ACLI Comments

Insurance Data Security Model Law

8/17/2017 draft (version 2)

In anticipation of discussion during the 2/21/17 Drafting Group call and conclusion of the Drafting Group's consideration of the 8/17/2016 draft (version 2) of the proposed Insurance Data Security Model Law, the ACLI respectfully submits comments relating to the following:

(i) **Section 2**, as proposed to be modified in the "Sections 2 and 3 Discussion Document (from the 12/20/16 call);"

(ii) **Section 4.F.,** as proposed to be modified in the "Provisions Related to Third Party Service Providers – Proposed Revisions to Version 2 for Jan. 10 Drafting Group Call" and in Peter Kochenburger's "Comments to Section 2, 4.F, G, & 6;"

(iii) **Section 5**, with particular focus on the modifications proposed in the "Provisions Related to Third-Party Service Providers – Proposed Revisions to Version 2 for Jan. 10 Drafting Group Call;"

(iv) **Section 6**, as proposed to be modified in the "Provisions Related to Third-Party Service Providers – Proposed Revisions to Version 2 for Jan. 10 Drafting Group Call" and as proposed in the 8/17/2016 draft (version 2)

(v) **Section 7.** as proposed in the 8/17/2016 draft (version 2);

(vi) **Section 12.** as proposed in the 8/17/2016 draft (version 2); and

(vii) Definition of "**Personal Information**," as proposed to be modified in the "Sections 2 and 3 Discussion Document (from the 12/20/16 call)" and in the "Provisions Related to Third-Party Service Providers – Proposed Revisions to Version 2 for Jan. 10 Drafting Group Call."

ACLI's comments relating to the above are as follows:

(i) Section 2. Purpose and Intent

Since the 2/21/17 call may be the last Drafting Group call to discuss the 8/17/2016 draft ("version 2") of the Insurance Data Security Model Law ("Model Law") before publication of a third version of the proposed Model Law, ACLI wishes to underscore that it is fundamentally important that any standards imposed under the Model Law constitute the exclusive security and breach notification standards applicable to insurance licensees within individual states and provide the basis for uniform standards, to be consistently enforced and provide level consumer protection, from state to state. It also is fundamentally important that any new security standards be risk based and flexible and that any new breach notification standards be workable.

Accordingly, as discussed in ACLI comments previously submitted to the Drafting Group, it is very important that Section 2, be modified as proposed in the "Sections 2 and 3 Discussion Document

(from the 12/20/16 call)," to eliminate the last two sentences, that commenced "This Act shall not be construed as superseding, altering or affecting any statute, regulation, order or interpretation of law in this state … " For the same reasons, it also is very important to eliminate the drafting note at the end of Section 6 in version 2, that provides for each state to determine whether it is necessary to include all or parts of Sections 5 and 6 in its statute.

(ii) Section 4.F. Oversight of Third-Party Service Provider Arrangements

These comments are submitted to follow up on discussion during the 2/7/17 conference call of the Drafting Group.

ACLI believes the proposed modification to Section 4.F. in the "Provisions Related to Third Party Service Providers – Proposed Revisions to Version 2 for Jan. 10 Drafting Group Call," to eliminate the language that provided for a licensee to be "responsible for *any* failure by such third-party providers to protect personal information provided by the licensee to the third-party service providers consistent with this Act" *(Italics added.)* was appropriate and very important. Such a requirement would inappropriately and unnecessarily subject insurance company licensees to strict liability for *any* failure by any third-party service provider to protect personal information in a manner consistent with the Model Law.

Some insurance company licensees have hundreds or even thousands of third-party service providers, that not only differ in size and the sophistication of their security systems and controls, but in the nature and amount of a licensee's customer personal information to which they may have access. As a result, third-party service providers differ greatly in the risk they pose to the security of a licensee's customer personal information.

ACLI believes it is appropriate to require licensees to require their third-party service providers by contract to implement measures designed to meet the security requirements of the Model Law. However, it would be virtually impossible for insurance company licensees to protect against *any* failure by any of their third-party service providers to protect personal information or to comply with the Model Law. ACLI also respectfully, but strongly, disagrees with assertions that it is appropriate to assume that insurance company licensees will be able to persuade all of their service providers, especially their large cloud providers, to adhere to the security requirements of the Model Law or to indemnify insurer licensees in the event of a breach or failure by the service provider to comply with the Model Law.

Accordingly, ACLI respectfully, yet strongly, opposes reinsertion of the following sentence into Section 4.F. as proposed by Mr. Kochenburger: "The licensee shall be responsible for any failure by such third-party service providers to so comply." It also is not entirely clear how the requirement to "confirm" that a service provider is "*able* to implement appropriate measures to secure the licensee's personal information …" *(Italics added.)* may be legally construed.

Further, in view of the great variability in the amount of customer personal information to which different third-party service providers may have access, different service providers' security systems and protocols and the widely varying levels of risk posed by different third-party service providers, ACLI submits that requirements relating to third-party service provider oversight that are flexible and risk based are most likely to lead to the most effective and successful security protections.

Accordingly, ACLI urges modification to Section 4.F., as proposed to be modified in the "Provisions Related to Third Party Service Providers – Proposed Revisions to Version 2 for Jan. 10 Drafting Group Call" to include language that tracks the language of the NAIC Standards for Safeguarding Customer Information (Safeguards) Model Regulation, and to read as follows (*Language proposed to be added is **IN RED, IN BOLD AND IN ALL CAPS**; language proposed to be deleted **[is stricken, in red, in brackets, and in bold].**):*

INSURANCE DATA SECURITY MODEL LAW
Provisions Related to Third-Party Service Providers
[Proposed Revisions to Version 2 for Jan. 10 Drafting Group Call]

Section 4. Information Security Program

F. Oversight of Third-Party Service Provider Arrangements

THE [~~the~~] licensee shall:

(1) Exercise due diligence in selecting each third-party service provider; and

~~(1)~~(2) REQUIRE ITS SERVICE PROVIDERS BY CONTRACT TO IMPLEMENT APPROPRIATE MEASURES DESIGNED TO MEET THE OBJECTIVES OF THIS SECTION AND, WHERE INDICATED BY ITS RISK ASSESSMENT, TAKE APPROPRIATE STEPS TO CONFIRM THAT ITS THIRD PARTY SERVICE PROVIDERS HAVE SATISFIED THESE OBLIGATIONS.

[~~Confirm and document with each third-party service provider that it is able to implement appropriate measures to secure the licensee's personal information that is held in a system maintained by the third-party service provider.~~]

~~contract only with third-party service providers that are capable of maintaining appropriate safeguards for personal information in the licensee's possession, custody or control, and the licensee shall be responsible for any failure by such third-party service providers to protect personal information provided by the licensee to the third-party service providers consistent with this Act.~~.

(iii) Section 5. Investigation of a Data Breach

ACLI has the following concerns with the definitions of "Personal information" and "Third-party service provider" and the language of Section 5., as proposed to be modified in the "Provisions Related to Third-Party Service Providers – Proposed Revisions to Version 2 for Jan. 10 Drafting Group Call" and as proposed in the 8/17/2016 draft (version 2):

(i) ACLI is very concerned by and respectfully opposed to the proposed modifications to the definition of "Personal Information" and the language of Section 5.A. that would tie the

requirements to investigate under Section 5 and to provide the notices under Section 6 to "possession," rather than to "ownership" of personal information that has or may have been subject to a data breach.

In line with the majority of existing state breach notification laws (that impose notification requirements on persons that own or license variously defined personal information), it is most appropriate for the owner, or other party acting on behalf of the owner, to investigate and provide notice of breaches. Also in line with the majority of existing state breach notification laws, it is important to distinguish between the responsibilities of the owner (or licensee) of the information and a third-party service provider or other entity or person that maintains, but does not own (or license) the information.

Under the NAIC Model Privacy of Consumer Financial and Health Information Regulation (Model Privacy Regulation), licensees are required to protect the confidentiality and security of their consumers' and customers' nonpublic personal information, and to provide their consumers and customers privacy notices that reflect their policies and procedures to protect the information. ACLI respectfully submits that in a model data security law solely applicable to insurance licensees, it is most appropriate for the owner of consumer/customer information, that has the legal responsibility to protect the confidentiality and security of the information and to provide related privacy notices, to be charged with the responsibility to investigate and provide notices of breaches in the security of the information.

(ii) In line with the above, ACLI does not believe that the Model Law should require third-party service providers to perform the investigatory steps described in Section 5.B., as proposed in Section 5.C. Instead, in the event of a data breach of a third-party service provider, in line with the thrust of the majority of existing state breach notification laws, the third-party service provider should be required to notify the licensee owner of the data breach and to cooperate with the owner licensee, which should have responsibility to investigate and provide the requisite notices relating to the breach. At the same time, the Model Law should permit agreements between a licensee and another licensee, a third-party service provider or other third party to provide for coordination and fulfillment of any of the Model Law's investigation or notice requirements. Accordingly, ACLI suggests deletion of Section 5.C. and modification to Sections 6.E. and 6.G. as indicated below.

(iii) Related to the above, ACLI is concerned by the proposed modification to the definition of "Third-party service provider" to add the phrase "not otherwise defined as a licensee" which would make it so that producers would never be third-party service providers under the Model Law. There is concern that exemption of producers from the scope of this term, without any clarification or limitation, will give rise to confusion. It will result in treatment of producers that differs from their treatment and obligations as "business associates" under the breach notification provisions of the HIPAA Privacy Rule and existing state breach notification laws (under which they may variously own or license personal information, or maintain, but not own or license, personal information).

(iv) As indicated previously, ACLI believes the Model Law's security requirements should be applicable to "Personal information," defined to track the definition of "Nonpublic Personal Information" in the NAIC Model Privacy Regulation and the Model Law's investigation and notice requirements should be applicable to a subset of "Personal information," sensitive personal information, the unauthorized acquisition of which is likely to render the subject of the information vulnerable to harm. Accordingly, ACLI believes that the investigation requirements in Section 5 should only apply to sensitive personal information (i.e. Personal information listed in specific sections of the definition of this term that describe sensitive personal information).

(v) As indicated in ACLI comments relating to the definition of "Data breach," previously submitted to the Drafting Group, ACLI believes that the inclusion of the unauthorized release or use of sensitive personal information within the scope of the definition of "Data breach" is likely to unnecessarily and significantly broaden the term, particularly in connection with unauthorized internal releases or uses of the information unlikely to result in harm – particularly if this term does not include a harm trigger. Accordingly, ACLI believe that the investigation requirements in Section 5 should not include requirements relating to the unauthorized release or use of sensitive personal information.

(vi) To address concern that has been raised with respect to use of the phrases "third-party service provider" and "third party," ACLI suggests substitution of the phrase "third party" with the phrase "other party" in Sections 5 and 6, as indicated below.

In view of all of the above, ACLI respectfully urges modification to the definitions of "Personal information" and "Third-party service provider," in Section 3, and to the language of Section 5, as proposed to be modified in the "Provisions related to Third-Party Service Providers – Proposed Revisions to Version 2 for Jan. 10 Drafting Group Call" to read as follows: (*Language proposed to be added is **IN RED, IN BOLD AND IN ALL CAPS**; language proposed to be deleted **[is stricken, in red, in brackets, and in bold].**):*

INSURANCE DATA SECURITY MODEL LAW
Provisions Related to Third-Party Service Providers
[Proposed Revisions to Version 2 for Jan. 10 Drafting Group Call]

Section 3. Definitions

As used in this Act, the following terms shall have these meanings:

H. "Personal Information" means~~:~~ **[~~information possessed by a licensee or provided by a licensee to a third party service provider and includes:~~]**

(1) A financial account number relating to a consumer, including a credit card number or

debit card number, in combination with any security code, access code, password, or other personal identification information required to access the financial account; or

***

I. "Third-party service provider" means a person or entity [~~,not otherwise defined as a licensee,~~] that contracts with a licensee to maintain, process, store or otherwise have access to personal information OWNED BY [~~under~~]the licensee. [~~'s possession, custody or control~~.]

***

Section 5. Investigation of a Data Breach

A. If the licensee learns that a data breach HAS OR MAY HAVE OCCURRED IN RELATION TO [~~of~~] personal information, LISTED IN SECTIONS 3(H)(1)(a)(I)-(IV), (H)(2), (H)(3), OR (H)(4),[1] OWNED BY THE LICENSEE OR MAINTAINED BY A THIRD PARTY SERVICE PROVIDER OF THE LICENSEE, [~~has or may have occurred~~] ~~in relation to personal information in the possession, custody or control of the licensee or any of the licensee's third party service providers,~~ the licensee [~~,~~] or [~~a third~~] OTHER party acting on behalf of THE [~~that~~] licensee, shall conduct a prompt investigation.

B. During the investigation, the licensee, or [~~a third~~] OTHER party acting on behalf of the licensee, shall, at a minimum:

(1) Assess the nature and scope of the data breach or potential data breach;

(2) Identify any personal information LISTED IN SECTIONS 3(H)(1)(a)(I)-(IV), (H)(2), (H)(3), or (H)(4) that may have been involved in the data breach;

(3) Determine whether the personal information LISTED IN SECTIONS 3(H)(1)(a)(I)-(IV), (H)(2), (H)(3), or (H)(4) has been acquired [~~, released or used~~] without authorization; and

(4) Perform or oversee reasonable measures to restore the security of the information systems compromised in the data breach in order to prevent further unauthorized acquisition [~~, release or use~~] of personal information LISTED IN SECTIONS 3(H)(1)(a)(I)-(IV), (H)(2), (H)(3), or (H)(4) [~~in~~] OWNED BY the licensee [~~'s possession, custody or control~~].

[1] These citations refer to subsections of the definition of "Personal information," as proposed to be modified in these comments (commencing on p. 21), that describe sensitive personal information.

~~[C. If the licensee learns that a data breach has or may have occurred in maintained by third party service provider, the licensee will confirm and document that the third-party service provider has completed the steps listed in Section 5B above.]~~

(iv) Section 6. Notification of Breach of Data Security

ACLI continues to believe that it is fundamentally important that all notices required under the Model Law, including notices to the commissioner, be subject to a harm trigger. ACLI respectfully submits that insurance licensees that investigate and learn about the details relating to an unauthorized acquisition of personal information (or data breach) are best positioned to determine whether there is a reasonable likelihood of resulting harm.

ACLI continues to believe that a harm trigger for consumer notices will avoid unnecessarily alarming consumers when there is little to no likelihood of harm and help protect against desensitization of consumers by over, duplicative, or conflicting notification. Similarly, a harm trigger for notification to commissioners will avoid unnecessary resource strain on state insurance departments. A harm trigger will avoid an unnecessary endless stream of ministerial notifications to consumers and insurance departments.

ACLI has the following concerns with the provisions of Section 6, as proposed to be modified in the "Provisions Related to Third-Party Service Providers – Proposed Revisions to Version 2 for Jan. 10 Drafting Group Call":

(i) The notice obligations throughout Section 6. are not applicable to sensitive personal information (i.e. Personal Information listed in specific sections of the definition of this term that describe sensitive personal information.).

(ii) Section 6.E. does not make it clear that when there is a data breach of a third-party service provider that maintains, but does not own, sensitive personal information, that the service provider shall immediately notify and coordinate with the licensee owner of the information.

(iii) Two important technical clarifications should be made to Section 6.F.: The title of this subsection should refer to notice of data breaches of reinsurers (rather than to notice regarding data breaches of insurers to reinsurers); and it should be clarified that in the event of data breach of a service provider of a licensee that is acting as an assuming insurer, the service provider shall provide notice to the licensee that is acting as an assuming insurer.

(iv) ACLI is respectfully opposed to a statutory requirement for insurers to notify producers of data breaches in view of all the other notice obligations imposed under Section 6.G. ACLI believes that requirements for notices between insurers and their producers are most appropriately governed by contractual arrangements between the parties. Relatedly, ACLI is concerned that the Model Law does not make it clear that nothing in the Model Law abrogates any agreements between a licensee and another licensee, a third-party

service provider or other third party to fulfill the investigation and notice requirements imposed under Sections 5 and 6, respectively. Accordingly, ACLI urges substitution of the current language of Section 6.G. with the language proposed below.

In view of all of the above, ACLI respectfully urges modification to the provisions of Section 6, as proposed to be modified in the "Provisions Related to Third-Party Service Providers – Proposed Revisions to Version 2 for Jan. 10 Drafting Group Call" as follows: (*Language proposed to be added is **IN RED, IN BOLD AND IN ALL CAPS**; language proposed to be deleted **[is stricken, in red, in brackets, and in bold].**):*

INSURANCE DATA SECURITY MODEL LAW
Provisions Related to Third-Party Service Providers
[Proposed Revisions to Version 2 for Jan. 10 Drafting Group Call]

***

Section 6. Notification of a Data Breach

A. If following an investigation under Section 5, the licensee determines that A DATA BREACH ~~[an unauthorized acquisition]~~of personal information listed in LISTED IN SECTIONS 3(H)(1)(a)(I)-(IV), (H)(2), (H)(3), or (H)(4)[2] ~~[Section 3H(1), (2)(a) through (f), (3) or (4) involved in a data breach]~~has occurred, the licensee, or OTHER ~~[a third]~~ party acting on behalf of the licensee, shall notify:

***

Notification to the Commissioner

Notwithstanding the responsibilities prescribed in Sections 5A and 6A of this Act, no later than three (3) business days after determining that a data breach has occurred, the licensee, or OTHER ~~[a third]~~ party acting on behalf of the licensee, shall notify the commissioner that a data breach has occurred. The licensee shall provide as much of the following information as possible:

***

C. Notification to Consumer Reporting Agencies

The licensee, or OTHER ~~[a third]~~ party acting on behalf of the licensee, shall notify, as expediently as possible and without unreasonable delay, after determining that a data breach has occurred, each consumer reporting agency, if the data breach involves personal information listed in SECTIONS 3(H)(1)(a)(I)-(IV), (H)(2), (H)(3), or (H)(4)

[2] These citations refer to subsections of the definition of "Personal information," as proposed to be modified in these comments (commencing on p. 21), that describe sensitive personal information.

Section 6D

This section setting notification to affected consumers has a number of significant problems.

Section 6D(1) arbitrarily eliminates consumer notification if certain types of personal information have been lost or stolen. As discussed above, we strongly oppose two categories of personal information for protection and for data breach notification purposes. If the personal information is sensitive enough to warrant protection, it is sensitive enough to warrant a data breach notice to a consumer if the personal information are lost or stolen. As we have stated many times, the data breach notification is the only substantive means to empower a consumer to take action to protect him or herself or their family.

The time frames provided insurers for data breach notices to consumers in Section 6D(1) are much too long and unnecessarily so. Timely notification is essential for consumers to take action to protect themselves in the event of lost or stolen personal information. The lengthy delay in consumer notification of data breaches in the current draft seriously compromises consumers' ability to take timely action to protect themselves.

In addition and just as important a problem, the time frame in the current draft is tied to the date of the breach and not to the date of approval of the notice by the commissioner. Our edits address these problems.

Our proposed edits include a provision requiring the licensee to develop a data breach notification template for pre-approval by the commissioner such that only items 6D(2)(a) and (b) need be added to the template in the event of a data breach. We also recommend that the NAIC or states adopting this provision develop these templates utilizing best practices in writing and testing consumer disclosures.

We also suggest replacing the vague "straightforward language" with the objective measure of text not exceeding a 10^{th} grade reading level. Alternatively, reference could be made to existing state readability and disclosure requirements in the insurance code. In addition, the model should incorporate or reference state laws requiring similar consumer notices be provided in languages in addition English. We do not attempt to set out these languages here as state laws presumably vary considerably.

In Section 6D(2)(a) we add language to specify that the notice include the specific types of personal information lost or stolen. This is one of the most important provisions because the purpose of the data breach notice is to empower consumers to take action to protect themselves. If the data breach notice provides only a generic description of the lost or stolen information – e.g. "your health information" – the notice will fail to achieve its purpose. If health information was breached, the notice should specify: your medical history, your medications and prescriptions, your current medical condition, your treatment history, etc.

In Section 6D(2)(b) refers to action taken to safeguard the information. It is unclear what it means to safeguard information that has been lost or stolen.

D. Notification to Consumers

(1) The licensee shall notify all consumers whose personal information ~~listed in Section 3H(1), (2)(a) through (f), (3) or (4) was affected~~ was part of the data breach as soon ~~expediently~~ as possible and ~~without unreasonable delay, in~~ no case later than five (5)~~sixty (60) calendar~~ business days after the licensee has received approval by the commissioner for the data breach notice. ~~determining that a data breach has occurred.~~

(2) Not later than ten (10) business days after determining that a data breach has occurred. The licensee shall submit to the ~~Prior to sending the notification, the licensee shall provide the~~ commissioner ~~with a draft of~~ the proposed data breach notification~~written communication~~ to consumers. The commissioner shall ~~have the right to~~ review and approve the data breach notification ~~proposed communication~~ before the licensee sends it to consumers~~, to ensure compliance with this subsection and to prescribe the appropriate level of consumer protection pursuant to Section 7.~~

As part of the licensee's data security program, the licensee shall prepare a draft notice containing parts c through g below for pre-approval by the commissioner so that in the event of a data breach the licensee need add only the information in sections a and b.

The notice ~~must be written in straightforward language and~~shall include the following information written at not greater than a 10th grade reading level~~:~~ [Add language requiring licensee to make available notices in languages other than English as appropriate or as directed by state law.]

(a) A description of the specific type of information involved in the data breach. . Specific types of personal information means particular data elements including, for example, types of medical information, types of financial information or types of information allowing identification of the consumer;

(b) A description of the action that the licensee or third-party service provider has taken to safeguard the information;

{Section c and d omitted to conserve space]

(e) Contact information for the ~~three~~ nationwide credit bureau consumer reporting agencies;

(f) Contact information for the licensee or its designated call center, including e-mail, internet and telephonic methods of contact; and

(g) An offer from the licensee to the consumer to provide appropriate identity theft protection services free of cost to the consumer for a period of not less than twelve (12) months, if appropriate, or other consumer protections ordered by the commissioner pursuant to Section 7 of this Act.

(3) The licensee will provide the consumer notification in the following order with notification by the second or third method only if the earlier method fails or is not available:

(a) By text to mobile devices if the consumer has agreed to be contacted in this manner ~~through e-mail or other means~~ pursuant to [insert reference to state Electronic Transactions Act.]; ~~or~~

(b) By e-mail , if the consumer has agreed to be contacted in this manner pursuant to [insert reference to state Electronic Transactions Act.];

(c) By letter sent by first-class mail;

(d) By substitute method, subject to approval by the commissioner. ~~if the licensee demonstrates to the commissioner's satisfaction that the cost of providing notice by Section 6D(3)(a) or (b) would be excessive or that another legitimate reason exists for substitute notice. The substitute method must include conspicuous posting of the notice on the licensee's publicly accessible website and publication in statewide xmedia in this state.~~

Section 6E

We offer modest edits to the version of this section in the January 24, 2017 call materials.

Notice Regarding Data Breaches of Third-Party Service Providers

In the event of a data breach in a system maintained by a third-party service provider, the licensee shall comply with the notice requirements of Sections 6A through D. T~~, unless~~ ~~t~~he third party service provider may ~~has agreed to~~ send the required notices on behalf of the licensee. I~~f~~~~n~~ the ~~event that the~~ licensee relies upon the third-party service provider ~~agrees~~ to send the required notices, the licensee will confirm and document that these actions were~~is was~~ completed as required in this Act, and if not, the licensee will be responsible for necessary additions or corrections to the notices. The computation of licensee's deadlines shall begin on the day after the third-party service provider notifies the licensee of the data breach or the licensee otherwise has actual knowledge of the data breach, whichever is sooner.

Section 7

Our principal comment on Section 7 is that the model could include a requirement that the credit bureau consumer reporting agencies provide credit freeze service without charge for a period of not less than 30 years to consumers whose personal information was part of a data breach. With this provision there is no need to include a provision for the commissioner to order a licensee to pay for credit freezes of data breach victims. A number of states already require consumer reporting agencies to provide credit freeze service without charge. Legislation to require free credit freeze services for victims of a data breach has been introduced in Maryland, as one example.[4]

If the section specifying that data breach victims shall have free access to credit freezes is not added, then the provision for the commissioner to direct a licensee to pay for data breach victims' credit freezes should be added back.

> Section 7. Consumer Protections Following a Data Breach
>
> After reviewing the licensee's data breach notification, the commissioner shall prescribe the appropriate level of consumer protection required following the data breach and how long that protection will be provided. The commissioner may order the licensee to offer to pay for twelve (12) months or more of identity theft protection for affected consumers~~, pay for a credit freeze,~~ or take other action deemed necessary to protect consumers.
>
> Notwithstanding any other law in this state, any consumer notified by a licensee of personal information acquired without authorization may utilize a credit freeze without charge by a consumer reporting agency for a period of not less than 30 years following data breach notification to the consumer. ~~Drafting Note: Many states have statutes providing that a consumer reporting agency cannot charge a fee for a credit freeze on a consumer file when the consumer is a victim of identity theft, which is shown by providing a police report. For an example, see Tex. Bus. & Com. Code § 20.04(b). As an alternative to having the licensee pay for the credit freeze, a state should consider referencing that law and providing that the credit freeze is free for consumers after the data breach is reported to law enforcement by the licensee, by showing a data breach notification letter from the licensee. The state may also need to amend its free credit freeze law to ensure this is covered.~~

[4] http://mgaleg.maryland.gov/2017rs/bills_noln/hb/thb0212.pdf

If the data breach has affected consumers in other states, the commissioner shall, consistent with the requirements of [reference to statute describing the commissioner's general powers] and with the circumstances of the data breach as they affect consumers in this state, cooperate with the insurance regulators of those states in prescribing the appropriate level of consumer protection described in the previous sentence.

Sections 8 and 9

We support sections 8 and 9 as drafted. We have previously commented on the reasonableness and necessity of Commissioner rulemaking authority.

Section 10

We oppose the inclusion of section 10. Existing statutes already provide protection for sensitive licensee information and consumer personal information, already provide regulators with the ability to confidentially share information with other regulators and law enforcement and already provide confidentiality for examination work papers. The proposed section 10 adds addition confidentiality provisions that conflict with consumer protection and with reasonable practices by regulators to date. Information provided to regulatory authorities under this Act should have the same level of protection as sensitive information provided to insurance departments when the departments are investigating other possible regulatory violations or conducting financial or market conduct examinations. Otherwise, the proposed section 10 provisions will prevent otherwise obtainable information from disclosure, undermining state public freedom of information laws.

If section 10 is retained, we suggest the following edits.

Section 10. Confidentiality

A. Any documents, materials or other information in the control or possession of the department of insurance that are furnished by a licensee or an employee or agent thereof acting on behalf of licensee pursuant to Section 6B~~(2), (3), (4), (5), (6), (8), (11), and (12),~~ or that are obtained by the insurance commissioner in an investigation or examination pursuant to Section 8 of this Act shall be subject to the same confidentiality provisions as [insert citation to state's examination law confidentiality provisions.] ~~by law and privileged, shall not be subject to [insert reference to state open records, freedom of information, sunshine or other appropriate law], shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action.~~

However, the insurance commissioner is authorized to use the documents, materials or other information in the furtherance of any regulatory or legal action brought as a part of the insurance commissioner's duties.

~~B. Neither the insurance commissioner nor any person who received documents, materials or other information while acting under the authority of the insurance commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to Section 10A.~~

B~~C~~. In order to assist in the performance of the insurance commissioner's duties under this Act, the insurance commissioner:

(1) May share documents, materials or other information, including the confidential and privileged documents, materials or information subject to Section 10A, with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient agrees to maintain the confidentiality and privileged status of the document, material or other information;

(2) May receive documents, materials or information, including otherwise confidential and privileged documents, materials or information, from the National Association of Insurance Commissioners, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material or information; and

(3) [OPTIONAL] May enter into agreements governing sharing and use of information consistent with this subsection.

C~~D~~. No waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information shall occur as a result of disclosure to the commissioner under this section or as a result of sharing as authorized in Section 10B~~C~~.

E. Nothing in this Act shall prohibit the insurance commissioner from releasing final, adjudicated actions including for cause terminations that are open to public inspection pursuant to [insert appropriate reference to state law] to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates or subsidiaries.

Drafting Note: States conducting an investigation or examination under their examination law may apply the confidentiality protections of that law to such an investigation or examination.

Section 12

As discussed in prior meetings, we support the inclusion of commissioner authority to promulgate regulations as necessary to implement and enforce this act. Such rulemaking authority is particularly important given the very broad and general requirements of section 4 for which regulators will surely develop best practices over time. We offer edits to clean up the current wording.

Section 12. Rules and Regulations

The commissioner is authorized to promulgate rules and regulations ~~may, upon notice and opportunity for all interested persons to be heard, issue such rules, regulations and orders~~ as ~~shall be~~ necessary to carry out the provisions of this Act. Any rulemaking pursuant to this section shall conform to the requirements of the [state administrative procedures act].

IIABA Comments (02/07 Call)

INSURANCE DATA SECURITY MODEL LAW

Section 3. Definitions

As used in this Act, the following terms shall have these meanings:

A. "Consumer" means an individual, including but not limited to applicants, policyholders, insureds, beneficiaries, claimants, certificate holders and others whose personal information is in a licensee's possession~~, custody or control~~.

~~B. "Consumer reporting agency" has the same meaning as "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis" in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).~~

Comment [WB1]: This definition is unnecessary if Section 6 is deleted.

~~C. "Data breach" means the unauthorized acquisition, release or use of personal information.~~

~~The term "data breach" does not include the unauthorized acquisition, release or use of encrypted personal information if the encryption, process or key is not also acquired, released or used without authorization.~~

Comment [WB2]: This definition is unnecessary if Section 6 is deleted.

~~D.~~B. "Encrypted" means the transformation of data into a form which results in a low probability of assigning meaning without the use of a protective process or key.

~~E. "Harm or inconvenience" means any of the following or the reasonable likelihood thereof:~~

Comment [WB3]: This definition is also unnecessary.

~~(1) Identity theft;~~

~~(2) Fraudulent transactions on financial accounts; or~~

~~(3) Other misuse as defined by [insert state definition of misuse or comparable term, if applicable].~~

~~Drafting Note: Several states have defined the term "misuse" in state law and can refer to this in Section 3E(3). If a state does not have this term defined, they may consider either deleting that paragraph or defining misuse above using a definition similar to that of other states. For example, see 17-A Me. Rev. Stat. § 905-A, which provides that~~

~~A person is guilty of misuse of identification if, in order to obtain confidential information, property or services, the person intentionally or knowingly:~~

~~A. Presents or uses a credit or debit card that is stolen, forged, canceled or obtained as a result of fraud or deception;~~
~~B. Presents or uses an account, credit or billing number that that person is not authorized to use or that was obtained as a result of fraud or deception; or~~
~~C. Presents or uses a form of legal identification that that person is not authorized to use.~~

~~F.~~C. "Information security program" means the safeguards that a licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personal information.

Comment [WB4]: We have not proposed the deletion of this definition, but we wonder if it is necessary in light of the specificity provided in Section 4.

~~G.~~D. "Licensee" means any person or entity licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this state.

~~H.~~E. "Personal Information" means:

Comment [WB5]: A definition of "personal information" is still needed, and this is one of the issues that the drafting group continues to discuss. There has been discussion of utilizing the Florida definition, and that is an approach IIABA could likely support.

~~I.~~F. "Third-party service provider" means a person or entity, other than a licensee, that contracts with a licensee to maintain, process, store or otherwise have access to personal information ~~under~~ for the licensee~~'s possession, custody or control~~.

Section 4. Information Security Program

A. Implementation of an Information Security Program

Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities and the sensitivity of the personal information in the licensee's possession~~, custody or control~~, each licensee shall develop, implement~~,~~ and maintain a comprehensive written information security program that

contains administrative, technical, and physical safeguards for the protection of personal information. The licensee shall document, on an ongoing basis, compliance with its information security program.

B. Objectives of Information Security Program

A licensee's information security program shall be designed to:

(1) Protect the security and confidentiality of personal information;

(2) Protect against any anticipated threats or hazards to the security or integrity of the information;

(3) Protect against unauthorized access to or use of personal information, and minimize the likelihood of harm or inconvenience to any consumer; and

(4) Define and periodically reevaluate a schedule for retention of personal information and a mechanism for its destruction when no longer needed.

C. Risk Assessment

The licensee or an entity acting on behalf of a licensee shall:

(1) Designate an employee or employees responsible for the information security program;

(2) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of personal information or personal information systems;

(3) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;

(4) Assess the sufficiency of policies, procedures, personal information systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the licensee's operations, including:

(a) Employee training and management;

(b) Information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and

(c) Detecting, preventing, and responding to attacks, intrusions, or other systems failures; and

(5) Implement information safeguards to manage the threats identified in its assessment, and regularly assess the effectiveness of the safeguards' key controls, systems, and procedures.

D. Risk Management

The licensee shall~~, at a minimum: (1) D~~design its information security program to mitigate the identified risks, commensurate with the sensitivity of the personal information in the licensee's possession, ~~as well as~~ the size and complexity of the licensee, and the nature and scope of the licensee's activities~~, based on generally accepted cybersecurity principles, including~~ The licensee shall consider whether the following security measures~~, as~~ are appropriate for the licensee and, if so, implement such measures:

Comment [WB6]: The revisions proposed here are included for the purpose of clarity and are intended to more closely mirror Section 4(A).

(1~~a~~) Place access controls on information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent the unauthorized acquisition, release or use of personal information to or by employees or unauthorized individuals outside of the licensee;

(2~~b~~) Restrict access at physical locations containing personal information, only to authorized individuals;

IIABA Comments (02/07 Call)

(3c) Encrypt all personal information while being transmitted on a public internet network or wirelessly and all personal information stored on a laptop computer or other portable computing or storage device or media;

(4d) Ensure that information system modifications are consistent with the licensee's information security program;

(5e) Utilize ~~state-of-the-art techniques, such as multi-factor~~ authentication procedures, segregation of duties, and employee background checks for employees with responsibilities for, or access to, personal information;

(6f) Regularly test or monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

(7g) Implement response procedures that specify actions to be taken when the licensee suspects or detects that unauthorized individuals have gained access to information systems;

(7h) Implement measures to protect against destruction, loss, or damage of personal information due to environmental hazards, such as fire and water damage or technological failures; ~~and~~

(8i) Develop, implement, and maintain procedures for the secure disposal of personal information in any format; and~~.~~

(92) Include cybersecurity risks in the licensee's enterprise risk management process.~~; and~~

~~(3) Use generally accepted cybersecurity principles to share information and stay informed regarding emerging threats or vulnerabilities.~~

E. Oversight by Board of Directors

If the licensee has a board of directors, the board or an appropriate committee of the board shall~~, at a minimum~~:

(1) Oversee the development, implementation, and maintenance of the licensee's information security program, including assigning specific responsibility for the plan to the licensee's executive management; and

(2) Require the licensee's executive management to report in writing at least annually, the following information:

(a) The overall status of the information security program and the licensee's compliance with this Act; and

(b) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, data breaches or violations and management's responses thereto, and recommendations for changes in the information security program.

F. Oversight of Third-Party Service Provider Arrangements

(1) The licensee shall

(a1) Exercise due diligence in selecting each third-party service provider; and

(b2) Confirm and document with each third-party service that it is able to implement appropriate measures to secure the licensee's personal information that is held in a system maintained by the third-party service provider.

(2) A third-party service provider shall:

Comment [WB7]: Section 4(F)(1) incorporates the revisions discussed on the January 10 drafting group call. As discussed, we also propose the addition of Section 4(F)(2), a series of tailored provisions that would apply directly to third-party service providers.

IIABA Comments (02/07 Call)

(a) Implement appropriate administrative, technical, and physical measures to protect and secure the personal information that a third-party service provider has been contracted to maintain, process, store, or otherwise access for a licensee;

(b) Upon request from a licensee, represent and warrant compliance with the requirements of subparagraph (a) in writing; and

(c) If a third-party service provider learns that a ["data breach" or other term of art used in the state's data breach notification law] involving the personal information that a third-party service provider has been contracted to maintain, process, store, or otherwise access for a licensee has occurred, the third-party service provider shall notify the licensee in the most expedient time possible and without unreasonable delay.

Comment [WB8]: This provision is intended to be the mirror image of Section 4(F)(2). Alternatively, this provision could require third-party service providers that handle personal information to comply with the information security requirements of Section 4(A-E) and 4(G).

G. Program Adjustments

The licensee shall monitor, evaluate and adjust, as appropriate, the information security program consistent with any relevant changes in technology, the sensitivity of its personal information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to personal information systems.

Section 5. Notification to the Commissioner

A licensee shall notify the commissioner when a ["data breach" or other term of art used in the state's data breach notification law] has occurred. The notification to the commissioner shall be made no later than three (3) business days after determining that a data breach has occurred and in a manner consistent with the requirements of [insert reference to the state's data breach notification law].

Comment [WB9]: The goal with this provision is to ensure that regulators receive notice when their licensees are the victims of a data breach. There may be other ways to address this particular issue, and we are certainly prepared to discuss this and other options.

~~**Section 5. Investigation of a Data Breach**~~

Comment [WB10]: As we discussed, we propose the deletion of Section 5-7.

~~A. If the licensee learns that a data breach has or may have occurred in relation to personal information in the possession, custody or control of the licensee or any of the licensee's third-party service providers, the licensee shall conduct a prompt investigation.~~

~~B. During the investigation, the licensee shall, at a minimum:~~

~~(1) Assess the nature and scope of the data breach or potential data breach;~~

~~(2) Identify any personal information that may have been involved in the data breach;~~

~~(3) Determine whether the personal information has been acquired, released or used without authorization; and~~

~~(4) Perform or oversee reasonable measures to restore the security of the information systems compromised in the data breach in order to prevent further unauthorized acquisition, release or use of personal information in the licensee's possession, custody or control.~~

~~**Section 6. Notification of a Data Breach**~~

~~A. If following an investigation under Section 5, the licensee determines that an unauthorized acquisition of personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) involved in a data breach has occurred, the licensee, or a third party acting on behalf of the licensee, shall notify:~~

~~(1) All consumers to whom the personal information relates;~~

~~(2) The insurance commissioner in the licensee's state of domicile and the insurance commissioners of all the states in which a consumer whose information was or may have been compromised resides;~~

(3) The relevant Federal and state law enforcement agencies, as appropriate;

(4) Any relevant payment card network, if the data breach involves payment card numbers; and

(5) Each consumer reporting agency, if the data breach involves personal information relating to 500 or more consumers.

B. Notification to the Commissioner

Notwithstanding the responsibilities prescribed in Sections 5A and 6A of this Act, no later than three (3) business days after determining that a data breach has occurred, the licensee shall notify the commissioner that a data breach has occurred. The licensee shall provide as much of the following information as possible:

(1) Date of the data breach;

(2) Description of the data breach, including how the information was exposed, whether lost, stolen, or breached;

(3) How the data breach was discovered;

(4) Whether any lost, stolen, or breached information has been recovered and if so, how this was done;

(5) The identity of the source of the data breach;

(6) Whether licensee has filed a police report or has notified any regulatory, government or law enforcement agencies and, if so, when such notification was provided;

(7) Description of the type of information lost, stolen, or breached (equipment, paper, electronic, claims, applications, underwriting forms, medical records etc.);

(8) Whether, if the information was encrypted, the encryption, redaction or protection process or key was also acquired without authorization;

(9) The period during which the information system was compromised by the data breach;

(10) The number of total consumers and consumers of each state affected by the data breach;

(11) The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;

(12) Identification of efforts being undertaken to remediate the situation which permitted the data breach to occur;

(13) A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the data breach; and

(14) Name of a contact person who is both familiar with the data breach and authorized to act for the licensee.

The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the commissioner concerning the data breach.

C. Notification to Consumer Reporting Agencies

~~The licensee shall notify, as expediently as possible and without unreasonable delay, after determining that a data breach has occurred, each consumer reporting agency, if the data breach involves personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) relating to 500 or more consumers. Notification must include the date of the data breach, an estimate of the number of persons affected by the data breach, if known, and the actual or anticipated date that persons were or will be notified of the data breach.~~

~~D. Notification to Consumers~~

~~(1) The licensee shall notify all consumers whose personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) was affected as expediently as possible and without unreasonable delay, and in no case later than sixty (60) calendar days after determining that a data breach has occurred.~~

~~(2) Prior to sending the notification, the licensee shall provide the commissioner with a draft of the proposed written communication to consumers. The commissioner shall have the right to review the proposed communication before the licensee sends it to consumers, to ensure compliance with this subsection and to prescribe the appropriate level of consumer protection pursuant to Section 7.~~

~~The notice must be written in straightforward language and include the following information:~~

~~(a) A description of the type of information involved in the data breach;~~

~~(b) A description of the action that the licensee or third-party service provider has taken to safeguard the information;~~

~~(c) A summary of rights of victims of identity theft prepared under § 609(d) of the Fair Credit Reporting Act (15 U.S.C. 1681g(d));~~

~~(d) The steps consumers can take to protect themselves from identity theft or fraud, which shall include an explanation that consumers shall have a right to do the following:~~

~~(i) Place a 90-day initial fraud alert on their consumer reports;~~

~~(ii) Place a seven-year extended fraud alert on their consumer reports;~~

~~(iii) Place a credit freeze on their consumer reports;~~

~~(iv) Have a free copy of their consumer report from each credit bureau;~~

~~(v) Receive fraudulent information related to the data breach removed (or "blocked") from their consumer reports;~~

~~(vi) Dispute fraudulent or wrong information on their consumer reports;~~

~~(vii) Stop creditors and debt collectors from reporting fraudulent accounts related to the data breach;~~

~~(viii) Receive copies of documents related to the identity theft; and~~

~~(ix) Stop contacts from debt collectors related to the data breach;~~

~~(e) Contact information for the three nationwide consumer reporting agencies;~~

~~(f) Contact information for the licensee or its designated call center; and~~

~~(g) An offer from the licensee to the consumer to provide appropriate identity theft protection services free of cost to the consumer for a period of not less than twelve (12) months, if appropriate, or other consumer protections ordered by the commissioner pursuant to Section 7 of this Act.~~