August 10, 2015

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

Via email to Pat Simpson at psimpson@naic.org and Sara Robben at srobben@naic.org

---

RE: CYBERSECURITY BILL OF RIGHTS – Comments on the Draft

Dear Commissioner Hamm:

Below are comments on the exposed draft of the Cybersecurity Bill of Rights. We hope that you will find the comments useful in the discussion of this document that your Task Force has on the agenda for the upcoming national meeting of the NAIC.

Most of our comments fall in one of the following three categories:

- ***Technical Issues Related to Data Breaches*** Comments that deal with technical issues related to data breaches, including cybersecurity-specific concepts and terminology, such as the very definition of a data breach
- ***Possible Intended and Unintended Uses of the Document*** Comments and observations on how the document can be used by regulators, the industry, and consumers, including both the very positive effect and some potentially negative impact of certain language in the draft
- ***Potential Issues of General Nature*** Comments and observations that are limited to identifying potential general concerns

Strong Support for Your Mission

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 sensitive nature is addressed to the fullest extent possible. Insurance transactions often involve disclosure of large volumes of such information to insurance companies and other entities overseen by state insurance regulators. In the event of a data breach affecting this information, consumers may suffer irreparable damage. *We applaud your work* on using the regulatory framework to reduce this risk.

Importance of Consumer Protection in the Era of Cyber Risk

Growing volume of consumer data is at risk. This risk is growing and evolving. The number of disclosed data breaches is just one indicator of this risk and its increasing magnitude. The risk to consumers is not limited to traditional fraudulent use of existing credit cards and other financial accounts or opening new accounts. Other consequences may be even more destructive, such as certain kinds of reputational damage. Fraudulent use of personal medical records can lead to severe consequences such as a situation where wrong medical treatment is prescribed to a critically injured person. Unfortunately, there are too many examples of what may go wrong and has already been observed to go wrong. Insurance consumers rely on insurance companies and other regulated entities to protect them from this risk and to ensure that sensitive information obtained from consumers is properly secured.

Intended and Unintended Use

We understand that the following three uses of the document being drafted have significant merit:

1. The insurance-specific Cybersecurity Bill of Rights can be used as a general guidance in making changes to the Model Laws promulgated by the NAIC and typically adopted by state legislatures with few or no modifications.

   This is an important because the document, when further improved, can be a useful benchmark for drafters of the Model Laws. Changes to some of the NAIC Model Laws are required to address the issues of protecting security of consumer information obtained in insurance-related transactions.

2. State-specific versions of the Cybersecurity Bill of Rights can be used by state regulators and be disseminated to insurance consumers in individual states.

   The NAIC template can become the basis for making these modifications and creating customized documents that properly reflect laws and regulations of each state and that also clearly specify that such a document or some of its clauses apply only to a certain state. The NAIC template may have specific suggestions to state regulators on what clauses are universally applicable and not state-specific.

3. The document can be used to create more formal and detailed guidelines for insurance companies, producers and other entities regulated by states.

   In addition to the already mentioned potential modifications to the Model Laws, the document may be utilized in guidelines for conducting IT examinations that are part of the overall financial examinations of insurance companies, guidelines for market conduct examinations, and other oversight and enforcement activities.

At the same time, we are concerned that the document can be unintentionally misused. This concern is based primarily on the ease of misunderstanding its purpose and some of its content. We recognize the difficulty involved in the drafting process and making a document on a technical topic simple yet accurate. This unavoidable difficulty is the primary reason we have these concerns.

Consequently, we make the following recommendations:

1. The document, in its current form or if only minor modifications are made, should not be used in communications with consumers.

2. Unless significant changes are made or important clarifications are introduced, no single document of this nature should be used in all states in communications with consumers because the current differences in state laws are too great.

Many consumers are unfamiliar with insurance laws and regulations in their states and may be even less familiar with the issues involved in data breaches and safeguarding personal information. Reading this document may result in wrong expectations on their part. The suggestion, at the very end of the exposed document, to contact state insurance departments for more details, is unlikely to affect the already formed understanding. This understanding may be inaccurate, such as in cases where some of the listed consumer "rights" do not exist in a certain state.

What's a Data Breach?

The section Standard Definitions provides definitions of six terms. Other terms are not defined. Given the goal of making the document simple and understandable, this is appropriate.

Definition of Data Breach Definition of data breach is critical to understanding the key clauses of the draft. We assume it is the reason why this definition is placed first, not following the alphabetic order, on the list of Standard Definitions.

We agree with the importance of properly defining this term but have significant concerns about the definition used. In particular, we are concerned that the many existing definitions of data breach are difficult to reconcile. As a consequence, it is difficult to provide one definition that would be applicable in all cases where data breaches are mentioned in the document.

In most cases, consumer rights described in the document seem to be derived from the *state breach notification laws*. For this reason, the definition of a breach should be consistent with how this term is defined in state laws. However, these laws differ by state and in most cases do not use the term "data breach" at all. Instead, terms such as "breach of security," "breach of system security," "breach of the security of the system," "breach of security of computerized data," "breach of the security of the system data," and others are used. In some cases, they are defined in ways very similar to the definition used in the draft, while in other cases the meaning can be quite different. The definition in the draft requires that "unlawful and unauthorized acquisition" of relevant data occur. State breach notification laws may in some cases define breach of security to include unauthorized access even where acquisition has not occurred. There are other differences.

A third of the document is devoted to describing consumer rights derived from *federal laws*. This too calls for consistency in the definitions; otherwise, the rights described may not exist. The document uses the same term "data breach" to describe rights derived from HIPAA (as in #5). In the HIPAA context, the term data breach is used, which makes it easier to assure consistency.

The current HIPAA definition of a "breach," applicable to protected health information, refers to its unauthorized acquisition, access, use or disclosure. #5 in the draft refers to this "data breach" of protected health information under HIPAA. The use of the term data breach here is not consistent with the definition provided in the draft. The definition in the draft requires information "acquisition" (and more specifically "unlawful and unauthorized acquisition") while not including information access, use or disclosure in the definition of the data breach presumed to apply to all situations the draft describes. This difference can be quite significant. There are other differences as well.

These are just some of the concerns related to the definition of a data breach in the document.

Definition of Personally Identifiable Information The definition provided in the draft is correct in the sense that it is logical and is derived (directly or indirectly) from the definition originally developed for use by federal agencies (Privacy Act). For the most part, state breach notification laws make use of the same definition. However, there are significant differences in how exactly Personally Identifiable Information (PII) is defined in state laws that require notification in case of a breach. In some cases, these definitions are completely inconsistent with the definition in the draft. Some states also use other terms instead of or in addition to PII, adding to potential confusion and creating an unacceptably high chance of the document being misunderstood by consumers and resulting in wrong expectations.

Other definitions Certain terms are defined in the Standard Definition section. The intent appears to be to provide additional clarification to consumers who may not be familiar with the terminology used in the insurance field as well as some of the terms related to cybersecurity. The concern is fully justified and the need to explain the key terms is clear.

Some consumers are insufficiently familiar with the term *Insurance* and would benefit from having a general explanation. However, we do not believe that these consumers will derive much benefit from the explanation that insurance is "a written contract issued by an entity (insurer) agreeing to accept a risk transfer from an individual, family, or business for a fee (premium)." (As a separate matter, this definition differs from other definitions that exist in the law or are provided as an explanation to consumers on the NAIC website. It can also be argued that the definition is not entirely correct. Regardless of these considerations, the definition does not help consumers to understand the term.)

We recommend that the definition be deleted. Consumers would benefit more from seeing definitions of other terms and explanation of concepts not currently provided. Insurance is the term generally understood. If the regulators believe it is important to define the term, we suggest that a different definition be used.

Definition of *Insurance Transaction* provided is broad and appears to include what can be referred to as insurance service. This leads to the question as to why #2 in the draft specifically refers to "insurance transaction or service." Unless some other meaning is intended, we suggest that the word service be deleted from #2. Alternatively, this word can be included in the Standard Definitions section.

"Other state-regulated entities" is the term used the document in numerous places. However, it is not clearly defined and is unlikely to be understood by consumers who may not be aware which entities

are subject to state regulation. We assume that only insurance regulation is assumed to be included. This too requires clarification. We also note that toward the end of the document, the term "regulated entities" is used instead of "state-regulated entities." We assume the word "state" has been accidentally omitted, but it is easy to take for granted that the broader term is used intentionally because it follows the discussion of federal regulations and links to the Federal Trade Commission website.

Redundant or Unclear Clauses

#6 in light of #4: At least on the surface, #6 appears to introduce no new information and be part of the broader requirements already stated in #4. Unless the intent is to introduce new information (in which case this intent should be clarified), the whole statement is redundant and should be deleted.

#3 vs. #4: The difference between #3 and #4 is not entirely clear. #4 refers to data breaches that are defined in a specific way later in the document. This makes it possible to interpret #4 as describing a situation different from the one described in #3. However, it is not clear that the distinction is intentional or that one is not a subset of the other (if they are different).

#4: The list of requirements is not reflective of the current state of affairs and the laws on the books in most states. While the NAIC may set a goal of having all of the items on the list ultimately become consumer rights, the list does not provide a fully accurate description of the rights consumers have now. We also point out again that not every state has breach notification laws at all.[1]

#7: Similar to above, this statement is too general and does not apply to every state. We also question the need to specifically mention paper records in this statement considering that (a) paper records are not mentioned elsewhere, (b) even in states that have breach notification laws, these laws often cover only electronic records, and (c) the title Cybersecurity Bill of Rights does not seem to apply to paper records.

If the regulators want to preserve this statement, its language should also be revised to make it clear what type of a data breach is being described. The current mention of "the event of a data breach of their security system, maintained by a third party service provider" creates the impression that the service provider's role is to maintain the main party's "security system" and that this security system has been breached. This cannot be the intent because the description immediately following makes it clear that the third-party service provider plays a completely different role from maintaining the main party's "security system."

#8: While restoring security is self-explanatory, it is unlikely that a consumer will understand what may be meant by restoring "confidentiality" of the information involved in a data breach.

#9: Providing identity theft protection for two years is not required in most states. A statement to the contrary would be misleading to consumers. We also point out that the definition of "identity protection" and the required scope of identity protection coverage are not provided.

[1] As of this date, three states do not have breach notification laws.

Please note that these comments and recommendations represent my personal views and are not intended to reflect the position of the P/C Risk-Based Capital Committee of the American Academy of Actuaries, which I chaired until approximately a year ago, or 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 any of these two organizations.

Sincerely,

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

cc: 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