NATIONAL ASSOCIATION OF PROFESSIONAL INSURANCE AGENTS

Local Agents Serving Main Street America℠

March 23, 2016

The Honorable Adam Hamm
Chair, NAIC Cybersecurity (EX) Task Force

The Honorable Raymond G. Farmer
Vice Chair, NAIC Cybersecurity (EX) Task Force

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

Attn: Sara Robben
Submitted via email: srobben@naic.org

Re: Preliminary Working and Discussion Draft of Insurance Data Security Model Law

Dear Commissioner Hamm and Director Farmer:

On behalf of the National Association of Professional Insurance Agents (PIA)[1], I hereby submit the following comments in response to the Preliminary Working and Discussion Draft of the Insurance Data Security Model Law (ñPreliminary Draftò) recently exposed by the National Association of Insurance Commissionersô (NAIC) Cybersecurity Task Force (ñTask Forceò). We begin by discussing the need for a model law on this topic and then provide specific feedback on the Preliminary Draft.

Necessity and Pace of Development of Model Law

PIA is pleased to work with the NAIC on the essential issue of cybersecurity and admire its leadership in addressing consumersô vulnerability to the misuse of their personal information. However, we remain perplexed about the exact problem the Preliminary Draft seeks to solve and are concerned about the need for a model law that would be passed with the expectation of adoption in some form in each state. Currently, 47 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands already have data security laws.[2] Such laws typically identify the entities that are required to comply with the laws, define ñpersonal information,ò describe what constitutes a breach of data security, provide notice requirements, and provide exemptions where appropriate. The pursuit of transforming this Preliminary Draft into a model

[1] 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.

[2] Security Breach Notification Laws, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

law would be a duplicative effort to achieve uniformity in an area already dominated by functional state laws.

Need for Interim Meeting

We also have concerns about the pace at which the Preliminary Draft was developed and exposed for comment. The Task Force publicly released the Preliminary Draft earlier this month for a three-week period in which to comment. We recognize the interest of the Task Force in moving efficiently on this important, time-sensitive topic. However, the Preliminary Draft contains proposals that raise significant concerns, the consequences of which cannot be fully explored in such a short exposure period.

We are providing these comments in advance of the March 23 deadline and expect to provide additional context for our comments as this process continues, including at the in-person meeting of the Task Force in New Orleans next month. We remain concerned about the underlying goal of the creation of a model law. However, if that is the inevitable conclusion of this process, we encourage the Task Force to engage in a comprehensive evaluation of the overarching goals and specific provisions of the model law.

In furtherance of that goal, we recommend the scheduling of an interim meeting of the Task Force following the New Orleans meeting, at which regulators and interested parties could delve more deeply into the policy goals sought to be achieved by a model law, to explore potential interactions among this Preliminary Draft and existing state and federal laws, and to serve as a collaborative section-by-section editing session. The goal of such a meeting would be to ensure that the model law interacts appropriately with existing state and federal legislative and regulatory requirements, to which licensees are already subject, and to ensure any model law goes no further than necessary to fill any existing gaps in federal or state law and/or regulation.

Comments on Preliminary Draft

Section 1: Purpose and Intent

This section of the Preliminary Draft declares that the model law establishes ñthe exclusive standards for data security and investigation and notification of a breach é .ò This language seems to preclude the Preliminary Draftôs interaction with existing state and federal law, despite the fact that such laws already exist to address many of the issues identified in this draft. As noted above, the goal of the eventual model law is unclear; however, if the intent is to cultivate a degree of uniformity that would improve on the existing 51 jurisdictional variations on data breach security law, this Preliminary Draft is unlikely to achieve that goal for reasons we elucidate below.

Section 2: Applicability and Scope

This Section, like Section 1, seeks to preempt other state laws addressing data security. However, it is not clear that the language of Section 2 effectively avoids duplication with existing and applicable state laws. This Section has the potential to create confusion in terms of how the model is intended to interact with longstanding federal laws like the Health Insurance Portability and Accountability Act, among others. Compliance with existing state and federal law should obviate the need for the second sentence of this Section.

Section 3: Definitions
We have serious reservations about the broad definition of ñlicensee.ò First, it establishes that the model will apply to anyone subject to licensing or registration by state insurance laws, leaving open the possibility of at least some licensees being subject to laws and regulations promulgated by competing authorities at the state level and the federal level. Moreover, placing insurance agents and carriers, for example, into the same single group and referencing them together throughout the model law does not properly acknowledge the sometimes competing interests of these two groups.

The definition of ñlicenseeò does not demonstrate a clear understanding of how the model law will interact with existing state and federal requirements with which licensees currently comply. Additionally, it groups into one category insurance businesses of all sizes and purposes; it sets forth as the standard a one-person insurance agency being treated under the law the same way as a multibillion dollar insurance carrier with an employee roster in the thousands.

Section 4. Information Security Program
We appreciate the effort the Task Force made to specify that the scale and scope of a licenseeôs information security program could be commensurate with the size and complexity of the licensee, the nature and scope of its activities, and the sensitivity of the data in need of protection. However, our aforementioned concerns about the overly broad definition of licensee and the potentially competing interests of licensees of different sizes and with different business objectives remain.

For example, Section 4.D., Risk Assessment, instructs licensees to ñ[d]esignate an employee or employees to coordinate the information security program.ò Some licensees have may have a handful of employees, none of whom would be qualified to execute any of the tasks required in Section 4.D.(2)-(5), let alone all of them.

These same concerns apply with equal measure to the tasks enumerated in Section 4.E.(1)(a)-(i). Additionally, Section 4.E. refers to the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* as a guide. However, the NIST *Framework* was recently the subject of a Request for Information on the basis that it might need to be updated, and a workshop on the future of the *Framework* is being held early next month to discuss the comments received and consider potential changes.[3]

We also have concerns about Section 4.G., which instructs licensees to specifically contract with their third-party service providers for said service providers to undertake particular tasks on behalf of the licensee. When a small-business licensee contracts with a relatively large third-party service provider, the contract is essentially one of adhesion, and the licensee has little or no bargaining power to change the terms of the agreement. Contracts of adhesion leave little room for negotiation, making it extremely challengingð if not completely impossibleð for small-business licensees to adhere to these terms.

[3] Views on the Framework for Improving Critical Infrastructure Cybersecurity, https://www.federalregister.gov/articles/2015/12/11/2015-31217/views-on-the-framework-for-improving-critical-infrastructure-cybersecurity.

Section 6. Investigation of a Breach of Data Security
Presumably, the word ñlicensee,ò used three times in Section 6.A., is intended to refer to a single entity that identifies a possible breach within its own system and then conducts an investigation into that possible breach. However, Section 3ôs overly broad definition of licensee leaves Section 6.A. ambiguous on this point. One recommended alternative to the existing wording might be, ñIf a licensee believes that a breach of data security has or may have occurred in relation to personal information that is maintained or communicated by that licensee, that licensee shall conduct an investigation.ò

Additionally, Section 6.B.(4)ôs ñreasonable measuresò requirement is subjective and therefore difficult to identify. A small business, with, for instance, five or fewer employees, would be unduly burdened by the requirements set forth in Section 6. A small-business licensee may not have sufficient resources to discover that a breach may have occurred until months or years after its occurrence. It may not have the resources to even 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.

Finally, perhaps the most unsettling aspect of Section 6 is the manner in which it serves as a trigger for the onerous licensee obligations set forth in subsequent sections.

Section 7. Notification of a Breach of Data Security
Section 7.A. is triggered by the licenseeôs conclusion, reached after the investigation required by Section 6, that a Section 6 breach is ñreasonably likely to cause substantial harm or inconvenience to the consumers [affected by the breach].ò Again, it is unclear what constitutes ñsubstantialò harm or inconvenience to consumers. Should a breach be deemed likely to cause such harm or inconvenience, the licensee or a third party acting on its behalf must provide notice ñwithout unreasonable delayò (though it is unclear what level of delay would rise to the level of being ñunreasonableò) to several entities, one of which is the applicable insurance commissioner. However, Section 7.B. requires that the licensee notify the commissioner within ñfive (5) calendar days of identifying a data breach.ò This requirement both conflicts with Section 7.A.(2) (mandating notification to the commissioner by the licensee or an agent thereof without unreasonable delay) and imposes an extremely burdensome timeframe for a licensee. The level of detail sought to be provided to the commissioner in that 5-day timeframe, as outlined in Section 7.B.(1)-(15), is similarly arduous and gives rise to substantial concerns about the practical workability of these provisions.

Moreover, we also have concerns about the precedent being set by Section 7.D.(3), which requires the licensee to submit ña draft of the proposed written communication to consumersò for the commissioner to edit. Read in conjunction with Section 7.D.(1), this gives the commissioner and the licensee 15 calendar days in which the commissioner shall edit the communication and then return it to the licensee, and the licensee must communicate with the consumer regarding the breach. This is a relatively short time in which to accomplish these tasks; again, we question the practicality of these provisions. In the same section, licensees are instructed in great detail as to what information must be included in such a communication.

With the benefit of the extensive list provided in Section 7.D.(3)(a)-(g), licensees are capable of effectively communicating with their customers about a data breach; their communications with their customers need not be subjected to editing by the commissioner. Additionally, this discretion could be variably applied by commissioners in different states, making this provision a means by which the enforcement of the law could vary greatly by state. Finally, under existing law, if a licensee communicates ineffectively with its customers, they may file complaints with a commissioner and/or take their business elsewhere; consumers can use existing measures to protect themselves from ineffective communications by licensees, rendering this commissioner editing process superfluous.

Section 8. Consumer Protections Following a Breach of Data Security
Section 8 provides that the commissioner will prescribe the ñappropriate level of consumer protection requiredò following a breach and the duration for which that protection will be provided. As previously noted, giving the commissioner this discretion, especially using the vague metric of appropriateness, has the potential to foster inconsistency across states.

Sections 9 and 10
Sections 9 and 10, like several others, lay the groundwork for potentially inconsistent application across states. These provisions also raise questions about the way the model law will interact with existing state laws and regulations. Normally, the prosecution of alleged violations of state law would fall to state attorneys general. It is unclear whether state attorneys general are expected to work in cooperation with state insurance commissioners, they are expected to engage in parallel investigative procedures that will occur concurrently with those of the commissioner, or they are expected not to act in instances of potential violations of state data breach laws.

Section 11. Confidentiality
Section 11.A. provides that documents or materials in the possession of an insurance department in connection with an investigation pursuant to this model law are not subject to subpoena. We are unsure whether such a provision is enforceable in court. The recipient of a subpoena always has discretion as to whether to comply, but that does not mean that states can legislate around the courtsô subpoena authority, nor does it mean that they can indemnify a noncompliant recipient of a subpoena against punishment for failure to comply.

Sections 9-14
These sections, setting forth an administrative process for addressing violations of the model law, appear to be redundant with the preexisting broad authority provided to the commissioner.

Section 15. Individual Remedies
It is difficult to comment in depth on Section 15.A. (regarding a consumerôs right to seek judicial relief for a licenseeôs failure to comply with sections of the model law that address consumer rights) without the enumeration of the applicable sections therein. However, as a general matter, allowing for a private right of action creates an unnecessary layer of enforcement against licensees, who are already subject to robust mechanisms for regulatory fines and penalties for violations.

Section 18. Rules and Regulations
Section 18 gives regulators broad authority to adopt implementing regulations ñas shall be necessary to carry out the provisions of this Act.ò The provision of such authority 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 NAICôs Cybersecurity Task Force has given to this issue, and we are grateful for the opportunity to 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: Sara Robben & Eric Nordman