NATIONAL ASSOCIATION OF PROFESSIONAL INSURANCE AGENTS

Local Agents Serving Main Street America℠

July 31, 2017

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

The Honorable Elizabeth Kelleher 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 5 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.

I hereby submit the following comments in response to the NAIC Cybersecurity Working Group's July 7, 2017 Draft of the Insurance Data Security Model Law (Draft #5) (herein referred to as "Draft #5"). We have a number of concerns with this draft, not least of which is the apparent intent of the Working Group to vote on it at the National Meeting in Philadelphia, one week from today. We also recognize that the Working Group has requested that our comments be limited to changes that have been made in this draft as it compares to Draft #4. Our substantive concerns will focus mainly on our numerous objections remaining unaddressed in Draft #5, as our voluminous previous expressions of same remain largely unacknowledged.

First, while we are pleased that Draft #5, like Draft #4, exempts licensees with under 10 employees from compliance with Section 4, we remain concerned about the definition of

[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.

"Nonpublic Information" (Section 3K), Licensees' obligations as they pertain to the activities and potential liabilities of Third-Party Service Providers [primarily addressed in Sections 4D(2), 4F, 5C, and 6D], the very short timeframe in which to provide notification to the relevant commissioner of a "Cybersecurity Event," the limited scope of the aforementioned exemption, the number of consumers affected by a Cybersecurity Event to trigger notification to the applicable commissioner, the effect of compliance with the 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 inconsistent language in Section 13.

PIA is pleased to be continuing our work with the NAIC on this important issue. However, Draft #5 is not an improvement over the existing patchwork of state laws, and, as such, without substantial revision, we will be unable to support Draft #5 within the NAIC process or at the state legislative level. Having said that, if passage by the Working Group of Draft #5 or similar will be the inevitable conclusion of this process, we encourage the Working Group to fully engage in a comprehensive evaluation of Draft #5 in advance of any vote on its merits. In furtherance of that effort, we offer the following comments and recommendations.

1. **Definition of Nonpublic Information**

Section 3K defines "Nonpublic Information" in a convoluted way in part by identifying it as the opposite of its opposite, or "information that is not Publicly Available Information." Cross-referencing it with the definition of Publicly Available Information (Section 3M) reveals that, to identify information that is, in fact, not publicly available, a Licensee must determine whether such information is "of the type that is available to the general public," whether the Consumer has the authority to request said information be kept private, and whether the Consumer has made such a request of the information at issue.

A clearer option might be to use the definition of "Nonpublic Personal Information" as provided in the Gramm-Leach-Bliley Act (15 U.S. Code 6809), for example.

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

Our next concern, which we have noted in the past and renew here, relates more broadly 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 3I and 3P, 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 in certain states and to certain 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 #5 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 will 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.

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 home-state commissioner within "72 hours from a determination that a Cybersecurity Event has occurred…", regardless of the resources available to the Licensee to do so. Introduced in Draft #4, this timeframe is even shorter than the three (3) business days provided for in Draft #3, 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, particularly small businesses. 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. Number of Consumers Affected by Cybersecurity Event

Because of the burdens Draft #5 will impose on small-business Licensees, which are described in greater detail elsewhere herein, we recommend that Section 6A(2) be amended to increase the number of Consumers affected by a Cybersecurity Event from 250 to 500 before notification of the relevant commissioner is required as described elsewhere in Section 6A.

5. Scope of Small-Business Exemption

Section 9 of Draft #5 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 #5, even with this language. One minor wording change that could substantially ameliorate our concerns would be to add "in this State" to modify "Licensee" in

Section 9A(1), as in, "A Licensee in this State with fewer than …" Agencies with agents licensed in more than one state would be required to comply with the requirements only of the state in which the Licensee is located. This would also mitigate our lingering concern about the potential for the model to be adopted with small but significant differences across the states and the possibility that Licensees would be subject to an array of potentially inconsistent state insurance data security laws.

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 3I) 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 #5. 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.

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. This class of exceptions would match the exempted class identified in the existing New York regulation on the subject, 23 NYCRR 500.

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

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.

7. **Inconsistent Language in Section 13**

The second sentence of Section 13 provides Licensees with one year to implement "Section 4" and two years to "implement Section 4F." As Section 4F is a subset of Section 4, Section 13 thus reads as though Licensees have both one year and two years to implement Section 4F. We recommend that this language be amended as follows. The second sentence should read, "Licensees not excepted pursuant to Section 9 shall have one year from the effective date of this Act to implement all of Section 4 other than Section 4F of this Act, and two years from the effective date of this Act to implement Section 4F of this Act."

Additionally, we urge the Working Group not to rush to vote on Draft #5 at the Philadelphia National Meeting without fully appreciating its implications, both intended and unintended. We understand the tremendous demands on commissioners' time, and only a week will pass between the comment deadline of July 31 and the Working Group's in-person meeting. We thus fear that commissioners will not have the chance to fully evaluate the comments and may be unable to bring that evaluation to bear when it comes time for them to vote.

Finally, we understand that there is some discussion of eventually making this model law an accreditation standard, and we appreciate this opportunity to express our serious reservations about that possibility.

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