ABA Comments dated January 9, 2017

American Bankers Association

Building Success. Together.

Sarah Ferman
Senior Government Relations Representative
P: 202-663-5510
SFerman@aba.com

January 9, 2017

Superintendent Elizabeth Dwyer
Director Anne Melissa Dowling
Co-Chairs, Cybersecurity Insurance Data Security Model Law Drafting Group
National Association of Insurance Commissioners
1100 Walnut Street
Suite 1500
Kansas City, MO 64106-2197

Attn: Tiffany Fosgate (TFosgate@naic.org)
Sara Robben (SRobben@naic.org)

Re: Insurance Data Security Model Law Drafting Group –
Review of Sections 2 and 3 of the Insurance Data Security Model Law)

Dear Superintendent Dwyer and Director Dowling:

On behalf of the American Bankers Association, we provide the following comments to the Insurance Data Security Model Law Drafting Group concerning Sections 2 and 3 of the December 20, 2016 version of the Insurance Data Security Model Law ("draft model law"). ABA is not a member of the Drafting Group, so we provide these comments as our *sole means* of offering direct input to the drafters.

The ABA is the leading trade association for banks selling insurance products and services. Its members include bank-affiliated insurance agencies and insurance companies that work with those agencies. Consequently, its members encompass entities that are subject to both Federal and state information sharing and cybersecurity requirements.

Sections 2 (Purpose and Intent) and 3 (Definitions)

We fully support the following language in Section 2A of the draft model law: "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." The language recognizes that the most effective way for a *single* state to regulate data breaches and protect the insurance-buying public in case of a data breach is to establish a single set of standards regarding data security and investigation and notification of a data breach. Section 2A does just that.

But as important is that there be a single set of standards across *all* states, and that can be effected only if the NAIC is on record supporting that approach. Therefore, we request that the following drafting note be added to the draft model law after Section 2, to get all states on board:

> The intention of the National Association of Insurance Commissioners is that this model law establishes a *single, uniform, multi-state* set of protections and requirements regarding data security and investigation and notification of data breach applicable to all licensees. Because a possible data breach could affect consumers in more than one state, states should adopt the model law *without material deviation from its terms.*

We also support language in Section 2B that states that compliance with the Gramm-Leach-Bliley Act's privacy and information security program requirements, as well as with its data breach notification requirements,[1] including any related regulations, is deemed to be compliance with Section 4 of the draft model law (Information Security Program) and with Section 6D – with one caveat: The type of personal information to which these "deemed compliance" provisions apply should be the same as the type of personal information protected by the privacy provisions in the Gramm-Leach-Bliley Act, as adopted by the NAIC.

Specifically, the draft model law states that the "deemed compliance" provision that would govern a licensee's information security program is only available for a licensee to the extent the Federal law and regulations "apply to all *personal information*, as defined in Section 3H [of the Model Law], in whatever form maintained by that licensee." (Emphasis added.) Section 3H currently defines "Personal Information" as the aggregate of five types of listed information. In comparison, Federal privacy law, as implemented by state insurance regulations for insurance licensees, applies to customer "nonpublic personal information," or NPI. NPI is defined in Section 4S of NAIC Model Regulation No. 672, *Privacy of Consumer Financial and Health Information Regulation.* The definition of nonpublic personal information in Model No. 672 should replace the current definition of "Personal Information" in the draft model law.

Note, also, that the current version of the draft model law includes the following Drafting Note at the end of Section 2: "This model law is intended to supplant the provisions of the NAIC's Standards for Safeguarding Consumer Information Model Regulation (#673)." Section 2B of Model No. 673 defines "Customer information" via reference to Section 4S of Model No. 672, the definition of "nonpublic personal information." Consequently, for purposes of consistency, and to employ a definition of information that licensees are very familiar with, we recommend that the Drafting Group define "Personal Information" in the draft model law via reference to the definition of "nonpublic personal information" in Section 4S of Model No. 672.

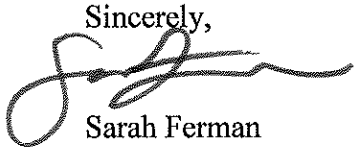
---

[1] Primarily Title V of Pub. L. No. 106-102, 113 Stat. 1338, enacted Nov. 12, 1999, codified at 15 U.S.C. §§ 6801-6809.

An additional advantage of revising the definition of "Personal Information" in this manner is that the scope of information covered by the draft model law would be the same as that covered by the Gramm-Leach-Bliley Act privacy regulations[2] that are administered by the Consumer Financial Protection Bureau, which apply to various types of banks. Because a data breach in the bank-insurance context could impact both a bank and an affiliated insurance agency with respect to regulatory compliance involving information sharing and data security, the proposed change to the definition of Personal Information in the draft model law would make Federal regulations consistent with state requirements.

If you have any questions regarding this letter, please contact me or our counsel, Chrys Lemon, at (202) 659-3900 or cdl@mcintyrelf.com.

Sincerely,



Sarah Ferman

[2] 12 C.F.R. Part 1016. See 12 C.F.R. § 1016.3(p) (defining "nonpublic personal information").

Hemisphere Cyber Risk Management Comments

Carter Schoenberg (Hemispherecybersec) comments:

I have some ideas I would like to provide the task force as my experience and expertise in this area bears direct relevance. There was a scenario highlighted that involved Google.

Whether you use Google, AWS, or AZURE, while these organizations provide SaaS and IaaS, the people and organizations buying are still responsible for locking it down. Even in a FedRAMP setup, the controls the buyer transfers to the CSP if roughly 68% of the total required controls to get an authorization to operate. The remaining 32+% are the responsibility of the system owner.

So if we use the Google scenario, and we have an "agent" named John Smith using a CSP vs. maintaining on a laptop,. if Google gets hit, all they will know is whether John Smith's PII was compromised in some manner. It would not be able to stipulate beyond that.

Regardless If you are using a CSP or on premise solution, the majority of firms breached (something like over 66%) are notified by an external party (FBI, local law enforcement, etc.). So if John Smith is a State Farm agent in Vienna, VA, the chance he will know he has been breached on his own is very VERY low.

I do believe there is an opportunity to assess how Carriers may stipulate terms and conditions or otherwise legally binding agreements as to how to ensure the protection of PII or other highly sensitive information. Does the NAIC have any purview on how the industry within each state addresses these types of relationship agreements?

Lastly, do you feel there is an opportunity to hold an out of band dialogue with yourself and other key stakeholders on this topic as it I do believe this will add value to the discussions on how to "best craft" sections 4F, 6B and 6E.

Carter Schoenberg, CISSP
President and Chief Executive Officer

North American Operations
HEMISPHERE Cyber Risk Management, LLC.
carter.schoenberg@hemispherecybersec.com
(703) 881-7785

Hemisphere Cyber Risk Management Comments

4 F. Oversight of Third-Party Service Provider Arrangements

The licensee shall contract only with third-party service providers that are capable of maintaining appropriate safeguards, as required by the state laws in which the licensee is located or other statutory authority, to protect~~for~~ personal information in the licensee's possession, custody or control. ~~, and t~~The licensee shall be responsible for any failure by such third-party service providers to protect personal information provided by the licensee to the third-party service providers consistent with this Act.

The licensee shall be responsible for ensuring all terms and conditions or service level agreements (including limitations of liability and ability to properly fund all costs associated with the breach) adequately describe the approach a third-party service provider will meet, at a minimum, the requirements set forth herein. In instances where these requirements cannot be met, the licensee shall assess proper compensating controls to reduce the risk exposure of a data breach.

6B. Notification to the Commissioner Notwithstanding the responsibilities prescribed in Sections 5A and 6A of this Act, no later than three (3) business days after determining that a data breach has occurred, the licensee shall notify the commissioner that a data breach has occurred. The licensee shall provide as much of the following information as possible:

(1) Date of the data breach;

(2) Description of the data breach, including how the information was exposed, whether lost, stolen, or breached, unless otherwise precluded from impeding a criminal investigation;

(3) How the data breach was discovered;

(4) Whether any lost, stolen, or breached information has been recovered and if so, how this was done;

(5) The identity of the source of the data breach;

(6) Whether licensee has filed a police report or has notified any regulatory, government or law enforcement agencies and, if so, when such notification was provided;

(7) Description of the type of information lost, stolen, or breached (equipment, paper, electronic, claims, applications, underwriting forms, medical records etc.);

(8) Whether, if the information was encrypted, the encryption, redaction or protection process or key was also acquired without authorization;

(9) The period during which the information system was compromised by the data breach;

(10) The number of total consumers and consumers of each state affected by the data breach;

(11) The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;

(12) Identification of efforts being undertaken to remediate the situation which permitted the data breach to occur;

Comment [U1]: I see this all the time. You must do A,B, and C but never a requirement to demonstrate how you can afford to offset the costs. If they cannot fund it and go out of business, this is a risk to the licensee. I see RFPs that stipulate (in addition to E&O, D&O, GL – that the awardee must have $X in data breach response coverages for 1st and 3rd parties)

Comment [U2]: In numerous cases, Law Enforcement Agencies (LEAs) do not want this information disclosed as it could handicap their investigation or ability to prosecute.

A case I am working right now addresses 35 states and 5 have reporting requirements if only a single record applies. Mass. Has a requirement that suggest that the notification to the consumer CAN NOT convey the tools tactics and techniques leveraged by the attacker.

The proposed language in 4f should satisfy this.

Comment [U3]: Same comment

Comment [U4]: Is this for benchmarking purposes or to assess potential negligence? The avg. time a system is organized before realization is over 250 days.

(13) A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the data breach; and

(14) Name of a contact person who is both familiar with the data breach and authorized to act for the licensee. The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the commissioner concerning the data breach.

6E. Notice Regarding Data Breaches of Third-Party Service Providers

In the event of a data breach in a system maintained by a third-party service provider, the licensee shall comply with Section 6A through D. The computation of licensee's deadlines shall begin on the day after the third-party service provider notifies the licensee of the data breach or the licensee otherwise has actual knowledge of the data breach, whichever is sooner.

Comment [U5]: No challenge on wording but our last call conveyed stakeholders took this as ownership. A system maintained by AZURE or AWS is still "Owned" by the system owner.

Comment [U6]:

Section 7. Consumer Protections Following a Data Breach

After reviewing the licensee's data breach notification, the commissioner shall prescribe the appropriate level of consumer protection required following the data breach and how long that protection will be provided. The commissioner may order the National Association of Insurance Commissioners 9 licensee to offer to pay for twelve (12) months or more of identity theft protection for affected consumers, pay for a credit freeze, or take other action deemed necessary to protect consumers. Drafting Note: Many states have statutes providing that a consumer reporting agency cannot charge a fee for a credit freeze on a consumer file when the consumer is a victim of identity theft, which is shown by providing a police report. For an example, see Tex. Bus. & Com. Code § 20.04(b). As an alternative to having the licensee pay for the credit freeze, a state should consider referencing that law and providing that the credit freeze is free for consumers after the data breach is reported to law enforcement by the licensee, by showing a data breach notification letter from the licensee. The state may also need to amend its free credit freeze law to ensure this is covered. If the data breach has affected consumers in other states, the commissioner shall, consistent with the requirements of [reference to statute describing the commissioner's general powers] and with the circumstances of the data breach as they affect consumers in this state, cooperate with the insurance regulators of those states in prescribing the appropriate level of consumer protection described in the previous sentence.

Comment [U7]: This will be critical to convey as some states do not require and NAIC is now stipulating you must. Great stuff here.

~~The licensee shall:~~

~~(1) Select and retain contract only with third-party service providers that are capable of maintaining appropriate safeguards for the personal information at issue;~~

~~(2) Require in the licensee's possession, custody or control, and the licensee shall be responsible for any failure by such third-party service providers to do the following, by contract:~~

~~(a) Implement and maintain appropriate safeguards for theprotect personal information at issue, including those security measures listed in [Section 4E(1), Risk Management].~~

~~(b) Notify licensee within three (3) calendar days of a discovery of a breach of data security in a system maintainedprovided by the licensee to the third-party service provider that has been contracted to maintain, store, or process data containing personal information on behalf of a licensee;~~

~~(c) Indemnify licensee in the event of a cybersecurity incident that results in loss;~~

~~(d) Allow licensee or its agents to perform cybersecurity audits of the third-party service provider; and~~
~~(e) Represent and warrant its compliance with all requirements; and~~

~~Oversee or obtain an assessment of the third-party service provider's compliance~~providers consistent with ~~contractual obligations, where appropriate in light of the licensee's risk assessment~~this Act.

Idaho Department of Insurance Comments

Regarding the following added language in Section 6.E:

In the event that the third-party service provider agrees to send the notices, licensee will licensee will confirm and document that this was completed.

The drafting group might want to consider revising that sentence to something along the following:

In the event that the third-party service provider agrees to send the notices, licensee will confirm and document that the notices were actually sent and that the notices satisfy the requirements expressed in this section.

Thomas A. Donovan
Deputy Director
Idaho Department of Insurance
700 W. State St. 3rd Floor
PO BOX 83720
Boise, ID 83720-0043
Tel. 208-334-4214
Cell 208-841-5437
Fax. 208-334-4398
tom.donovan@doi.idaho.gov
www.doi.idaho.gov