

May 16, 2017

By electronic delivery to:

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

Re: NAIC Insurance Data Security Model Law

Dear Director Farmer and Superintendent Dwyer:

The American Bankers Association ("ABA") writes to ask the Cybersecurity Working Group's Drafting Group to revise version 4 of the Insurance Data Security Model Law ("Model Law") to recognize that insurance agencies that are affiliated with banks already operate under the bank's Information Security Program, as dictated by Federal regulations.

ABA thanks the Drafting Group for the significant improvements in the new version of the Model Law, given that its scope has been limited primarily to require an insurance licensee to develop, implement and update an Information Security Program and to investigate and notify an insurance regulator of a Cybersecurity Event. We request that the Model Law be revised to deem adherence by an insurance agency with an affiliated bank's Information Security Program to constitute compliance with Sections 4 and 5 of the Model Law.

I. BACKGROUND

Since 2001, banks have been required to comply with existing Federal data security requirements which are designed to maintain bank safety and soundness. Banks must comply with existing Federal data security requirements. 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, so they routinely use a single Information System to manage data concerning both bank customers and insurance customers. As described below, the principal requirements of the new draft of the Model Law are very similar to those of the Federal data security guidelines, differing primarily in the level of detail. Therefore, we urge the Drafting Group to add language to the Model Law that reflects that compliance with the Federal data security guidelines by an insurance agency affiliated with a bank would constitute compliance with the Model Law with respect to the requirements regarding an Information Security Program and investigation of a Cybersecurity Event.

The *Interagency Guidelines Establishing Standards for Safeguarding Customer Information* (the "Interagency Guidelines") – jointly issued by the Federal Reserve, Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency¹ – establish requirements for the development and implementation of an Information Security Program to protect consumer information and customer information² and information systems, and for investigation and reporting of a Cybersecurity Event. The Interagency Guidelines apply to banks and their affiliates, but they expressly do not apply to "persons providing insurance."³ We have attached a copy of the Interagency Guidelines as issued by the Office of the Comptroller of the Currency.

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

² 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.

³ *Interagency Guidelines*, App. B, § I.A.

The main requirements of the Interagency Guidelines are as follows, with footnote references to the relevant language in the attachment:

Information Security Program. Banks must establish a comprehensive written Information Security Program that includes administrative, technical and physical safeguards that are appropriate to the bank's size.⁴

Program Objectives. The Information Security Program must be designed to ensure the security and confidentiality of customer information; protect against threats to the security and integrity of customer information; protect against unauthorized access to customer information that could result in substantial harm or inconvenience to a customer; and ensure proper disposal of customer information.⁵

Risk Assessment and Management. In developing an Information Security Program, banks are required to assess threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or of the bank's Information System. Banks must evaluate whether existing policies are sufficient to control risks. Banks also must determine which of several security measures are appropriate for the bank, given its size, including controls to access Information Systems, physical safeguards, encryption, dual control procedures, monitoring systems, response programs, and measures to protect against destruction or loss of customer information.⁶

Training and Testing. A bank must train its staff on its Information Security Program and it must test the program's controls, systems and procedures.

Oversight of Third Party Service Providers. Banks must oversee third party service provider arrangements, including the exercise of due diligence in selecting service providers and monitoring a service provider's compliance with the requirements of the bank's Information Security Program.⁷

Program Adjustment. Banks must adjust the Information Security Program as technology changes.⁸

Oversight by Board of Directors. A bank's board of directors must receive annual reports on the status for the bank's Information Security Program.⁹

Investigation of a Cybersecurity Event. Banks must develop and be prepared to implement a program to respond to a Cybersecurity Event, including investigating the nature and scope of the event.¹⁰

Notification of a Cybersecurity Event. A bank must notify its primary Federal regulator "as soon as possible" after becoming aware of a Cybersecurity Event, and it must notify law enforcement via a Suspicious Activity Report, as required by Federal regulations.¹¹

Notification to Customers. A bank is required to establish and implement a customer notification program.¹²

II. RECOMMENDATIONS

All of these requirements of the Interagency Guidelines are also requirements of the Model Law, although the Model Law addresses some of the topics in more detail. But with respect to the contents and implementation of an

⁴ *Id.*, § III.

⁵ *Id.*, § II.B.

⁶ *Id.*, § III.B.-C.

⁷ *Id.*, § III.D.

⁸ *Id.*, § III.E.

⁹ *Id.*, § III.A., F.

¹⁰ *Interagency Guidelines*, App. B, Supp. A (Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice), § II.A.1.-2, III.A.

¹¹ *Id.*, § I.A.b.-c.

¹² *Id.*, § III.

Information Security Program, both banks, in the case of the Interagency Guidelines, and insurance licensees, in the case of the Model Law, are given some flexibility in program development and implementation. Accordingly, so that insurance agencies affiliated with a bank are able to comply with one set of requirements regarding cybersecurity, we urge the Drafting Group to modify the Model Law to read that compliance by a bank-affiliated insurance agency with Federal data security requirements, as adopted and implemented by the bank affiliate, shall constitute compliance with Section 4 of the Model Law (Information Security Program) and Section 5 (Investigation of a Cybersecurity Breach), and to provide additional time to report a Cybersecurity Event to an insurance regulator. We recommend the following specific revisions:

1. Add the following exception to Section 9(A) of the Model Law:

“A Licensee that is affiliated with a bank that is in compliance with the Federal *Interagency Guidelines Establishing Standards for Safeguarding Customer Information* and that has fully adopted and implemented the bank’s Information Security Program and the bank’s policies regarding breach is deemed to be in compliance with the requirements of Sections 4 and 5.”

2. Change the first paragraph of Section 6(A) to read as follows (incorporating the strikeout): “Each Licensee shall notify the Commissioner as promptly as possible ~~but in no event later than 72 hours~~ from a determination that a Cybersecurity Event has occurred. . . .”

III. 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 Drafting Group to consider an insurance agency to be in compliance with Sections 4 and 5 of the Model Law if it relies on an affiliated bank’s Information Security Program. We also urge the Drafting Group to give insurance licensees more time to report a Cybersecurity Event to an insurance regulator.

We thank the Drafting Group for the opportunity to comment on the new version of the draft Model Law and look forward to discussing this comment letter with the Drafting Group on its next call.

Sincerely,