleviate concerns among Licensees subject to the already burdensome New York law will not be further encumbered by new obligations pursuant to the model.

6. Commissioner Authority

Finally, Section 12 provides that the commissioner may issue whatever regulations are necessary to carry out the provisions of the Act. This broad latitude to create other rules and regulations as the commissioner deems necessary undermines the uniformity sought by the Working Group. Moreover, the grant of such authority to commissioners will simply transfer state-by-state inconsistencies from the statutory level to the regulatory level and reinforce the patchwork of state laws and regulations this effort has been attempting to ameliorate.

PIA recognizes and appreciates the considerable thought and effort that the NAIC's Cybersecurity Working Group and attendant Drafting Group have given to this issue, and we are grateful for the opportunity to again provide the independent agent perspective. Please contact me at laurenpa@pianet.org or (703) 518-1344 with any questions or concerns. Thank you for your time and consideration.

Sincerely,

Lauren G. Pachman
Counsel and Director of Regulatory Affairs
National Association of Professional Insurance Agents

CC: Eric Nordman & Sara Robben