December 21, 2017

The Honorable Raymond G. Farmer
Director, South Carolina Department of Insurance
Post Office Box 100105
Columbia, SC 29202

Submitted via email to Director Farmer: rfarmer@doi.sc.gov

Re: South Carolina Proposed Insurance Data Security Law

Dear Director Farmer:

As you know, the National Association of Insurance Commissioners (NAIC) worked on an Insurance Data Security Model Law for the better part of three years. On Oct. 24, 2017, the Executive Committee of the NAIC passed the Insurance Data Security Model Law, making it ripe for state legislatures to include on their agendas for the 2018 legislative calendar. We understand that South Carolina's legislature will be considering a bill substantially similar to the NAIC model during its upcoming session, and we appreciate the opportunity to provide some feedback on that bill.

Background

The National Association of Professional Insurance Agents (PIA National)[1] worked closely with you and the rest of the commissioners at the NAIC to fine-tune the model so that compliance with its requirements would not be unnecessarily burdensome for small businesses. Over the course of the model's development, many of our recommendations were taken. However, despite our best efforts, we find the South Carolina version, which closely tracks the NAIC model, concerning, and we hope that we can again work together to achieve our shared goals of protecting both consumers and small businesses in South Carolina.

The South Carolina proposal, like the NAIC model law from which it emanates, requires insurance agencies and other members of the industry to take specific steps to prevent against cybersecurity events and outlines the requirements that need to be taken in the event of a breach. We are concerned about the overly broad definitions that potentially could capture physical as

[1] PIA is a national trade association founded in 1931, which represents member insurance agents in all 50 states, Puerto Rico, Guam, and the District of Columbia. PIA members are small business owners and insurance professionals who can be found across America.

well as electronic breaches, and breaches that involve public as well as nonpublic information; agencies' and individual agents' obligations as they pertain to the activities and potential liabilities of third-party service providers (like agency management systems); the very short timeframe in which to provide notification to the Director or his designee of a "Cybersecurity Event"; and the number of consumers affected by a Cybersecurity Event to trigger notification to the Director or his designee, among other issues.

To that end, below please find recommended amendments for inclusion in the South Carolina proposal. Please note that additional amendments may be requested based on the specific language of the introduced bill.

Proposed Amendments

1. In Section 38-55-810, *Purpose and Intent*, Section A seems to leave enough flexibility for the model to be adopted in conjunction with, rather than as a replacement of, existing South Carolina law. This conflicts with the NAIC's stated intent, which is "to supersede state and federal laws of general applicability that address data security and data breach notification."[2] To remedy this, we recommend the following revision:

   The purpose and intent of this Act is to establish the exclusive state standards applicable to Licensees for data security, ~~and standards for~~ the investigation of a Cybersecurity Event as defined in Section 38-55-820.A., and notification to the Director ~~of a Cybersecurity Event applicable to Licensees, as defined in Section 3~~. To the extent that other applicable state laws conflict with these requirements, they are hereby repealed. The foregoing notwithstanding, this law shall not supersede or inhibit any state or criminal law.

2. The definition of "Cybersecurity Event" seems to include events in which a facility in which hard copies of "Nonpublic Information" are stored are breached. Specifically, Section 38-55-820.D. defines a "Cybersecurity Event" as one in which there is "unauthorized access to, disruption or misuse of, an Information System ***or information stored on such Information System***" (emphasis added). This seems to suggest that, if hard copies of documents containing Nonpublic Information are physically stolen, where such information is also stored electronically (in an Information System, as defined in Section 38-55-820.G.), such a theft is covered by this model. For a model that purports to address issues raised by "cyber" security, this provision is overly broad. We recommend amending Section 38-55-820.D. as follows:

   "Cybersecurity Event" means an event resulting in unauthorized access to, disruption or misuse of, an Information System or Nonpublic ~~i~~Information stored on such Information System, if the event involves access to or disruption or misuse of electronic information

[2] http://www.naic.org/documents/index_committees_pending_final_170808_data_security_ml.pdf

resources. The term "Cybersecurity Event" does not include the unauthorized acquisition of Encrypted Nonpublic Information if the encryption, process or key is not also acquired, released or used without authorization. Cybersecurity Event does not include an event with regard to which the Licensee has determined that the Nonpublic Information Accessed by an unauthorized person has not been used or released and has been returned or destroyed.

3. To reinforce that only events that result in a breach concerning nonpublic information, we also recommend the following revision to Section 38-55-820.H., which defines "Information System" as follows:

   "Information System" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic Nonpublic ~~i~~Information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

4. The definition of "Nonpublic Information" included in Section 38-55-820.K. is not limited to electronic information and thus seems to suggest that, if hard copies of documents containing Nonpublic Information are physically stolen, such a theft is covered by this bill. For a proposal that purports to address the need to provide "data" security, this provision is overly broad. We recommend amending Section 38-55-820.K. as follows:

   "Nonpublic Personal Information" means electronic information that is not Publicly Available Information and is: […]

5. Similarly, the definition of "Publicly Available Information" included in Section 38-55-820.M. should be revised to comport with the definition of "Nonpublic Information" as revised above, as follows:

   "Publicly Available Information" means any electronic information that a Licensee has a reasonable basis to believe is lawfully made available to the general public from …

6. Section 38-55-830.D.(1) should be revised to match the language used in Section 38-55-830.A. This recommended change is as follows:

   Design its Information Security Program to mitigate the identified risks, commensurate with the size and complexity of the Licensee, the nature and scope of the Licensee's activities, including its use of Third-Party Services Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody or control.

7. The Risk Management protocols set forth in Section 38-55-830.D.(2) are excessively burdensome for some Licensees, especially considering that the bill is intended to govern

electronic and not physical breaches. We therefore recommend the following revision to Section 38-55-830.D.(2)(c):

Restrict physical access ~~at physical locations containing~~ to Nonpublic Information~~, only~~ to Authorized Individuals only;

8. Because of the outsized burden some of these provisions will place on small insurance agencies, we additionally recommend the following specific revisions to other parts of Section 38-55-830.D.(2)(e) and (g), respectively:

   Adopt secure development practices for in-house developed applications utilized by the Licensee ~~and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Licensee~~;

   […]

   Utilize effective controls, which may include Multi-Factor Authentication procedures for ~~any individual~~employees accessing Nonpublic Information;

   […]

9. We have many concerns regarding the treatment of Licensee relationships with third-party service providers. Small-business Licensees, out of necessity, frequently enter into what are known as contracts of adhesion. Large companies serving as Third-Party Service Providers are going to be reticent to change their cybersecurity practices to reflect compliance with a South Carolina-specific law that applies only to some Licensees. Small-business Licensees rarely can negotiate the details of their relationships with relatively large Third-Party Service Providers. Therefore, many Licensees will be subjected to whatever cybersecurity practices the Third-Party Service Provider already offers, whether those practices meet the standards applicable to Licensees in this Section. This issue comes up throughout the bill, beginning explicitly in Section 38-55-830.F.(2), which requires that Licensees "require a Third-Party Service Provider to implement appropriate administrative, technical, and physical measures" to protect information accessible to or held by the Third-Party Service Provider. We recommend this Section be rephrased as follows:

   A Licensee shall ~~require~~ request that a Third-Party Service Provider ~~to~~ implement appropriate administrative~~,~~ and technical~~, and physical~~ measures to protect and secure the Information Systems ~~and~~ containing Nonpublic Information that are accessible to, or held by, the Third-Party Service Provider.

10. Section 38-55-840.C. requires Licensees to enforce the provisions of Section 38-55-840.B. against Third-Party Service Providers. This provision will be near-impossible to enforce because it requires Licensees to ensure that a Third-Party Service Provider with which it does business not contractually shift its obligations pursuant to Section 38-55-840.B. back to the Licensee. Again, our concerns arise out of the likelihood that many such arrangements constitute contracts of adhesion between small-business Licensees and large Third-Party Service Providers. For that reason, we recommend the elimination of Section 38-55-840.C. and the renumbering of Section 38-55-840.D. accordingly.

11. The timeframe for notification to the Director or his designee is even shorter in this proposal than it was in early iterations of the NAIC model, in which it was three (3) business days. Seventy-two hours, particularly without regard for when during a week or what time of year those hours occur, would pose an extreme hardship to a small-business Licensee. This timeline is burdensome and raises substantial and serious concerns about the practical workability of this provision. For the foregoing reasons, Section 38-55-850.A. should be amended as follows:

    Each Licensee shall notify the Director or his designee as promptly as possible but in no event later than ~~72 hours~~10 (ten) days from a determination that a successful Cybersecurity Event involving Nonpublic Information in the possession of the Licensee has occurred, ~~when either of~~ if the ~~following criteria has been met~~Licensee reasonably believes that the Nonpublic Information involved is of 500 or more consumers residing in South Carolina and the Cybersecurity Event has a reasonable likelihood of materially harming a Consumer residing in South Carolina or reasonable likelihood of materially harming any material part of the normal operation(s) of the Licensee, and the Cybersecurity Event is either of the following:

    [original text of Sections 38-55-850.A.(1) and (2) should be deleted, and text of Sections 38-55-850.A.(2)(a) and (b) should be renumbered as Sections 38-55-850.A.(1) and (2)…]

12. The Director should not be bombarded with insignificant changes to the information Licensees have previously provided concerning Cybersecurity Events. To that end, Section 38-55-850.B. should be amended as follows:

    The Licensee making the notification required by Section 38-55-850.A. above shall provide as much of the following information as possible. The Licensee shall provide the information in electronic form as directed by the Director or his designee. The Licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the Director or his designee ~~concerning~~ regarding material changes to previously provided information relating to the Cybersecurity Event. […]

13. Section 38-55-850.B.9. requires Licensees to hazard a guess about the number of consumers in South Carolina affected by a Cybersecurity Event, even if that event has occurred in a Third-Party Service Provider system. To alleviate this challenge, this Section should be amended as follows:

    The number of total Consumers in this State affected by the Cybersecurity Event. The Licensee shall provide ~~the~~ its best estimate as promptly as possible ~~in the initial report~~ to the Director or his designee and update this estimate with each subsequent report to the Director or his designee pursuant to this section; […]

14. Section 38-55-850.D.1. should be amended as follows:

    In case of a Cybersecurity Event in a system maintained by a Third-Party Service Provider, of which the Licensee has become aware, the Licensee shall treat such event as it would under Section 38-55-850.A, unless the Third-Party Service Provider provides the required Section 38-55-850.A. notice to the Director or his designee.

15. To strengthen the confidentiality obligations to which Licensees are made subject by the bill, we recommend adding the following sentence at the end of Section 38-55-850.A.:

    The Director or his designee shall not otherwise make the documents, materials, or other information public without the prior written consent of the Licensee.

16. To bolster the confidentiality obligations to which Licensees are made subject by the model, we recommend adding the following as Section 38-55-870.F.:

    Documents, materials, or other information in the control of the National Association of Insurance Commissioners (NAIC) or a Third-Party Service Provider or other vendor pursuant to this Act shall be confidential by law and privileged, shall not be subject to [insert applicable open records, FOIA, sunshine, or other law], subpoena, or discovery or admission into evidence in any private civil action.

17. Section 38-55-880.A.1. should be amended as follows:

    A Licensee in this State is exempt from Section 38-55-830 of this Act if it meets any of the following criteria:
    a) ~~with~~ fewer than ten employees, including any independent contractors, or
    b) less than $5 million in gross annual revenue, or
    c) less than $10 million in year-end total assets~~is exempt from Section 4 of this Act~~. […]

PIA recognizes and appreciates the considerable thought and effort that Director Farmer and the rest of the South Carolina Department of Insurance have given to this issue, and we are grateful

for the opportunity to provide the independent agent perspective. Please contact me at laurenpa@pianet.org or (703) 518-1344 with any questions or concerns. Thank you for your time and consideration.

Sincerely,

Lauren G. Pachman
Counsel and Director of Regulatory Affairs
National Association of Professional Insurance Agents