

Via Electronic Mail to srobben@naic.org

September 16, 2016

The Honorable Adam Hamm
Chair, NAIC Cybersecurity (EX) Task Force
North Dakota Insurance Department
600 E. Boulevard Avenue
Bismarck, North Dakota 58505-0320

The Honorable Raymond G. Farmer
Vice Chair, NAIC Cybersecurity (EX) Task Force
South Carolina Department of Insurance
P.O. Box 100105
Columbia, South Carolina 29202

Re: Joint-Trade Association Comments on the NAIC's insurance Data Security Model Law

Dear Commissioner Hamm and Director Farmer,

On behalf of the undersigned trade associations, we are writing to express our views to the National Association of Insurance Commissioners ("NAIC") Cybersecurity (EX) Task Force ("Task Force") regarding the 8/17/16 draft (current draft) of the proposed new NAIC Model Insurance Data Security Law ("Model Law"). We acknowledge and thank the Task Force for the improvements reflected in the current draft of the Model Law. However, we continue to have fundamental and serious concerns with the current draft.

Accordingly, we strongly urge the Task Force to modify the current draft to: 1) ensure exclusivity within states so that the Model Law is the sole state data security and breach notification law applicable in a state, 2) ensure uniformity among state data security and breach notification laws, and 3) ensure workability of the Model Law.

We believe these issues are fundamental and need to be addressed for possible support of the Model Law. We also note that while these three items are threshold issues for the undersigned, there are additional issues which individual groups and organizations consider to be fundamental threshold issues which must also be addressed by the Task Force. We address those issues and proposed solutions in our individual trade association letters.

We remain committed to working with the Task Force as it continues to craft meaningful and workable data security and notification standards for the insurance industry.

Our specific comments on the Model Law are below.

Ensuring Exclusivity in a State

It is essential that any model law provide the exclusive state standard for data breach notification and data security within each state. However, language in Section 2 of the current draft may make it so that the Model Law may be construed not to provide the exclusive state standard. The language states, "[t]his 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.”

It is unclear how a licensee would be able to determine whether the provisions of the model are inconsistent with, or less strict than, those of an existing breach notification law. It is also unclear how the above referenced sentences are reconciled with the first sentence of Section 2 of the model which reads, “Notwithstanding any other provision of law including [insert reference to the state’s general data security breach notification law], the purpose and intent of this Act is to establish the exclusive standards in the state for data security and investigation and notification of a data breach applicable to licensees ...” These two portions of Section 2 contradict one another, with the former stating that the model is not intended to replace any existing state statute and the latter explicitly stating the model is intended to be the exclusive standard in the state.

Further, the inclusion of the drafting note at the end of Section 6 is also contrary to the goal of exclusivity. The drafting note states, “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 whole or in part, are necessary to be included.” This drafting note also would undercut exclusivity. Therefore, we strongly recommend the deletion of the two sentences in Section 2, commencing: “[t]his Act shall not be construed as superseding, altering, or affecting any statute, regulation, order or interpretation of law in this state ...” and the drafting note in Section 6.

Ensuring Uniformity in the States

We commend the NAIC for undertaking this effort to address the current patchwork of 47 differing breach notification statutes. Nevertheless, the current draft proposes requirements that would significantly undercut uniformity among states. Under Section 6.D.(2) of the current draft, a licensee is required to provide the commissioner a draft of the proposed consumer notice and the commissioner is granted the right to review the proposed communication before it is sent to consumers to ensure compliance with the Act. Under Section 7, the 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.”

These requirements would undercut the goal of uniform standards, to be uniformly enforced and provide level consumer protection, among the states. If the current draft is enacted across the country and there is a nationwide breach, a licensee may be required to send a draft of its proposed consumer notice to 50 different commissioners, wait for their review and possible edits to the notice, and then may be required to send 50 different consumer notices with state specific remediation. As a result, in connection with the same nationwide breach, consumers in different states may receive different notices, that provide different types of remediation, for different lengths of time.

The provision in Section 2 stating that an existing state law is not inconsistent with the provisions of the model if the protection afforded is greater than that provided under the act also would allow for inconsistencies amongst the states. In addition, in Section 12, the authority granted to the commissioner to promulgate rules and regulations gives rise to concern that different requirements may be imposed under different states’ rules or regulations. This would further undercut achievement of the goal of uniform national security and breach notification standards, consistently implemented and enforced, from state to state.

The requirements of these three sections are likely to delay notice to consumers, divert licensees' attention from investigation and remediation of the breach, and result in uneven consumer protection across the country.

Workability

While the industry recognizes that time is of the essence, it is important that the Model Law be workable. We are concerned that portions of the Model Law make it difficult for it to be practically implemented and enforced. The elimination of the harm trigger causes considerable workability concerns. It gives rise to concerns that consumers will be unnecessarily alarmed by notices, provided when there is little likelihood of harm, that contain possibly irrelevant information. There is concern that over-notification may desensitize consumers who will subsequently ignore notices, even in cases where there is a risk of harm.

In conclusion, we reiterate that the three issues described above are fundamental threshold issues for our trade associations. We urge modification of the current draft to address these and the other serious issues discussed in the trade associations' individual letters, and request another exposure and further discussion of the draft Model Law.

We look forward to continued dialogue and again remain committed to continuing to work with the Task Force to ensure a strong and workable Model Law.

Thank you for your consideration of these comments, and please contact us if you have any questions.

Sincerely,

<u>Organization</u>	<u>Name</u>	<u>Phone Number</u>	<u>E-mail Address</u>
American Bankers Association	Sarah Ferman	202-663-5510	sferman@aba.com
American Council of Life Insurers	Robbie Meyer	202-624-2184	robbiemeyer@acli.com
America's Health Insurance Plans	Bob Ridgeway	501-333-2621	bridgeway@ahip.org
American Insurance Association	Angela Gleason	202-828-7181	agleason@aiadc.org
Blue Cross Blue Shield Association	Paul Brown	202-626-4802	paul.brown@bcbsa.com
Council of Insurance Agents and Brokers	John Fielding	202-350-5864	john.fielding@ciab.com
Delta Dental Plans Association	Jason Daughn	202-355-8372	jdaughn@deltadental.com

Insured Retirement Institute	Chelsea Crucitti	202-469-3032	CCrucitti@irionline.org
National Association of Health Underwriters	Marcy Buckner	202-595-7589	mbuckner@nahu.org
National Association of Insurance and Financial Advisors	Gary Sanders	703-770-8192	gsanders@naifa.org
National Association of Professional Insurance Agents	Lauren Pachman	703-518-1344	laurenpa@pianet.org
National Association of Mutual Insurance Companies	Paul Tetrault	978-969-1046	ptetrault@namic.org
Property Casualty Insurers Association of America	Deirdre Manna	847-553-3613	deirdre.manna@pciaa.net
Reinsurance Association of America	Karalee C. Morell	202-783-8380	morell@reinsurance.org

CC: Sara Robben, Statistical Advisor, NAIC
Eric Nordman, Director of Regulatory Services and NIPR, NAIC