AMERICAN LAND TITLE ASSOCIATION

March 23, 2016

Commissioner Adam Hamm
Chairman, Cybersecurity Task Force (EX)
National Association of Insurance Commissioners
c/o Sara Robben, Statistical Advisor
Via email: Srobben@naic.org

Re: 3/2/2016 Preliminary Working and Discussion Draft of an Insurance Data Security Model Law

Dear Commissioner Hamm:

The American Land Title Association[1] (ALTA) appreciates the opportunity to comment on the early draft of the National Association of Insurance Commissioners' (NAIC) Preliminary Working and Discussion Draft of an Insurance Data Security Model Law. Data security is an important component of protecting consumers from cyber fraud. We appreciate that the NAIC recognizes the benefit of a single standard for data security and investigation and notification of a data breach. We are concerned that the Preliminary Working and Discussion Draft would not establish a single standard for consumer protection, which is likely to create confusion and conflict among various regulators, state attorneys general, courts, industry and consumers. As currently written, the Preliminary Working and Discussion Draft appears to take the most severe penalties, add an extensive additional regulatory burden and private rights of action under state regulation. No state today approaches data security in this manner.

We will continue to work with the NAIC to ensure that consumers' personal information is protected, that the laws governing this consumer protection are created in a transparent process that establishes a single standard for data security and breach notification. A single standard for data security is an important goal, since there are 47 state data security laws in place today.[2] State data breach notification laws appeared in 2003 and have subsequently been modified and have in many states been replaced by second generation statutes.

[1] The American Land Title Association, founded in 1907, is a national trade association and voice of the real estate settlement services, abstract and title insurance industry. ALTA represents over 6,000 member companies. With more than 8,000 offices throughout the country, ALTA members operate in every county in the United States to search, review and insure land titles to protect home buyers and mortgage lenders who invest in real estate. ALTA members include title insurance companies, title agents, independent abstracters, title searchers and attorneys, ranging from small, one-county operations to large, national title insurers.

[2] Our best information indicates that Alabama, New Mexico and South Dakota do not have statutes that address data breach notification.

Before drafting a state model law, policy makers should determine the best approach to protect consumers, whether a state model law would offer a single standard, and whether other alternatives could provide consumers with better protections. If a model law is employed, it should not duplicate or conflict with existing state law.

State insurance regulators will also need to consider whether this type of legal framework delivers consumers better data security and breach notification than they receive today under existing state and federal laws. State insurance regulators and policy makers should also consider whether states will pass two different data security laws - one for insurance companies and another for all other businesses.

If it is determined that a state model law is the best way to employ a single standard for data security, the NAIC should consider the benefits of beginning the drafting process by hosting an open conversation about data security. This open conversation would provide an opportunity for regulators, consumers and industry to identify a shared philosophy and approach to deterring, detecting and preventing cyber fraud. A roundtable of this type will also help licensees (including producers) understand the public policy objectives that NAIC is trying to achieve and how we can reach those shared goals together. A consensus view among regulators, industry and consumer groups about shared goals and objectives for data security will more effectively protect consumers. That consensus, followed by an open, transparent process of review, public comment and approval, will allow us to produce an effective standard for data security and investigation and notification of a breach of data security.

Without an open, thoughtful and constructive conversation, the Preliminary Working and Discussion Draft runs the risk that its purpose and effect will be neither clear nor transparent, and a subsequent model law is likely not to be adopted by state legislatures. This concern poses a significant risk for state insurance regulators. In addition, if the NAIC were to adopt a subsequent model law, it is possible that many licensees would prefer a state-by-state data security framework rather than this proposed single standard.

As it continues to consider a standard for data security and investigation and notification of a breach of data security, we encourage NAIC to consult existing state and federal requirements that licensees are already required to follow. It may also be prudent for the NAIC to engage with and solicit comment about the Preliminary Working and Discussion Draft from state and federal regulators including state Attorneys General, the Federal Trade Commission (FTC), and Consumer Financial Protection Bureau (CFPB).

In addition to the general comments above, below are section-by-section comments based upon an initial review of the Preliminary Working and Discussion Draft.

Section 2

The phrase, “No other provision of state or federal law or regulation regarding data security or investigation or notification of a breach of data security shall apply to licensees subject to the provisions of this Act,” appears to attempt to work around the Supremacy Clause in order to preempt existing state and federal data security and investigation and notification of a breach of data security. The Preliminary Working and Discussion Draft would be more effective were it to compliment, rather than attempt to preempt federal law.

Section 3

The definition of "breach of data security" under Section 3(A) is different than the definition many states, which also include in their definition of "breach of data security" the unauthorized use or acquisition of sensitive personal information. The definition of "encrypted" under Section 3(D) should more clearly define encryption, which most states require as a minimum of 128-bit encryption.

In addition, the definition of "personal information" in section 3(G)(2)(f, g and h) is overly broad in that it includes "information that the consumer provides to a licensee to obtain and an insurance product or service…" and "information about the consumer resulting from a transaction involving an insurance product or service…" and "information the licensee obtains about the consumer in connection with providing an insurance product or service…" These definitions could be construed to include any combination of publicly available information. A better alternative would mirror existing definitions of Personally Identifiable Information (PII) found in typical notification statutes.

Section 4

We strongly encourage the NAIC to consider how to make the requirements of Section 4(A) scalable, particularly to small producers. By way of example, there were at least 5,454 title insurance producers who issued 50 or fewer title insurance policies in 2015, which represents an estimated 24 percent of title insurance producers in the United States.[3] The regulatory burden for each one of these small producers to "develop, implement and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards for the protection of personal information" is unreasonably excessive in that it does not provide guidance for how this requirement would be scaled to smaller producers. We appreciate that Section 4(C) recognizes that an information security program be "appropriate" to the size and complexity of the licensee; however, greater clarity about what constitutes an appropriate scale would greatly benefit small producers. We will continue to work with the NAIC to find ways for these small producers to continue to protect consumer information in an appropriate manner.

Compliance with Section 4(E) for small producers is equally difficult to envision. The physical security access controls required by Section 4(E)(1)(b) are today required by only the largest physical locations of bank vendors. In addition, 4(E)(1)(e), (f), (g) and (h) would also present extraordinary costs and challenges to small producers and could likely have the unintended consequence of forcing many to consolidate or out of business, merely to meet these standards. Consolidation would decrease consumer choice and competition.

Section 4(E)(1)(c) appears to provide a safe-harbor for encrypted electronic personal information, although it would be helpful to clarify what compliance protections are provided by an encryption of electronic personal information and match or exceed the encryption safe-harbor found in many state data breach notification laws.

---

[3] This is the total number of title insurance producers that obtained an Occasional Use Waiver from ALTA for use of ALTA's copyrighted policy forms. An Occasional Use Waiver is available for those who, during the previous calendar year, wrote title insurance on 50 or fewer transactions. For more information, see: http://www.alta.org/membership/policyformslicense_FAQ.pdf.

Section 4(E)(3) appears to mandate that licensees be required to join an Information Sharing and Analysis Organization (ISAO). We agree that information sharing is an important element of an effective cybersecurity program; however, many producers, particularly small producers, may lack the technological and monetary wherewithal to effectively participate in an ISAO. Moreover, no common set of standards or guidelines currently exists for ISAOs. Therefore, membership in an ISAO does not guarantee that the licensee is better positioned to protect itself or its customers from cybersecurity threats. While the federal government has continually encouraged companies to share cyber threat information, most recently with the adoption of the Cybersecurity Information Sharing Act of 2015, it bears emphasis that the federal government has routinely emphasized that ISAO participation and cyber information sharing by a private entity must be voluntary.

Section 4(G)(2) outlines oversight of Third Party Service Providers, which set contractual commitments by Third Party Service Providers that may be impossible, particularly for small producers to obtain, thereby unreasonably and unnecessarily limiting the ways a licensee can ensure the protection of personal information by its service providers. Small producers often lack the resources, expertise and business-leverage to impose and enforce this requirement.

Section 5

We encourage the NAIC to clarify the intent and purpose of this section of the Preliminary Working and Discussion Draft. This section requires the licensee to provide consumers with information regarding the types of personal information collected and stored by the licensee and third-party service providers, but does not specify the content of these disclosures, how this information should be communicated to consumers, or timing of these disclosures. Some producers may not have a website to comply with Section 5(B). In addition, the data a title insurance licensee may collect varies based on the real estate transaction, location, and producer. Methods of storing data may vary across businesses and locations.

Section 7

This section describes what steps a licensee should notify consumers in the event of a breach of data security. A Model Law should include, directly or through accompanying regulations, each adopting state's form of "Notice of Breach" for consumers. Section 7(A) allows a licensee to determine whether a data breach, "is reasonably likely to cause substantial harm or inconvenience" to consumers. These are subjective standards that are likely to result in different interpretations. These standards should be more clearly defined.

Section 7(B) a significant added regulatory burden for licensees, who are required to provide the commissioner 15 different types of information about a data breach that "is reasonably likely to cause substantial harm or inconvenience" to consumers within 5 days of identifying the breach. It is not clear how this requirement will benefit consumers. In addition, in the first days after discovery of a breach, the victim's focus must first be on an initial assessment of the cause and scope of the breach and the implementation of measures to stop the breach and minimize damage. Requiring such a stringent notification requirement to regulators on a very short timeline of 5 days takes resources and focus away from the licensee's efforts to stop the attack to focus on the reporting requirements, potentially resulting in greater harm or harm to increased numbers of consumers. For a licensee operating in multiple states, the issue is compounded by having to make multiple notifications containing notification requirements unique to each regulatory agency's requirements.

Section 7(D)(1) requires consumer notification within 60 calendar days. Today, where consumer notification is required under state law, most states require notification "as soon as possible without unreasonable delay" and provide for the tolling of the notification period subject to the legitimate needs of law enforcement. The manner of consumer notice is also far more restrictive and expensive than most state statutes which permit notice by telephone, substitute notice, website notice and notice to the media.

Section 7(D)(3) establishes an unworkable mechanism whereby the insurance commissioner of each state must approve any draft notice to consumers about a data breach. The section does not outline the factors by which the commissioner should evaluate a draft notice. In addition, it is unclear how a single data breach that affects consumers in multiple states would be treated under the Model Law. Typically, the state data breach notification laws are triggered when the NPI of a consumer resident of that state is compromised as a result of the breach. The Preliminary Working and Discussion Draft currently reads, the notification to the insurance commissioner is triggered because of the licensure of the title producer in that state. The state of residence of the impacted consumers is not a factor in the notification approval process. Take, for example, an agent that is licensed in 30 states, and assume that all 30 states adopt this law. If the agent sustained a breach, presumably impacting only the residents of one state, say Florida, the way the Preliminary Working and Discussion Draft currently reads, the agent is still required to notify the commissioner of the 29 other states as a licensee of that state, and, presumably, all 30 insurance commissioners would have to approve the notification letter before it went to Florida residents. We could not find in the Preliminary Working and Discussion Draft where the commissioner notification or notification approval requirements were only where the breach impacted consumers in that state. It appears that it is tied to the fact that the entity is a "licensee" in that state.

Section 8

This section describes the insurance commissioner's responsibilities after reviewing the licensees draft notification in a single sentence. Subsequent drafts should more clearly define what constitutes "the appropriate level of consumer protection following a data breach and for what period of time that protection will be provided" to ensure regulatory, licensee and consumer expectations align. This section should more specifically enumerate the consumer protections the commissioner may prescribe as well as an objective standard by which the commissioner should make that prescription.

Section 9 & Section 10

These sections provide the insurance commissioner with "power to examine and investigate into the affairs of any licensee..." and appear to establish a new process for hearings, witnesses, appearances and service of process related to a data breach at a licensee. This section appears to establish a means by which licensees litigate with the various departments of insurance and in the courts. This is an inappropriate and overly-litigious approach that does not protect consumers, but rather establishes a costly, punitive process if consumer data is breached.

Section 11

Licensees have reported a number of instances in which "confidential" documents have not been kept confidential. Although it is not discussed in this version, this section of the Preliminary Working and Discussion Draft should outline standards for data security and investigation and notification of breach of data security applicable to state insurance departments (and their contractors)

for consumer data in their possession through their examination and supervision of licensees.

Section 15

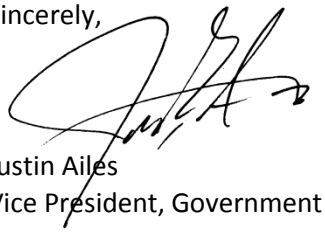
This section is inappropriate. If legislators in the various states see fit to create a private right of equity where one does not presently exist, that is the function of the legislature not an insurance commissioner. Section 15 establishes a new state-based private equitable right of action with attorneys' fees and costs. To our knowledge, no state insurance regulation exists today that provides this right of action. However, existing state and federal statutes afford a consumer with an adequate avenue to sue should he or she suffer actual harm. It is unclear why state insurance statutes should also provide private standing to sue in equity.

Section 20

The Effective Date should factor in an adequate phase-in period, allowing such covered entities a minimum 24 months necessary to: (i) come to understand the new requirements (presumably through industry educational events, articles and other guidance); (ii) hire appropriate third-party information security and privacy professionals; (iii) undergo testing and remediation; and (iv) undergo a risk assurance or certification process. NAIC should also commit to a robust national and local education and support program in order for licensees, particularly small producers to have a bona fide opportunity to become compliant.

ALTA looks forward to continuing to work with the NAIC to ensure that consumer data continues to be protected. Rather than be a punitive effort to punish licensees for being victims of criminals, a single standard for data security should be a joint effort to ensure information security for consumers. Should you have any questions about this comment letter, please contact me at justin@alta.org or 202-261-2937.

Sincerely,



Justin Ailes
Vice President, Government and Regulatory Affairs