May 15, 2018

The Honorable Lana Theis
Chair, Michigan State House Insurance Committee

Submitted via email to LanaTheis@house.mi.gov

Re: Testimony on Michigan House Draft Chapter 5A on Data Security

Dear Rep. Theis:

As you know, the National Association of Insurance Commissioners (NAIC) worked on its 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 2018 legislative calendars. As the Michigan House Insurance Committee prepares to consider Draft Chapter 5A on Data Security (herein referred to as Draft Chapter 5A), a bill that derives from the NAIC model, we appreciate the opportunity to provide some feedback on and context around that bill.

Background

The National Association of Professional Insurance Agents (PIA National)[1] worked closely with many commissioners and industry representatives at the NAIC to fine-tune the model so that compliance with its requirements would not be unnecessarily burdensome for our members, independent insurance agents who primarily operate small businesses. Over the course of the model's development, many of our recommendations were adopted. We are pleased that Draft Chapter 5A adopts many of the suggestions we have made repeatedly to the NAIC and the state legislatures of South Carolina and Rhode Island. However, we find a few provisions of Draft Chapter 5A concerning, and we hope that we can work together to achieve our shared goals of protecting both consumers and small businesses in Michigan.

Draft Chapter 5A, 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 definition of "CYBERSECURITY EVENT," which potentially could capture physical as well as electronic breaches; agencies' obligations as they pertain to the activities and potential

[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.

liabilities of third-party service providers (like agency management systems); the very short timeframe in which to provide notification to the commissioner of a "CYBERSECURITY EVENT"; and the number of consumers affected by a cybersecurity event to trigger notification to the Michigan insurance director, among other issues.

To that end, below please find recommended amendments for inclusion in Draft Chapter 5A.

Proposed Amendments

1. 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 553(C) defines a "CYBERSECURITY EVENT" as one in which there is "UNAUTHORIZED ACCESS TO, OR DISRUPTION OR MISUSE OF, AN INFORMATION SYSTEM ***OR NONPUBLIC INFORMATION STORED ON AN 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 553(F), such a theft is covered by this bill. For a bill that purports to address issues raised by "cybersecurity events," this provision is overly broad. We recommend amending Section 553(C) as follows:

   "CYBERSECURITY EVENT" MEANS AN EVENT RESULTING IN UNAUTHORIZED ACCESS TO, OR DISRUPTION OR MISUSE OF, AN INFORMATION SYSTEM OR NONPUBLIC INFORMATION STORED ON AN INFORMATION SYSTEM, IF THE EVENT INVOLVES ACCESS TO OR DISRUPTION OR MISUSE OF ELECTRONIC INFORMATION RESOURCES. "CYBERSECURITY EVENT" DOES NOT INCLUDE EITHER OF THE FOLLOWING:

   (i) THE UNAUTHORIZED ACQUISITION OF ENCRYPTED NONPUBLIC INFORMATION IF THE ENCRYPTION, PROCESS, OR KEY IS NOT ALSO ACQUIRED, RELEASED, OR USED WITHOUT AUTHORIZATION

   (ii) 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.

2. 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 Michigan-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 or not those practices meet the standards applicable to

licensees in this bill. This issue comes up throughout the bill, beginning explicitly in Section 555(6), which demands 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.

3. Section 557(3) requires licensees to enforce the provisions of Section 557(2) against third-party service providers. This provision will be nearly 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 557(2) 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 557(3) and the renumbering of Section 557(4) accordingly.

4. The timeframe for notification to the director is slightly longer in this proposal than in the NAIC model, in which it was 72 hours. However, three (3) business days, particularly without regard for when during a week or what time of year those days occur, would still 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 559(1) should be amended as follows:

EACH LICENSEE SHALL NOTIFY THE DIRECTOR AS PROMPTLY AS POSSIBLE BUT NOT LATER THAN TEN (10)~~3~~ BUSINESS DAYS AFTER A DETERMINATION THAT A SUCCESSFUL CYBERSECURITY EVENT INVOLVING NONPUBLIC INFORMATION THAT IS IN THE POSSESSION OF A LICENSEE HAS OCCURRED, ~~WHEN EITHER OF~~ IF THE ~~FOLLOWING CRITERIA HAS BEEN MET~~LICENSEE REASONABLY BELIEVES THAT THE NONPUBLIC INFORMATION INVOLVED IS OF TWO HUNDRED FIFTY (250) OR MORE CONSUMERS RESIDING IN MICHIGAN, THE LICENSEE IS DOMICILED IN MICHIGAN, AND THE CYBERSECURITY EVENT HAS A REASONABLE LIKELIHOOD OF MATERIALLY HARMING ANY MATERIAL PART OF THE NORMAL OPERATION(S) OF THE LICENSEE.~~:~~

[original text of Section 559(1)(A) and (B) would then be stricken]

5. Section 559(2)(I) requires licensees to hazard a guess about the number of consumers in Michigan 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 AND UPDATE THIS ESTIMATE WITH EACH SUBSEQUENT REPORT TO THE DIRECTOR UNDER THIS SECTION. […]

6. Section 559(4) should be amended as follows:

   FOR A CYBERSECURITY EVENT IN A SYSTEM MAINTAINED BY A THIRD-PARTY SERVICE PROVIDER, OF WHICH THE LICENSEE HAS BECOME AWARE, THE LICENSEE SHALL TREAT THE EVENT AS IT OTHERWISE WOULD UNDER THIS SECTION UNLESS THE THIRD-PARTY SERVICE PROVIDER PROVIDES THE NOTICE REQUIRED UNDER THIS SECTION TO THE DIRECTOR.

Unlike the NAIC model, and unlike the bill introduced in Rhode Island, Draft Chapter 5A does not acknowledge licensees that meet the requirements imposed by the New York Department of Financial Services (NYDFS) in 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies. While the NAIC model is, in part, modeled on 23 NYCRR 500, the NYDFS regulation is more draconian and less flexible. Licensees as defined in Draft Chapter 5A should be viewed as having complied with that bill if they comply with 23 NYCRR 500. We respectfully request that a provision to that end be added to Section 565.

PIA recognizes and appreciates the considerable thought and effort that Director McPharlin, Representative Theis, and many others 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