

July 31, 2017

Via email: srobben@naic.org

Director Raymond G. Farmer, Chair
Superintendent Elizabeth Kelleher Dwyer, Vice Chair
Cybersecurity (EX) Working Group
National Association of Insurance Commissioners
1100 Walnut Street, Suite 1500
Kansas City, MO 64106-2197

**Re: NAIC Insurance Data Security Model Law (Version 5) –
Comments of the American Bankers Association**

Dear Director Farmer and Superintendent Dwyer:

The American Bankers Association (“ABA”) writes to ask the National Association of Insurance Commissioners’ Cybersecurity (EX) Working Group to add a new exception to Section 9 of version 5 of the Insurance Data Security Model Law (“Model Law”). The addition would recognize that as dictated by Federal regulations, some insurance agencies that are affiliated with a bank already operate under the bank’s Information Security Program, so they should be able to rely on the bank’s program for purposes of the Model Law’s requirement to develop and implement an Information Security Program. As the Working Group has requested, we have provided additional concerns on the new draft that focuses on changes between version 4 and version 5 of the Model Law.

I. Background of Federal and State Regulation of Data Security

In enacting the Gramm-Leach-Bliley Act (“GLBA”), Congress intended that there be consistency among Federal and state data security standards, including those that apply to banks and to insurance licensees. Specifically, Title V of the GLBA requires Federal and state regulators to “establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical and physical safeguards–

- “to insure the security and confidentiality of customer records and information;
- “to protect against any anticipated threats or hazards to the security or integrity of such records; and
- “to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.”¹

¹ 15 U.S.C. § 6801(b).

With respect to insurance licensees, the GLBA recognizes that state insurance regulators have jurisdiction when it comes to insurance data security.²

The GLBA also directs that Federal and state agencies work to “assur[e], to the extent possible, that the regulations prescribed by each such agency are *consistent and comparable* with the regulations prescribed by the other such agencies.”³

Since 2001, banks have been required to comply with Federal data security guidelines that were adopted jointly by the Federal banking agencies for the purpose of maintaining bank safety and soundness.⁴ We have attached a copy of the *Interagency Guidelines Establishing Standards for Safeguarding* as issued by the Office of the Comptroller of the Currency.⁵ Many of ABA’s member banks have affiliated insurance agencies that would need to comply with the data security requirements established by the Model Law.

Banks and their affiliates often have common customers and use a single Information System to manage data concerning both bank customers and insurance customers. In that situation, both affiliated entities should be able to rely upon a single Information Security Program designed and implemented by one of the affiliates.

II. Recommendation

Given that GLBA anticipates that banks and insurance licensees will be able to comply with consistent information security standards with respect to Information Security Programs, independent of who regulates them, we urge the Working Group to add the following language to Section 9 of the Model Law to reflect that an insurance agency’s reliance upon, and adherence to, an affiliated bank’s Information Security Program will be deemed to constitute satisfaction of the requirements in Section 4 of the Model Law to establish and implement an Information Security Program. This addition would avoid a bank and an affiliated insurance agency each having to maintain an Information Security Program. We suggest the following language, to be added as a new Section 9(A)(4):

- “The following exceptions shall apply to this Act:

....

- “(4) A Licensee affiliated with a depository institution that maintains an Information Security Program in compliance with the *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*⁶ shall be

² 15 U.S.C. § 6805(a).

³ 15 U.S.C. § 6804(a)(2).

⁴ 66 Fed. Reg. 8616 (Feb. 1, 2001). See 15 U.S.C. § 6801(b); 12 C.F.R. Part 30, Appendix B; Part 208, Appendix D-2; Part 205, Appendix F; Part 364, Appendix B.

⁵ The Interagency Guidelines apply to both consumer information and customer information. *Interagency Guidelines*, App. B, § I.C.2.b.-e. “Customer information” is defined to mean any record that contains nonpublic personal information, as defined in regulations issued pursuant to the Gramm-Leach-Bliley Act – a term also used in the NAIC’s *Privacy of Consumer Financial and Health Information Regulation*, No. 672.

⁶ 12 CFR Part 30, Appendix B; Part 208, Appendix D-2; Part 205, Appendix F; Part 364, Appendix B.

considered to meet the requirements of Section 4, provided that the Licensee produce, upon request, documentation satisfactory to the Commission that independently validates the affiliated depository institution's adoption of an Information Security Program that satisfies the Interagency Guidelines."

III. Other Comments and Recommendations

Additional comments concerning the changes between version 4 and version 5 of the Model Law are addressed below.

- **Section 2 (Purpose and Intent)**

- Section 2(A) should be revised to reflect that the purpose and intent of the Model Law is to establish the "exclusive" standards for data security, investigation and breach notification applicable to Licensees in the state. The proposed language is needed to ensure that a Licensee is required to adhere to only one set of data security requirements in a particular state.

- **Section 3 (Definitions)**

- We support the revised definition of "Cybersecurity Event" in Section 3(D) to mean "an event resulting in unauthorized access to, disruption or misuse of, an Information System or information stored on such Information System." The proposed recommendation would define the term to include only an actual event, not merely an attempt to gain unauthorized access to protected information in an Information System.

- **Section 4 (Information Security Program)**

- We support revised Section 4(D)(1), which requires a Licensee to design an Information Security Program "commensurate with the size and complexity of the Licensee's activities. . . ." This language confirms that the Model Law will not use a "one-size-fits-all" approach to either the Licensee's performance of a risk assessment or its design of an Information Security Program.
- Likewise, we support the revision to Section 4(D)(2) that now leaves to the Licensee's discretion, which listed security measures it determines to be appropriate given the nature and scope of its operations. We also appreciate that version 5 takes the same approach to the Licensee's decision whether to adopt Multi-Factor Authentication procedures.

- **Section 6 (Notification of a Cybersecurity Event)**

- Section 6(A)(1) requires a Licensee to notify the insurance commissioner of the Licensee's home state, in the case of an insurance agency, within 72 hours after it

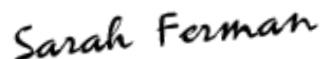
determines a Cybersecurity Event has occurred. Notification is also required to an insurance commissioner in any state where a breach of Nonpublic Information involves 250 or more residents of the state who are likely to be materially harmed by the breach. We support limiting the notification requirement to the Licensee's home state, but we question the need to notify any other state. If that requirement remains, we urge that the threshold for number of affected residents of the state be increased to at least 500.

IV. Conclusion

Insurance agencies affiliated with a bank often use a common Information System to manage information about both banking customers and insurance customers. An insurance agency will rely on the Information Security Program developed by the affiliated bank to protect the Information System and the data it contains. As long as the bank's Information Security Program complies with the *Interagency Guidelines*, an affiliated insurance agency should be able to rely on the bank's program. The ABA urges the Working Group to consider an insurance agency to be in compliance with Section 4 of the Model Law if it relies on an affiliated bank's Information Security Program that satisfies Federal requirements. We also urge the Working Group to give insurance licensees more time to report a Cybersecurity Event to an insurance commissioner.

We thank the Working Group for the opportunity to comment on the new version of the draft Model Law and look forward to further discussion on the Model Law.

Sincerely,



Sarah Ferman
Senior Government Relations Representative
American Bankers Association