American Bankers Association

Building Success. Together.

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

September 15, 2016

Commissioner Adam Hamm, Chair
Cybersecurity (EX) Task Force
National Association of Insurance Commissioners
1100 Walnut Street
Suite 1500
Kansas City, MO 64106-2197

Attn: Sara Robben (Srobben@naic.org)

**Re: Insurance Data Security Model Law –**
**Comments of the American Bankers Association**

Dear Commissioner Hamm:

On behalf of the American Bankers Association (ABA), I provide the following comments to the Cybersecurity (EX) Task Force concerning version 2 of the Insurance Data Security Model Law ("Draft Model Law"). We appreciate the work the Task Force has done to significantly improve the Draft Model Law, but the American Bankers Association has three primary concerns about the revised draft and some specific comments on issues the Draft Model law addresses that are already addressed in another NAIC Model Regulation.

**Primary Concerns**

ABA has three major concerns about the Draft Model Law. First, it is important that the Model Law be drafted so that the model is the *exclusive* word on insurance data security and breach notification and remediation in each state's body of laws and regulations. Section 1 of the Draft Model Law contains the following language, which is right on target: "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." (Emphasis added.) But Section 2 eviscerates Section 1 by stating the following:

> 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.

The language in Section 2 must be deleted to achieve the stated objective of exclusivity. Additionally, there is a drafting note at the end of Section 6 that contains language that is contrary to the objective of exclusivity: "Section 5 and Section 6 may be duplicative of current state law. Each state should conduct its own analysis to determine whether or not Section 5 and Section 6, in who[le] or in part, are necessary to be included." The drafting note needs to be deleted, because it anticipates that a state will have other laws that address insurance data security.

Second, the Draft Model Law should ensure *uniformity* among state data security laws. It should not provide states with the authority to have standards that differ from the standards of other states. Section 6.D.(2) of the Draft Model Law requires a licensee to provide the commissioner with a draft of any proposed breach notification, for review before it is sent to consumers. Under Section 7, the insurance commissioner is "(i) directed to prescribe the appropriate level of consumer protection required after a data breach and how long the protection will be provided; and (ii) granted the authority to order the licensee to offer to pay for 12 months or more of identity theft protection, to pay for a credit freeze, or to take other action deemed necessary to protect consumers." This language will likely result in non-uniformity among the states regarding data security, breach notification and remediation. Given that the adoption of the Model Act is an unknown in each State's own legislative agenda, failure to ensure exclusivity could create a serious financial and compliance burden on licensees that operate in multiple states. Third, the Draft Model Law should be *practical.* Elimination of the harm trigger could result in consumers being unnecessarily alarmed by notices, when the probability of harm is low. The Draft Model Law must have a clear, common sense harm trigger.

**Additional Comments**

We recommend that the NAIC's Standards for Safeguarding Customer Information Model Regulation (No. 673-1) ("Safeguarding Model Regulation") be rescinded, as it addresses several general topics related to information security in a manner very similar to (in some cases, verbatim with) those contained in the Draft Model Law. The following are examples of overlap between the Draft Model Law and the Safeguarding Model Regulation.

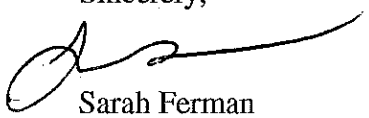
| Security and Breach Issue | Draft Model Law | Safeguarding Model Regulation |
|---|---|---|
| Establish an Information Security Program | § 4 | §§ 3 and 4 |
| Conduct a Risk Assessment | § 6 | § 4(C) |
| Manage Risk | § 4(D) | § 7 |
| Oversee Third Party Service-Provider | § 4(F) | § 8 |

| | | |
|---|---|---|
| Arrangements | | |
| Adjust the Program as needed | § 4(G) | § 9 |

Finally, because the Safeguarding Model Regulation implements the requirements of the Gramm-Leach-Bliley Act,[1] the Draft Model Law should include a sentence that states that compliance with it shall constitute compliance with Section 501 of the Gramm-Leach-Bliley Financial Modernization Act (15 U.S.C. § 6801) as well as any other state laws or regulations that implement that law.

We appreciate the opportunity to comment on the Draft Model Law.

Sincerely,



Sarah Ferman

[1] Section 505 of the Gramm-Leach-Bliley provides that state insurance regulators shall implement and enforce requirements concerning data security. *See* 15 U.S.C. § 6805(a)(6), (b)(2)