MCINTYRE & LEMON, PLLC

ATTORNEYS AND COUNSELORS AT LAW
MADISON OFFICE BUILDING
1155 15TH STREET, N.W.
SUITE 1101
WASHINGTON, D.C. 20005
TELEPHONE (202) 659-3900
FAX (202) 659-5763
WWW.MCINTYRELF.COM

March 23, 2016

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

Dear Chairman Hamm:

On behalf of the American Bankers Insurance Association ("ABIA"),[1] we provide the following comments to the Cybersecurity (EX) Task Force concerning the draft Insurance Data Security Model Law ("draft Model Law").

Meeting the challenges of data security in the most effective way requires a consistent, uniform regulatory approach to data security, and to the investigation and notification of a breach of data security, that works well across a variety of business sectors – not just those involved in the business of insurance. Therefore, it is important for the Task Force to recognize that existing federal and state regulatory regimes establish requirements for data security, and that Congress continues to consider broad legislation concerning data security and the investigation and notification of a breach of data security. While ABIA does not oppose the development of an Insurance Data Security Model Law, we urge the Task Force to work to ensure that the draft Model Law is consistent with existing data security law, and that it anticipate the development of a federal data security regime that would apply across all business sectors.

[1] The ABIA is the leading trade association for banks selling insurance products and services. ABIA's members include bank-affiliated insurance agencies and insurance companies that work with those agencies.

Existing Laws and Regulations

Insurance licensees are already subject to several laws and regulations concerning data security. Section 501 of the Gramm-Leach-Bliley Act ("GLBA") requires financial institutions, including insurance companies and agencies, to establish procedures to ensure the "security and confidentiality of customer records and information" and to "protect against any anticipated threats or hazards to the security or integrity of such records."[2] The GLBA anticipated that state insurance regulators would establish and enforce a regulatory regime for insurance licensees that is consistent with the GLBA requirements,[3] and the NAIC's Standards for Safeguarding Customer Information Model Regulation (No. 673-1) does just that. It requires an insurance licensee to develop and implement a comprehensive written information security program that includes risk assessment protocols and oversight of service providers.[4] These requirements are similar to those set forth in Section 4 of the draft Model Law. Therefore, the Task Force should consider revising the draft Model Law so it does not duplicate the requirements of the other model. That approach would be better than removing Model No. 673-1 from the NAIC's model law inventory, given that a majority of the states have adopted Model No. 673-1 in some form.

The NAIC also has adopted the Privacy of Consumer Financial and Health Information Regulation (No. 672-1), which is also applicable to insurance licensees. Developed based on the information privacy provisions in Title V of the GLBA,[5] the model regulation sets forth restrictions on insurance licensees' disclosure and use of customer nonpublic personal information. The Task Force should also consider that model as it goes forward.

Additionally, Part C of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[6] required the Department of Health and Human Services to adopt national standards for the electronic transmission of health information, including standards for the establishment of safeguards for the security of health information.[7] The issued regulations[8] apply to health plans, which includes some licensees – again raising the potential for conflicting regulatory requirements.

Finally, in December 2015, the President signed H.R. 2029, the Cybersecurity Information Sharing Act.[9] It permits private companies to monitor their networks for cybersecurity purposes, take defensive measures to stop cyber attacks, and share cyber threat information with each other and with the government. Its provisions also should be considered.

---

2 15 U.S.C. § 6801.
3 15 U.S.C. §§ 6801(b), 6805(a)(6).
4 NAIC Model Regulation No. 673-1, §§ 3-8.
5 15 U.S.C. §§ 6801 *et seq*.
6 42 U.S.C. §§ 1320d *et seq*.
7 42 U.S.C. § 1320d-2(d).
8 45 C.F.R. Part 164.
9 Pub. L. No. 114-113, Div. N.

Preemption

Given the breadth of the existing federal and state requirements regarding data security, the Task Force should reconsider the preemption language in Section 2 of the draft Model Law. Section 2 states that "[n]o 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." (Emphasis added.) That language raises an important question: Would the language in Section 2 have any actual effect on federal preemption of the draft Model Law? If a federal law expressly preempts, or is judged to preempt, a state law, the fact that the state law says it is not subject to federal preemption would have no legal effect.

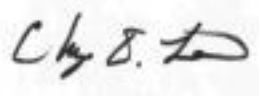
The preemption issue also is relevant to ongoing efforts to enact Federal data security and breach investigation/notification law. ABIA and its parent, the American Bankers Association, support Congressional legislation that requires companies to comply with uniform, nationwide standards for safeguarding customer information and investigating and responding to data breaches. Several data security bills are still pending before Congress, and some have preemption language in them. Specifically, the Gramm-Leach-Bliley Act sets a floor at the Federal level and permits the states to have more strenuous requirements. The Data Security Act of 2015 (H.R. 2205 and S. 961), on the other hand, would replace state laws with a Federal data protection, investigation and notification standard. As it is currently drafted, H.R. 2205 provides that its enforcement would be by the insurance regulator of the state of domicile of the licensee, or the lead state insurance regulator in the case of an insurance group.

We believe, therefore, that Section 2 of the draft Model Law should be revised to remove the reference to "federal" law and regulations.

ABIA plans to continue to be involved in the Task Force's work on the draft Model Law, but we urge the Task Force to work to develop a model law that is consistent with existing law and regulations, and that anticipates development of a broad Federal regulatory regime that governs data security and the investigation and notification of data breaches.

Sincerely,

McINTYRE & LEMON, PLLC



Chrys D. Lemon