Sections 2 and 3 Discussion Document (from the 12/20/16 call)

Insurance Data Security Model Law

Section 2. Purpose and Intent

A. Notwithstanding any other provision of law including [insert reference to state's general data security breach notification law], the purpose and intent of this Act is to establish the exclusive standards in this state for data security and investigation and notification of a data breach applicable to licensees, as defined in Section 3G~~.~~.

B. It is not the intent of this Act to require that a licensee send notice to consumers affected by a data breach under Section 6D when notice has been or is being sent to consumers in accordance with a federal statute or regulation applicable to that licensee. It is also not the intent of this Act that a licensee be required to set up a separate information security program under Section 4 if that licensee has established and maintained an information security program in accordance a federal statute or regulation applicable to that licensee. If a licensee relies upon this provision it shall provide to the Commissioner upon request the specific federal statute or regulation upon which it relies and the manner in which it asserts compliance.

A licensee subject to and compliant with the privacy and information security program requirements of Pub.L. 106–102, 113 Stat. 1338, enacted November 12, 1999, or to Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996, any amendments thereto, and any accompanying regulations ~~such statutes, or rules, regulations, procedures or guidelines established thereunder~~, is deemed compliant with Section 4, Information Security Program, of this Act to the extent such statutes, rules, regulations, procedures, or guidelines apply to all personal information, as defined in Section 3H, in whatever form maintained by that licensee.

Comment [JMM1]: We may place this language in Section 4.

A licensee subject to and compliant with data breach notification requirements of Pub.L. 106–102, 113 Stat. 1338, enacted November 12, 1999, or to Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996, any amendments thereto, and any accompanying regulations ~~such statutes, or rules, regulations, procedures or guidelines established thereunder~~, is deemed compliant with Section 6D, Notification to Consumers. ~~This Act shall not be construed as superseding, altering, or affecting any statute, regulation, order or interpretation of law in this state, except to the extent that such statute, regulation, order or interpretation is inconsistent with the provisions of this Act and then only to the extent of the inconsistency. A state statute, regulation, order or interpretation is not inconsistent with the provisions of this Act if the protection such statute, regulation, order or interpretation affords any person is greater than the protection provided under this Act.~~

Comment [JMM2]: We may place this language in Section 6.

C. This Act may not be construed to create or imply any new private cause~~s~~ of action for violation of its provisions that does not already exist under the laws of this state nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

Drafting Note: This model law is intended to supplant the provisions of the NAIC's Standards for Safeguarding Consumer Information Model Regulation (#673). Therefore, states that have adopted that model law should repeal it when it enacts this 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)).

C. "Data breach" means the unauthorized acquisition, release or use of personal information that is reasonably likely to result in harm or inconvenience to a Consumer.

Comment [JMM3]: We will be discussing the definition of data breach on the call. Look for the Data Breach Definition Comparison Chart posted under Meeting Materials at: http://www.naic.org/cmte_ex_cybersecurity_tf.htm .

The term "data breach" does not include:

(1) the unauthorized acquisition, release or use of ~~encrypted~~ personal information that is encrypted or otherwise protected by another method that renders the information unreadable, unusable, inaccessible, or indecipherable if the encryption~~,~~ or other protective process or key is not also acquired, released or used without authorization.

(2) the good faith acquisition of personal information by an employee if not subject to further disclosure; or

(3) the unauthorized disclosure of personal information to an employee of another licensee if no further disclosure~~.~~

(4) the unauthorized disclosure of personal information where the licensee has a good faith belief that the person to whom the unauthorized disclosure was made is not reasonably able to retain the information.

D. "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:

(1) Identity theft;

(2) Other types of fraud; or ~~Fraudulent transactions on financial accounts;~~ ~~or~~

(3) Any act or event that results in financial or reputational damage or loss of privacy to the consumer.

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

G. "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. "Personal Information" means:

(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

(2) ~~Information including:~~

The first name or first initial and last name of a Consumer in combination with:

(a) The Consumer's non-truncated social security number;

(b) The Consumer's driver's license number, passport number, military identification number, or other similar number on a government-issued document;

~~(c) A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online or financial account of the Consumer;~~

(~~d~~ c) Biometric data of the Consumer that would permit access to financial accounts of the Consumer;

(~~e~~ d) Any information of the Consumer that the licensee has a legal or contractual duty to protect from unauthorized access or public disclosure;

~~(f) The Consumer's date of birth;~~

(~~g~~ e) Information that the Consumer provides to a licensee to obtain an insurance product or service used primarily for personal, family, or household purposes from the licensee;

(~~h~~ f) Information about the Consumer resulting from a transaction involving an insurance product or service used primarily for personal, family, or household purposes between a licensee and the Consumer;

(~~i~~ g) Information the licensee obtains about the Consumer in connection with providing an insurance product or service used primarily for personal, family, or household purposes to the Consumer; or

(~~i~~ h) A list, description, or other grouping of Consumers (and publicly available information pertaining to them), that is derived using the information described in Section 3H(2)(g) through (i), that is not publicly available.

(3) A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online or financial account of the Consumer;

(~~3~~ 4) Any of the data elements identified in Section 3H(2)(a) through (f) when not in connection with the Consumer's first name or initial and last name, if those elements would be sufficient to permit the fraudulent assumption of the Consumer's identity or unauthorized access to an account of the Consumer.

(~~4~~ 5) The first name or first initial and last name of a Consumer in combination with any information or data except age or gender, that relates to:

(a) The past, present or future physical, mental or behavioral health or condition of a Consumer;

(b) The provision of health care to a Consumer; or

(c) Payment for the provision of health care to a Consumer.

The term "personal information" does not include publicly available information that is lawfully made available to the general public and obtained from federal, state, or local government records; or widely distributed media.

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

Third-Party Service Provider Provisions Redline Document

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 under the licensee's possession, custody or control.

Section 4. Information Security Program

F. Oversight of Third-Party Service Provider Arrangements

The licensee shall:

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

~~(1)~~(2) 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.~~

Section 5. Investigation of a Data Breach

A. If the licensee learns that a data breach of personal information 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~~occurred, the licensee, or a third party acting on behalf of that licensee, shall conduct a prompt investigation.

B. During the investigation, the licensee, or a third 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 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.

C. If the licensee learns that a data breach has or may have occurred in in a system maintained by a 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.

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:

* * *

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, or 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 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 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

The licensee, or a third party acting on behalf of 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.

*** * ***

E. 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, unless the third-party service provider has agreed to send the notices. In the event that the third-party service provider agrees to send the notices, licensee will confirm and document that this was completed. 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.

F. Notice Regarding Data Breaches of Insurers to Reinsurers

(1) In the event of a data breach involving personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) where the licensee is acting as an assuming insurer and does not have a direct contractual relationship with the affected consumers:

(a) The assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile; and

(b) The ceding insurers that have a direct contractual relationship with the affected consumers shall fulfill the notification requirements imposed under Section 6A through D.

(2) In the event of a data breach involving personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) that is held in a system maintained by a third-party service provider of a licensee acting as an assuming insurer and does not have a direct contractual relationship with the affected consumers, the third-party service provider shall notify the licensee of the data breach immediately upon determination that a breach has occurred.

G. Notice Regarding Data Breaches of Insurers to Producers of Record

In the event of a data breach involving personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) where the licensee is an insurer, the insurer shall, without unreasonable delay, notify the producers of record of all affected consumers.

Definitions ABA Refers to in Comment Letter Dated January 9

Definitions ABA Refers to in Comment Letter Dated January 9, 2017

Standards for Safeguarding Consumer Information Model Regulation (#673)
Section 2 - Definitions

A. "Customer information" means nonpublic personal information as defined in Section [cite applicable section of state regulation that corresponds with Section 4S of the NAIC Privacy of Consumer Financial and Health Information Model Regulation] about a customer, whether in paper, electronic or other form, that is maintained by or on behalf of the licensee.

Privacy of Consumer Financial and Health Information Regulation (#672)
Section 4 - Definitions

S. "Nonpublic personal information" means nonpublic personal financial information and nonpublic personal health information.

T. (1) "Nonpublic personal financial information" means:

(a) Personally identifiable financial information; and

(b) Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

(2) Nonpublic personal financial information does not include:

(a) Health information;

(b) Publicly available information, except as included on a list described in Subsection T(1)(b) of this section; or

(c) Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.

(3) Examples of lists.

(a) Nonpublic personal financial information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information that is not publicly available, such as account numbers.

(b) Nonpublic personal financial information does not include any list of individuals' names and addresses that contains only publicly available information, is not derived in whole or in part using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

U. "Nonpublic personal health information" means health information:

(1) That identifies an individual who is the subject of the information; or

(2) With respect to which there is a reasonable basis to believe that the information could be used to identify an individual.

V. (1) "Personally identifiable financial information" means any information:

(a) A consumer provides to a licensee to obtain an insurance product or service from the licensee;

(b) About a consumer resulting from a transaction involving an insurance product or service between a licensee and a consumer; or

(c) The licensee otherwise obtains about a consumer in connection with providing an insurance product or service to that consumer.

(2) Examples.

(a) Information included. Personally identifiable financial information includes:

(i) Information a consumer provides to a licensee on an application to obtain an insurance product or service;

(ii) Account balance information and payment history;

(iii) The fact that an individual is or has been one of the licensee's customers or has obtained an insurance product or service from the licensee;

(iv) Any information about the licensee's consumer if it is disclosed in a manner that indicates that the individual is or has been the licensee's consumer;

(v) Any information that a consumer provides to a licensee or that the licensee or its agent otherwise obtains in connection with collecting on a loan or servicing a loan;

(vi) Any information the licensee collects through an Internet cookie (an information-collecting device from a web server); and

(vii) Information from a consumer report.

(b) Information not included. Personally identifiable financial information does not include:

(i) Health information;

(ii) A list of names and addresses of customers of an entity that is not a financial institution; and

(iii) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names or addresses.