Thanks Jennifer. I talked to my folks and the general thought is that they are supportive of version of 2A that you presented on the call last week. In terms of some potential enhancements here is our thought in a red line.

> Notwithstanding any other provision of law including [insert reference to state's general data security breach notification law], the purpose and intent of this Act is to establish the exclusive standards in this state for data security and investigation and notification of a data breach applicable to licensees, as defined in Section 3G. A licensee that is subject to and complies with the privacy, safeguards and breach notification provisions of Pub.L. 106–102, 113 Stat. 1338, enacted November 12, 1999, or to Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996, and any accompanying regulations, is deemed to be in compliance with the requirements of Section 4 and Sections 6C and D, to the extent such laws apply to personal information maintained by licensees

Another topic that we did not get to last week that I wanted to bring up is in the definition of personal information. The general thought is that if the information obtained in a breach is also generally available to the public then it should not trigger the breach notification requirements. Here is our thought for a change to the end of the definition of personal information:

The term "personal information" does not include publicly available information that is lawfully made available to the general public and obtainable from federal, state, or local government records, commercially available products or widely distributed media.

Another option would be to incorporate this type of language into the definition of harm or inconvenience. The idea would be that a breach that results in personal information being lost that is also available from a public or commercial resource does not cause harm.

Best,

Steve

Steve Gottheim | Senior Counsel | American Land Title Association | 1800 M St N.W., Suite 300 South | Washington, DC. 20036 | Ph: (202) 261-2943 / (800) 787-ALTA (2582) (ext. 230) | Fax: (202) 223-5843 / (888) FAX-ALTA (239-2582)

On behalf of the California Department of Insurance and Commissioner Dave Jones, I want to thank you for organizing today's ad hoc cyber model law drafting group call. The adoption of a NAIC Cybersecurity Model Law is a very important objective and we are grateful for this opportunity to work with you as we develop this draft.

Towards the end of the call, you requested that we share with you California's current statutory requirements as they relate to the events that trigger an insurer's obligation to issue a breach notice to affected personnel.

The "Harm" Trigger

California Civil Code section 1798.82(a) requires a business to disclose any breach of the security of its systems to any resident of California when that resident's "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

The ad hoc drafting group is currently considering text which would leave it to the discretion of the insurer so that it would only need to disclose a breach of its systems if, in the opinion of the insurer, the breach is "is reasonably likely to cause substantial harm or inconvenience to the consumers…"

A quick comparison of California's current law with the ad hoc drafting proposal shows just one of many reasons why it is very likely California's Legislature would reject an NAIC cyber model law such as the one under discussion today. It seems likely that, like California, other states' laws could also prevent the adoption of a "harm" trigger.

Section 2 (Purpose and Intent) and the Risks to Uniformity

As the "harm" trigger example illustrates, many states will not be able to adopt a model law that is similar to the ad hoc group draft, because some standards will fundamentally conflict with their own state laws. We strongly urge you to reconsider Section 2 of the draft model law so that it will serve as a "floor" rather than a "ceiling" that states may adopt. A "floor" will permit a certain minimum level of uniformity of standards that insurers can rely upon in developing their cybersecurity programs for compliance with state laws. The establishment of a "floor" as opposed to a "ceiling" also carefully balances insurers' desire for uniformity against our country's long-standing policy in the McCarran Ferguson Act that the regulation of insurance is a matter best left to the individual states to decide.

Importantly, although the insurer trades have emphasized the need for a uniform model law, the language discussed today actually creates more uncertainty than clarity regarding uniformity. This is because the ad hoc group draft incorporated insurers' request to create a "safe harbor" for insurers that comply with Health Insurance Portability and Accountability Act (HIPAA) and Gramm Leach-Bliley Act (GLBA). This safe harbor is unworkable and would inject confusion, because under both HIPAA and

GLBA, states are *expressly authorized* to adopt standards that are stronger than those established under federal law.

Thus, for example, in Title 15, United States Code section 6807, GLBA expressly provides that a state law is not inconsistent with GLBA "if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subchapter…" Similarly, with regard to HIPAA, the Department of Health and Human Services specifically provides that HIPAA does not preempt a state's law if a determination is made that the state law meets one or more conditions, including: 1) the law is necessary "to ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation," or 2) "[t]he provision of State law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter." (45 Code Fed. Regs. section 160.203, subds. (a)-(b).)

Although the insurer trades, no doubt, sought to establish GLBA and HIPAA as "safe harbors" to prevent any stronger, non-uniform state protections, each of these federal laws expressly allow states to do precisely that. If the ad hoc committee recommends these revisions to Section 2, the model law will become less clear and the "safe harbor" will ultimately prove to be illusory.

Proposed Language for Section 2

For the foregoing reasons, we respectfully request that the ad hoc committee propose language that is similar to the "alternate suggested language" that the Georgia Department of Insurance recommended on page 2 of their September 19, 2016 comments:

"Notwithstanding any other provision of law including [insert reference to state's general data security breach notification law], the purpose and intent of this Act is to establish the
exclusive minimum standards in this state for data security and investigation and notification of a data breach applicable to licensees, as defined in Section 3G. This Act shall not be construed as superseding, altering, or affecting any statute, regulation, order
or interpretation of law in this state, except to the extent that such statute, regulation, order or interpretation is inconsistent with the provisions of this Act and then only to the extent of the inconsistency. A state statute, regulation, order or interpretation is not inconsistent with the provisions of this Act if the protection such statute, regulation, order
or interpretation affords any person is greater than the protection provided under this Act."

Once again, we thank you for your leadership and continued efforts on behalf of insurance consumers and the regulated entities. We also thank you for your

consideration of our comments above and we look forward to a continuing, cooperative and constructive dialogue as we work to improve this draft of the NAIC Model Law.

Sincerely,

-Bryant

Bryant W. Henley, Assistant Chief Counsel, Legal - Government Law Bureau | California Department of Insurance | 300 Capitol Mall - Suite 1700, Sacramento, CA 95814 | bryant.henley@insurance.ca.gov | ☎Office: (916) 492-3558 | Fax: (916) 324-1883

Jennifer:

Good morning, and thanks very much for the email regarding the definition of "data breach." In addition to addressing that question, I wanted to also address a couple of other Section 3-related concerns too. I hope this is helpful, and I am happy to chat in more detail at any time about any of these issues.

Thanks again.

Wes

Definition of "data breach"

We recommended revising the definition of the "data breach" along these lines, and I hope this makes sense.

> *The term "data breach" does not include: (1) the unauthorized acquisition, release or use of ~~encrypted~~ personal information that is encrypted or otherwise protected by another method that renders the information unreadable, unusable, inaccessible, or indecipherable if the encryption or other protective process or key is not also acquired, released or used without authorization; (2) …*

Definition of "third-party service provider"

In our written comments to the task force, we also addressed the agent community's concerns with the definition of "third-party service provider. I have copied the text from our September letter below:

> *IIABA urges the task force to make clear that one licensee cannot be considered the third-party service provider of another licensee for purposes of this model. Under the proposal, every licensee will have its own independent data security, investigation, and breach notification obligations, and there is no reason why the requirements of Section 4(F), which relate to a licensee's relationship with a third-party service provider, should apply to a licensee-to-licensee relationship.*
>
> *The revision described above is imperative to the independent agent community, and we offer this recommendation to eliminate confusion about whether an insurer could be a service provider of an independent insurance agent or vice versa. In the independent agent context, the producer (and not the insurer) owns and has exclusive control over customer information. This longstanding and well-established doctrine is confirmed in agent-company contracts, and some jurisdictions have statutorily codified the principle as well.*
>
> *As currently drafted, the proposed model identifies insurers as third-party service providers of independent insurance agents and imposes a host of unintended burdens and requirements on producers as a result. This problem arises in part because the draft defines "third-party service provider" to include an entity "that contracts with a licensee to … have access to personal information under the licensee's possession, custody, or control." Given the clear ownership rights (or control) that independent agents have to their client information, this definition would make insurers the third-party service providers of agents. As a result, the draft would also make an independent agent responsible for any failure by one of its carriers to protect the personal information the agent shared with the company, require the agent to investigate any data breach suffered by the insurer, and mandate that the agent provide the required notices to regulators and consumers. Independent agents should not be responsible for satisfying the requirements of the model when personal information is shared with an insurer and that insurer subsequently suffers a breach, and we do not believe such an outcome is intended by the task force. For the reasons identified above, we urge you to revise the definition of "third-party service provider" to exclude licensees.*

To address these concerns, we propose the use of the following definition instead.

> *"Third-party service provider" means a person or entity, other than a licensee, that contracts with a licensee to maintain, process, store or otherwise have access to personal information for the licensee.*

Use of the terms "custody" and "control"

In several instances, the proposed model also includes definitions and extends requirements to those who are in "possession, custody, or control" of personal information, and the use of the words "custody" and "control" creates confusion about who is the responsible party. This construction and the use of these terms, for example, creates unique challenges for the independent agency system, and it would make independent agents responsible for the investigation of data breaches suffered by insurers. Independent insurance agents own and control their customer information, so the draft would make a producer the responsible party in the event that personal information is communicated by the agent to another party (i.e. an insurer) and that party suffers a breach. We believe independent agents should not be responsible for satisfying these requirements when personal information is shared with an insurer and that insurer subsequently suffers a breach, and we suspect that this outcome was not intended by the task force. There may be a variety of ways to address this problem, but we have proposed deleting the various references to "custody or control" from the model (including the use of those terms in the definitions of "consumer" and "third-party service provider").

Jennifer McAdam
Legal Counsel
National Association of Insurance Commissioners

Ms. McAdam-

In the discussion this past Tuesday, November 15th, a potential issue may have been passed over that is a predicate to Section 2.

Starting with, what is a Data Breach?

> **"Data breach" means the unauthorized acquisition, release or use of personal information that is reasonably likely to result in harm or inconvenience to a Consumer."**

which leads back to the underlying definition of PI, which contains this exclusion:

> **"The term "personal information" does not include publicly available information that is lawfully made available to the general public and obtained from federal, state, or local government records; or widely distributed media."**

Licensees store and must safe keep PI obtained directly from Consumers. Their Privacy Policies require it. Unfortunately Consumers believe "everything about me is private," and that they are the sole source of private and confidential PI. We believe most, and in time perhaps all, demographic parameters obtained by a Licensee's application process are ALSO publicly available. The Model Law's exclusion of publicly available information may present, after a data breach, a Licensee with an avenue to readily demonstrate public availability and escape Notification requirements. In addition, unfortunately, government databases have been breached and the misappropriated data is for sale on the dark web. Does that unconventional dark web availability mean misappropriated data is "publicly available?"

From different vantage point... Is anonymized data PI?

Academic research demonstrates PHI, which has been anonymized (for use in marketing or for other purposes)

(a) by expunging first name and last name, and

(b) perhaps also by expunging other parameters, such as SS#, DriversLicense#, DOB, etc.,

can often be employed with powerful analytics to accurately identify the underlying person. This *big data* capability potentially compromises the utility of the Model Law's definition of PI. Does the Model Law contemplate triggering Notification after a data breach that only exposed anonymized data?

We appreciate the open and transparent Model Law drafting process and appreciate our opportunity to submit comments during the process. Thank you for your consideration.

Respectfully submitted,

T. Robin Cole, III
President

The Rite Group
5303 Old Cape Rd East
Jackson, MO 63755
(573)-334-4439 - office
(573) 200-3058 - cell
(573) 334-3471 - fax