October 9, 2015

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: CYBERSECURITY BILL OF RIGHTS – Comments on the Revised Draft

What are Data Breaches, What Measures are Taken to Prevent Them, and What Can be Expected if a Data Breach Affecting Personal Information Happens?

Dear Commissioner Hamm:

Below are comments on the current draft of the Cybersecurity Bill of Rights. We hope that your Task Force will find the comments useful in its decision-making process.

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. 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.

Some of the comments reiterate important points we have made previously.

Similar to the comments we submitted in August in response to the request of the NAIC Cybersecurity Task Force, most of the comments below fall into one of the following three categories: (a) technical issues related to data breaches, including cybersecurity-specific concepts and terminology, such as the very definition of a data breach, (b) possible unintended uses of the document, focused on improving the language of the draft, and (c) comments and observations of a general nature.

The Challenge of Providing Uniform Language Applicable to Any Insurance Consumer

Because the specific requirements and expectations differ, in some cases dramatically, from state to state and from one situation to another, it is very difficult to develop a comprehensive description of

what these requirements and expectations are. Unintentionally providing information that may be false in a particular case or can simply be misunderstood is a significant risk.

Much of the draft language is based on state laws dealing with mandatory notifications of exposed parties in the case of a data breach affecting their personal information.

- As of today, three of the fifty states in the US do not have in place laws dealing directly with data breach-related notifications.

- The forty-seven states and the District of Columbia that do have such laws lack consistency in (1) the definition of the data breach that triggers the legal requirements and (2) the requirements themselves. In some cases, the differences are significant.

- Federal laws, regulations, and guidelines use different definitions and create different rights and requirements based on the type of breach, information potentially compromised, type of company, etc.

- Common colloquial usage of the term data breach can differ from any of the above.

Specific Recommendations

1. Provide clear **guidance to state regulators** to indicate that the document should not be assumed to reflect rights, requirements, and expectations applicable to insurance consumers and insurance enterprises in their states. In all likelihood, the specific language will need to be adjusted.

2. Include prominent language in the document to **explain to consumers** that not all of the provisions mentioned (even after modifications made by individual states) may apply to them. Prominently emphasize that the document is a simplified summary and should not be relied on by itself.

3. **Reduce the use of categorical language** in general and also where the specific requirements may differ significantly based on jurisdiction. For example, even in states that have data breach notification laws, these laws generally have exceptions to allow the extension of the notification period. (See "never more than 60 days after a data breach is discovered" in #4.)

4. **Avoid interpreting federal laws** and regulations or what can be seen as providing such interpretation. (For example, consider the language of #6. Also, note that the fifth bullet point in #6 may be interpreted as already included in the previous bullet point in the current simplified language.)

5. Use **a single definition of data breach**. The current definition in the Standard Definitions section is not entirely consistent with the definition in the statement #4. This seemingly insignificant difference is important in many contexts.

6. Avoid ambiguity and possible **inconsistency between the terms *data breach* and *personal information* (*personally identifiable information*)**. For example, the current definitions,

combined with the descriptions in the text, may easily create the impression that revealing a person's full name is by itself a data breach. (See #4 and the Standard Definitions section.) This is usually not the case from the legal point of view.

7. Make it clear that the provided **definition of the data breach is simplified**. This is necessary even if the definition is changed from the one in the current draft. The actual definition differs among state laws and is typically also different from the relevant federal laws. Some state laws avoid defining a data breach (security breach) and intentionally use other terminology. In addition, the term *data breach* may be used in many other contexts and have different meanings.

8. **Avoid imposing unreasonable and possibly illegal requirements** on businesses, especially where it is not intended. For example, #2 articulates the expectation that privacy policies, including information on how certain data is stored and protected, be posted on the websites of insurance companies and agencies. It is unclear whether details of how certain data is protected are expected to be posted on websites, especially if the websites are not used for insurance transactions. This language also creates the impression that there is a requirement to have a website. This is a reasonable expectation regarding insurance companies, but it is unlikely that every single insurance agent has a website, and we are not aware of any requirement that every such agent have one.

9. The note in italics at the bottom of page 1 should not create the expectation that the specific rights are triggered only "when you get a notice that your personal information was involved in a data breach." **Specific rights and expectations are not triggered by a breach notification.** In fact, they exist before a data breach and after the data breach even if notification has not been provided.

10. Delete the **definition of insurance transaction**. It is inconsistent with some of the common usage because of the term transaction is often understood to mean a legal transaction that would not be entered into if the insurer declines to issue a policy or the applicant chooses not to enter into the insurance contract. This meaning would exclude activities such as determining the price of insurance mentioned in the definition. On the other hand, if the current definition is used, it should include activities such as administering insurance policies (including collection of insurance premiums). Since the term insurance transaction is not used anywhere except in the Standard Definitions section, we suggest that it be deleted.

11. Provide greater clarity regarding whose **obligation** it is **to maintain security and provide notifications of data breaches**. For example, #4 describes the right to "get a notice from your insurance company, agent, or any business they contract with," which creates a clear – and usually wrong – impression that the obligation to provide notification of a data breach is shifted from the insurance company that has experienced the breach at its third-party service provider to that service provider.

12. **Avoid unfamiliar terms or untraditional use of terms such as *data warehouse***. In #1, the term *data warehouse* by itself should not imply the use of a third-party vendor. While more than one definition of a data warehouse exists, the simplified common definition is that

of a central repository of data (often transaction data) from one or more sources that can be used for the purposes of reporting and data analysis.

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