August 10, 2015

Commissioner Adam Hamm, Chair
C/O Pam Simpson
NAIC Cybersecurity (EX) Task Force
444 N. Capitol Street NW, Suite 700
Washington, DC 20001

VIA EMAIL: psimpson@naic.org

RE: Proposed Cybersecurity Bill of Rights

Dear Commissioner Hamm,

On behalf of the Council of Insurance Agents & Brokers (CIAB), the National Association of Health Underwriters (NAHU), the National Association of Insurance and Financial Advisors (NAIFA), and the National Association of Professional Insurance Agents (PIA), we would like to offer comments on the proposed "Cybersecurity Bill of Rights." We understand the purpose of the Cybersecurity Bill of Rights to be twofold: (1) to ensure that consumers know what rights and remedies they have under applicable state and federal law, and (2) to accurately outline what a consumer can expect in the event that their personally identifiable information is compromised. We fully support the efforts of the NAIC to ensure that consumers know and understand their rights in the event of a breach of their personally identifiable information.

Drafting a document to achieve the above stated goals is an arduous task given the differing laws and regulations governing cybersecurity and breach notification. This is compounded by the fact that many regulators, state legislators, and the federal government are all working to update and amend current rules governing these issues. We commend the NAIC for undertaking the drafting of the Cybersecurity Bill of Rights and for being a leader on cybersecurity issues.

While we support creating a Cybersecurity Bill of Rights, we are concerned that, as currently drafted, it may create confusion for consumers as to exactly what rights they have following a breach by implying that certain rights, which are not contained in all applicable state and federal laws, exist for all consumers. We kindly request that in working toward a final Cybersecurity Bill of Rights, the NAIC consider as to each stated right that breach notification laws vary from state-to-state and under federal law, and craft each stated right accordingly. In fact, clearly stating that the specifics of each state's law and federal law vary as to consumer rights following a breach of nonpublic personally identifiable information on the Cybersecurity Bill of Rights may help alleviate potential consumer confusion.

With this in mind, please see our comments below. We hope that these suggestions will assist the NAIC in drafting a Cybersecurity Bill of Rights that accurately reflects consumer expectations, rights, and remedies under applicable federal and state law.

Right #2: We suggest replacing "adequately protecting" with "taking steps to safeguard," or similar language. We believe it most accurately depicts the expectation that consumers have. Every consumer should expect that those holding personally identifiable information are safeguarding it to the best of their abilities. What is "adequate" will depend on the type of information kept, how the information is kept, and the type of business keeping the information; the common thread is that all businesses take steps to safeguard the information.

Alternatively, the NAIC may wish to simply remove the word "adequately" or define "adequately safeguard" in line with the above comments so that consumers have a clear idea of what they can expect.

Rights #3, #4, #6, and #7: We suggest removing the language "from an insurer, insurance producer, or other state-regulated entity" and adding "as outlined in applicable state and federal law" to each of the above mentioned rights.

The reasons for the first part of this suggestion are we believe that, as currently written, it is confusing for the consumer to understand who is responsible for sending the notice and it could be read to suggest that multiple notices regarding the same issues would be sent. We believe saying "receive notice" or "receive notice from the regulated entity that suffered the breach" more succinctly conveys what notifications a consumer can expect to receive under current state and federal laws.

As for the second part of the suggestion, state and federal laws contain differing breach notification requirements. Clearly stating that when a consumer is legally entitled to receive a notification is "controlled by applicable state and federal laws" will help consumers understand that notification requirements vary depending on the type of breach and the location of the affected consumer. For the same reason, we also suggest removing the "60-day" requirement from Rights #4 and #6.

Rights #6 and #7: We suggest adding language stating that notice would occur if there is a "risk of theft or fraud." Most applicable state breach notification laws require that there be a risk of harm for notification to be trigged and this standard is used in #3 of the Cybersecurity Bill of Rights. Adding language to convey that notice is given if there is a "risk of harm" more appropriately conveys what rights are provided under state laws in a manner that will not create confusion or unnecessary notifications for consumers.

Right #9: Requirements under state and federal laws in relation to credit monitoring protection services vary and few laws require that credit monitoring services be offered to impacted individuals. Generally, laws do not require that identity theft protection, which differs from credit monitoring, be offered in the event of a breach. Nor do any laws, which we are aware of, mandate impacted consumers receive credit monitoring. Instead, some laws provide that credit monitoring must be offered at no cost to the consumer, at which time it is at the option of the consumer to accept said service. Overwhelmingly, credit monitoring is voluntarily offered by companies to impacted consumers following a breach.

We are concerned that Right #9 as written would confuse consumers as to what they can expect to receive under state and federal laws. We suggest that Right #9 be removed or otherwise amended to reflect that consumers may be offered credit monitoring and/or identify theft protection services based on the circumstances of the breach and applicable laws.

We appreciate the considerable effort that has gone into drafting the Cybersecurity Bill of Rights and we are grateful for the opportunity to provide our perspective on this important issue. We are happy to work with the NAIC on further specific language changes and suggestions should you so desire. Please contact us with any questions or concerns. Thank you again for your time and consideration.

Organization	Contact	Phone Number	E-Mail Address
CIAB	Amy Forester Roberti, Vice President Industry Affairs	202-350-5860	amy.roberti@ciab.com
NAHU	Marcy Buckner, Vice President of Government Affairs	202-595-7589	mbuckner@nahu.org
NAIFA	Steve Kline, Director State Government Relations	703-770-8187	skline@naifa.org
PIA	Jennifer Webb, Counsel & Director of Regulatory Affairs	703-518-1344	jennwe@pianet.org