https://NavigationAdvisors.com

March 23, 2016

Adam Hamm
Chair
Cybersecurity Task Force
National Association of Insurance Commissioners (NAIC)
1100 Walnut Street, Suite 1500
Kansas City, MO 64106-2197

To Sara Robben at srobben@naic.org

RE: INSURANCE DATA SECURITY MODEL LAW – Comments on the NAIC Preliminary Working and Discussion Draft

Dear Commissioner Hamm:

We are pleased to offer the following comments on the Preliminary Working and Discussion Draft of the INSURANCE DATA SECURITY MODEL LAW being discussed by the NAIC. We hope that your Task Force will find the comments useful in its decision-making process.

These comments are limited to specific areas of the current draft and are not intended to incorporate all of our views and suggestions.

Support for the Development of the Model Law

We fully support your goals of protecting consumers from cyber-related threats and making sure that any damage to consumers or compromise of their personally identifiable information of a sensitive nature is addressed to the fullest extent possible. The focus of our comments on potential areas of improvement is not in any way indicative of a negative view of this initiative.

The growth and evolving nature of cyber threats puts consumers and our society at an increasing risk. We applaud your work on using the regulatory framework to reduce this risk, putting in place both standardized protections for consumers and corresponding requirements for insurance entities.

Definitions of *Data Breach* and Other Terms

The existing state laws related to mandatory data breach notification, other state laws, and the various federal laws and requirements do not use a consistent definition of *data breach*; the laws generally do not define the term directly but use other terminology instead. We appreciate that this presents a significant challenge to the drafters. It also makes it particularly important to assure, wherever possible, that the definitions presented do not introduce an additional level of compliance requirements simply because of the need to use a new and different definition.

Before providing a specific recommendation, we would like to understand whether the definition of *data breach* is intended to be modified by individual states so that it conforms to the corresponding definitions in the so-called "data breach notification laws" in these states. (We note that these laws have not been adopted in every state at this point and in some cases differ significantly in both defining data breaches and specifying mandatory actions when such events occur.)

The definition in the current draft is as follows:

> "Breach of data security," "breach," "data breach," or "security breach" means the unauthorized acquisition of personal information.
>
> The term "breach of data security" does not include the unauthorized acquisition of personal information that is encrypted, redacted, or otherwise protected by another method that renders the information unreadable and unusable if the encryption, redaction, or protection process or key is not also acquired without authorization.

The definitions used in the various laws and regulations often differ from the one provided. For example, there is often a distinction made between known, likely, and potential acquisition of personal information by unauthorized parties. Depending on the law and the jurisdiction, the definition of *data breach* can be broader or more narrow. It can also be broader in some respects and more narrow in others.

The same applies to other terms such as *personal information* and *encryption*. Depending on how these terms are defined, the definition of *data breach* will change as well.

We believe it is necessary to decide whether the intent is to

(a) have the definitions modified in individual states to conform to the definitions in the existing state laws[1] concerning mandatory data breach notification or definitions in other state or federal laws, or
(b) take leadership in establishing a uniform definition that will then be used in all or most jurisdictions[2]

[1] The likely result of presenting the model law in its current form to a state legislature.

Of equal importance is the definition of *personal information*, which in the current draft appears very broadly defined, so is open to interpretation. We do not provide specific suggestions on how to define any of these terms because this issue is directly related to the need to understand the intent in defining the term *data breach* as mentioned above.

The term *encrypted* is open to interpretation as well, because there are many types of encryption, some of which are weaker than others.

Cybersecurity Framework

We believe that the requirement to use as a guide the *Framework for Improving Critical Infrastructure Cybersecurity* developed by the National Institute of Standards and Technology (NIST) is unnecessary and inappropriate. The NIST Framework has been designed as a voluntary framework for the critical infrastructure. Its imposition, even as a guide, on every entity licensed by a state insurance department is an unreasonable burden that does not achieve the goal of improving cybersecurity in an optimal way. It is a particular issue for very small businesses.

While the core concepts of the NIST Cybersecurity Framework are useful in almost any environment, it is unreasonable and unnecessary to expect a small business that is not part of the critical infrastructure to have familiarity with the voluntary NIST Framework and be required to use it as a guide. We do not believe that any specific framework can be seen as directly applicable to all insurance licensees.[3]

Specific Information Sharing Mechanisms

We do not believe the requirement to use an Information Sharing and Analysis Organization (ISAO) to be reasonable. Assuming that the intent is to have the same definition of ISAO as used in the federal laws and regulations, it is not practical for every insurance licensee to use an ISAO. Nor is it always necessary. There are other ways to obtain information necessary for improving cybersecurity.

Data Ownership in the Context of Data Security

The provisions of Section 5 (Consumer Rights Before a Breach of Data Security) beg the question of who is the owner of the data and whether an insurance entity may sell or transfer personally identifiable consumer information to another entity, with other entity not necessarily being subject to insurance regulation. The question of data ownership is not new

---

[2] With the understanding that not all states will agree with any uniform definition, and considering the fact that three states at this point do not have data breach notification laws at all.

[3] We do see potential advantages to the use of the NIST Cybersecurity Framework by insurance companies but do not believe it should be a requirement for any insurance entity.

and is not directly related to the cybersecurity requirements in Section 5. However, it has to be properly addressed.

Providing Notice

We believe that the requirement to provide to the commissioner a draft of the proposed written communication to consumers no later than forty-five (45) calendar days after identifying a data breach, with the right to edit the proposed communication before the licensee sends it to affected consumers, is unnecessary and potentially counterproductive. In particular, it can lead to unreasonable delay when the goal is to inform those affected by a data breach in the most expeditious manner.

Given that some specific requirements are already included in the proposed model law, we suggest that the requirement to provide a draft notification to the commissioner be replaced by the requirement to provide a copy of the notification, and by empowering the commissioner to require an additional modified notification if the original notification does not meet these requirements.

Risk Assessment

The Risk Assessment sub-section of Section 4 (Information Security Program) lists specific actions related to risk assessment but does not indicate the frequency with which they have to be undertaken. We suggest that a reference to specific standards, industry practices or reasonableness be included.

Specific Risk Assessment

The current language includes the requirement to "[a]ssess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information." It can be argued that the language dealing with the consequences of a data breach and actions required to be taken in case a data breach occurs does not seem to differentiate among various degrees of data "sensitivity." Based on this interpretation and for this particular purpose it, is only relevant whether a breach of sensitive information has occurred, making the degree of sensitivity not important.

We understand this argument and bring it to your attention. However, we do not necessarily advocate that any language be changed based purely on that argument.

Electronic vs Other Data

The draft of the Model Law appears to apply to all data and not be limited to data stored in an electronic format. We believe it would be beneficial to clarify the scope of the proposed requirements.[4]

Please note that these comments and recommendations represent my personal views and the views of Navigation Advisors LLC. They are not intended to reflect the position of the CAS Task Force on Cyber Risk, which I currently chair. These personal views should not be seen as a public policy statement, nor as a position taken by this organization.

Sincerely,

Alex Krutov, FCAS, ASA, MAAA, CERA
President
Navigation Advisors LLC
alex.krutov@navigationadvisors.com
www.navigationadvisors.com

cc: Raymond G. Farmer, Vice Chair of the NAIC Cybersecurity Task Force
Eric Nordman, Director of the NAIC Center for Insurance Policy & Research
Tony Cotto, NAIC Financial Policy and Legislation Counsel
Patrick McNaughton, Chair of the NAIC ITEWG
Aaron Brandenburg, NAIC Economist and Statistical Information Manager

[4] The current mandatory data breach notification laws adopted by most states are not always consistent is whether they apply only to electronic data.