NATIONAL ASSOCIATION OF PROFESSIONAL INSURANCE AGENTS

Local Agents Serving Main Street America℠

April 17, 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: Questions Raised at Denver Meeting of the National Association of Insurance Commissioners' (NAIC) Cybersecurity Working Group

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 additional comments in response to the National Association of Insurance Commissioners' (NAIC) Cybersecurity Working Group's February 27, 2017 Draft of the Insurance Data Security Model Law (Draft #3) (herein referred to as "Draft #3"). The following comments will be responsive only to the new issues raised by the Working Group during the Denver meeting and about which comments were invited. Those two issues are first, whether to model the next draft of the NAIC's Insurance Data Security Model Law on 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), which went into effect on March 1 of this year; and second, whether to bifurcate the issues of data security and data breach and thereby limit the NAIC model law to the issue of data security only.

[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.

Incorporated by reference herein and via attachment hereto are the prior comments filed by PIA National concerning Draft #3.

As noted in our earlier comments, we appreciate regulators' efforts to address some of the concerns raised throughout this process and recognize that Draft #3 reflects those efforts, to varying degrees. However, Draft #3 still leaves us with a sizeable number of serious reservations, which are outlined in our previous comments.

The two issues raised here are the incorporation of 23 NYCRR 500 and the limitation of the scope of the NAIC model to the issue of data security only. PIA National supports, with some reservations, the inclusion of some features of 23 NYCRR 500; those features will be identified below. PIA National supports without reservation the idea of narrowing the scope of the NAIC model to address only data security (tasks licensees would be asked to complete pre-breach). We discuss each item in turn.

1. **Bifurcation of Pre- and Post-Breach Issues**

During the Denver meeting of the Cybersecurity Working Group, Director Farmer raised the possibility of narrowing the scope of the insurance data security model law to address pre-breach requirements of licensees and excise from the next draft the post-breach requirements. We understand the Working Group's intent is to produce a fourth draft of the model law soon after the April 17 comment deadline. PIA supports this reduction in the scope of the Working Group and Drafting Group's work as we anticipate the content of the forthcoming draft.

We had a number of grave concerns about the data breach requirements set forth in Draft #3 and may be more likely to support the final NAIC model if it is limited in scope to data security only. While reaching consensus on data security provisions may be challenging, the last two months have demonstrated that the differences among stakeholders on Draft #3 as a whole are virtually intractable.

Using Draft #3 as a model, then, this bifurcated approach would necessitate the elimination of Sections 5-7. We recommend the elimination of Sections 8 and 9 as well, as those give power to commissioners that are redundant with their existing authority. A bifurcated approach would likely include Draft #3's Sections 1-4 and 10-14 or revised equivalents thereto. In Section 3, subparts C-E (definitions of Consumer Reporting Agency, Data Breach, and Data Breach Without Use of Personally Identifiable Information, respectively) would be eliminated as unnecessary, as might some other definitions, depending on the content of the remaining sections.

Regarding the surviving sections of Draft #3, we remain concerned about the broad definition of "Licensee," as well as the scalability of the data security requirements and the scope of authority licensees are expected to exercise over third-party service providers. For further information on those concerns, we refer you to our March 14 comment letter (attached).

With that understanding, the remainder of our comments will focus on the most significant elements of 23 NYCRR 500 for independent insurance agents with regard to data security only.

2. <u>23 NYCRR 500</u>

a. Definition of "Covered Entity." In the New York regulation, the definition of "covered entity" includes agents with nonresident licenses. This definition is overly broad and would, if adopted as part of the NAIC model, encompass licensees in states that have not adopted the model or have adopted a slightly altered version of the model, and those variations could cause substantial confusion for nonresident licensees. We would prefer the definition of "covered entity" exclude nonresident licensees.

b. Exemption. We support the concept of excluding licensees with fewer than 10 employees, those with less than $5m in gross annual revenue, or those with less than $10m in year-end total assets. However, if adopted as part of the NAIC model, the exemption should be from the law as a whole, not from only the most onerous of its provisions. Additionally, we support the regulation's exemption of employees, agents, representatives, or designees of licensees.

c. Risk Assessment. We applaud the design of the Risk Assessment as set forth in 23 NYCRR 500 for its flexibility. It permits covered entities (licensees) to "consider the particular risks of" that licensee's business operations related to cybersecurity. However, we have concerns that this provision is still too prescriptive as it relates to small- and medium-sized insurance agencies, and we respectfully request that the limited exemption be expanded to meet the specific needs of very small companies.

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

Enclosure

NATIONAL ASSOCIATION OF PROFESSIONAL INSURANCE AGENTS

Local Agents Serving Main Street America℠

March 14, 2017

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

The Honorable Elizabeth Dwyer
Chair, NAIC Cybersecurity (EX) Working Group Drafting 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: February 27, 2017 Draft of Insurance Data Security Model Law (Draft #3)

Dear Director Farmer and Superintendent Dwyer:

On behalf of the National Association of Professional Insurance Agents (PIA)[2], I want to first express our thanks for your patience as we have worked together, regulators, industry representatives, and consumer representatives, 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 National Association of Insurance Commissioners' (NAIC) Cybersecurity Working Group's February 27, 2017 Draft of the Insurance Data Security Model Law (Draft #3) (herein referred to as "Draft #3").

We appreciate regulators' efforts to address some of the concerns raised throughout this process and recognize that Draft #3 reflects those efforts, to varying degrees. However, Draft #3 still leaves us with a sizeable number of serious reservations, which are outlined below.

1. PIA's Position on Draft #3

PIA is pleased to be continuing our work with the NAIC on the important issue of cybersecurity. However, Draft #3 is not an improvement over the existing patchwork of state laws, and, as such, without substantial revision, we are unable to support Draft #3 within the NAIC process or at the

[2] PIA is a national trade association founded in 1931, which 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

state legislative level. Having said that, if passage by the Working Group of Draft #3 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 #3. In furtherance of that effort, we offer the following comments and recommendations.

2. Definitions

a. Data Breach. The term "Data Breach" now seems to include embedded definitions of "Acquisition" and "Data Breach Without Use of Personally Identifiable Information." We have concerns about these definitions.

i. First, data breaches now seem to selectively include "acquisitions" or "unauthorized acquisitions" by virtue of Section 3(D).

ii. Second, rather than creating a clear harm trigger, as we have recommended throughout this process, that would legally define a Data Breach, the definition of "acquisition" now excludes data breaches for which the Licensee has determined "with a very high degree of certainty" that the Personally Identifiable Information (PII) released to an unauthorized person has not been used, and the PII has been returned or destroyed without further release. This mechanism appears to operate the way a more traditional, objective harm trigger would; however, the phrase "very high degree of certainty" is extremely subjective. A Licensee would be hard-pressed to know whether such a metric had been met, and a commissioner would be similarly challenged to demonstrate that a Licensee had violated this standard. This will lead to uncertainty when determining whether a breach has even occurred.

b. **Data Breach Without Use of Personally Identifiable Information.** Relatedly, the term "Data Breach Without Use of Personally Identifiable Information" is now defined as a Data Breach in which a Licensee determines, again "with a very high degree of certainty," that the PII acquired by an unauthorized person has not been used, and that said PII has been returned or destroyed without further release or acquisition. This directive is unclear and not workable, as Licensees will have no means by which to determine "with a very high degree of certainty" what has become of PII acquired by an unauthorized person, and such a standard still leaves ambiguity as to how it is to be applied by licensees and enforced by commissioners. Again, a clear harm trigger would be far preferable to this "very high degree of certainty" standard for our small-business, independent insurance agent members, and it would benefit all Licensees to have a clearer understanding of what constitutes a Data Breach for reporting purposes.

c. **Recommendation:** PIA urges regulators to use harm trigger language like "reasonable likelihood of substantial harm to consumers," which is similar to the harm trigger language used in many existing state data breach notification laws[3] and closely resembles language used in earlier drafts of this model. First, as

[3] See https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf (accessed March 13, 2017).

discussed in greater detail below[4], Draft #3 would impose substantial compliance burdens on our members, many of which are small insurance agencies. Without a meaningful harm trigger, those burdens will require small agencies to incur substantial costs to notify consumers and provide remediation even when a suspected breach causes no harm. Such requirements are unnecessarily burdensome and will exacerbate the challenges insurance agents will face in attempting to comply with the terms of Draft #3. Finally, we are concerned about the desensitizing effect the virtual absence of a harm trigger will have on consumers and other recipients of breach notifications. No one wants consumers to receive so many notices of possible breaches that each individual notice becomes meaningless to them. Draft #3 implicitly concludes that nearly every data breach causes harm. Without an objective harm trigger, every breach is theoretically a harm trigger. Potentially every breach would require Licensees to notify consumers, commissioners, and relevant federal and state law enforcement agencies, all of whom will have lost valuable time evaluating and acting on such notifications. When eventually notified of a data breach that *is* reasonably likely to cause substantial harm to consumers, those recipients will undervalue it at their peril.

d. **Licensee.** As we have mentioned repeatedly over the past several months, we have strong concerns about the broad definition of "Licensee" in the context of agents' relationships with carriers and in the context of potential third-party liabilities. The latest definition of "Licensee" in Section 3H combines into one category all who are or should be registered pursuant to state insurance laws. It still assumes that all carriers and agencies of all sizes always share the same resources. Contrary to the premise on which this definition is based, there is often no clear boundary of ownership or custody of information when it passes from one Licensee to another, and that vagueness will pose challenges in the context of assigning liability for a breach.

    i. Additionally, the definition of "Licensee" groups into one category insurance businesses of all sizes and purposes; a one-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 #3. This burden 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 numbers of employees and all levels of sophistication and resources, financial and otherwise.

    ii. For example, it is unclear which Licensee will be responsible when a third-party provider fails to protect personal information provided by the Licensee. If an agent and a carrier pass consumer information back and

[4] See Pages 4-5 for a more comprehensive discussion of scalability.

forth through a third-party agency management system, and that third-party system is breached, it is unclear whether the agent, the carrier, the third party, or some combination thereof will be held responsible. This ambiguity could be resolved with changes to the definitions of "Licensee" and "third-party service provider" (found in Section 3J(4)).

iii. To address these issues, we recommend that the definition of "Licensee" be revised from "any person or entity licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this state …" to "any person or entity licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered, and that employs 500 or more persons, pursuant to the Insurance Laws of this state …"

3. **Licensee Risk Management Provisions**

a. **Information Security Program.** According to Section 4F, Licensees are required to exert extraordinary authority over third-party service providers. For example, Section 4F(2) requires Licensees to "[r]equire its Third Party Service Providers **by contract** to implement **appropriate measures** designed to meet the objectives of this section and take **appropriate steps** to confirm that its Third-Party Service Providers have satisfied these obligations" [emphasis added]. We have a number of concerns about this provision.

i. First, exclusions should be added to this provision for Licensees who contract with the federal government, as they do with the Federal Emergency Management Agency's (FEMA) National Flood Insurance Program and the Risk Management Agency's (RMA) Federal Crop Insurance Corporation. Neither FEMA nor the RMA are going to be willing negotiators in creating contracts specific to Licensees that accommodate the provisions of the model law. If FEMA and RMA are to eventually be expected to abide by state laws based on this model, they should be provided with an adequate phase-in period to make these changes.

ii. Second, FEMA and RMA are good examples of contracts of adhesion that small-business Licensees enter into all the time out of necessity. Like FEMA and RMA, large companies serving as third-party service providers are going to be reticent to contractually bind themselves by laws imposed only on the Licensees. Small-business Licensees rarely have the opportunity to negotiate contracts with relatively large third-party service providers. Therefore, many Licensees will be subjected to whatever safeguards the third-party service provider offers in terms of personal information protection, whether or not those safeguards are "appropriate."

iii. Third, Section 4F(2) requires Licensees to contractually obligate their third-party service providers to implement "appropriate" measures and take "appropriate" steps. This is similar to the vague language used earlier

in Draft #3 and fails to explain even at a basic level what would constitute "appropriate" measures and steps.

iv. Section 5B(4) raises questions about the extent to which a third-party service provider would permit a Licensee to take "reasonable measures to restore the security of the information systems compromised in the Data Breach…."

b. **Scalability Concerns.** We recognize and appreciate that language was changed in Section 4D, Risk Management, specifying that the scale and scope of a Licensee's information security program could be commensurate with the nature, scope, scale, and complexity of the Licensee and the nature of the breach.

i. Having said that, we remain gravely concerned about the burden our smallest member agencies will face pursuant to Draft #3, even with the new language.

ii. 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. 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." Many Licensees may have a handful of employees and scarce resources to hire outside help to execute these directives.

iii. Specifically, in Section 4D(2)(c), it is impractical to require even Licensees with the fewest resources to "[p]rotect by encryption or other appropriate means, all Nonpublic Personal Information stored on a laptop computer or other portable computing or storage device or media." Some of our members are five-person businesses; some are even smaller. Some lack the resources to encrypt personal information as described here.

iv. This problem also exists with regard to Section 4D(3), which requires Licensees to "include cybersecurity risks" in their enterprise risk management processes.

4. **Licensees' Post-Breach Requirements.** Requirements are a minimum. Section 5B sets forth the Licensee's obligations following a breach using the phrase "at a minimum," thereby establishing the list as a floor rather than a ceiling.

a. Small businesses would face extraordinary financial and logistical hardships in complying with such requirements. Section 5B(4)'s "reasonable measures" requirement is subjective and therefore difficult to define. A small business, with, for instance, five or fewer employees, 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 breach *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.

b. **Three-Day Requirement.**
    i. Pursuant to Section 5D, if a small-business Licensee experiences a breach, it must notify its commissioner within "three (3) business days after determining that a Data Breach … may have occurred…", regardless of the resources available to the Licensee to do so. This timeframe would be extremely burdensome to a Licensee. The level of detail sought to be provided to the commissioner in that three-day timeframe, as outlined in Section 5D(1)-(15), is similarly arduous and gives rise to substantial concerns about the practical workability of these provisions.
    ii. Section 5D(11) is particularly burdensome; it requires the Licensee to provide the Commissioner with "[t]he number of total Consumers and Consumers of each state affected by the Data Breach." While generally Section 5D acknowledges that the provision of the listed information will be an ongoing process as information becomes available, with regard to Section 5D(11) 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 each state within three days of a breach will prove unworkable for small Licensees.
    iii. Many small insurance agencies do not have a full-time IT staff member. It could take substantially longer than three business days for a part-time IT staff member to acquire sufficient information about a breach to provide a commissioner with even the most minimal details (date, description, and means of discovery) of the breach.
    iv. **Recommendation:** We urge the Working Group to adopt a timeframe of at least 30 business days in which to notify the commissioner.

c. **Notification to Commissioners.** In accordance with Section 6A(1), Licensees are required to provide notice to "[t]he commissioners of all the states in which a Consumer whose Personally Identifiable Information was or may have been part of the Data Breach resides and the Licensee's domiciliary commissioner." This provision leaves open the possibility that Licensees will be required to provide notifications of potential breaches to all 50+ commissioners. Moreover, the requirement in Section 6C(3) that Licensees prepare a draft consumer notice for preapproval by the commissioner will impose undue burdens on both Licensees and commissioners, who will be required to review potentially thousands of draft consumer notices that will never be used.

d. **Technical Correction.** Finally, as we noted on last week's call, Section 6(C)(4)(d) should begin with the word "Substitute" rather than "Substantive."

5. **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.

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