ACLI Comments

11/22 Proposed Revisions

Insurance Data Security Model Law

Section 2. Purpose and Intent

ACLI believes it is most important that this section make it clear that the Insurance Data Security Model Act (Act) is intended to establish the exclusive standards for data security and investigation and breach notification in the state.

Accordingly, we very much appreciate the proposed modification to this section to eliminate the sentences: "This Act shall not be construed as superseding, altering or affecting any statute, regulation, order or interpretation of law in this state …. A state statute, regulation, or interpretation is not inconsistent with the provisions of this Act …"

ACLI also recognizes the importance of trying to lessen consumer confusion by eliminating duplicative notices relating to the same breach.

At the same time, ACLI is concerned that the proposed 11/22 modifications to Section 2 to provide for deemers of compliance for licensees subject to and compliant with the federal Gramm Leach Bliley Act (GLBA) and rules and regulations promulgated thereunder is likely to give rise to confusion. This is the case for several reasons. The GLBA itself does not impose any breach notification requirements. Also, there is no intent to provide a deemer of compliance with the Act based on compliance with the NAIC Standards for Safeguarding Consumer Information Model Regulation (Model Safeguards Regulation), that provides for implementation of the GLBA security requirements by insurance licensees. In fact, the goal is for the Act to supplant the Model Safeguards Regulation.

Given the above, ACLI suggests that the 11/22 version of Section 2 be clarified by eliminating the two provisions for deemers for compliance with the GLBA and rules and regulations established thereunder.

ACLI also suggests elimination of the proposed drafting note. If the two provisions relating to the GLBA deemers are eliminated, there is less reason to include the proposed drafting note. The possible effect of the proposed drafting note is not altogether clear, which also could give rise to confusion.

More specifically, ACLI suggests that the 11/22 version of Section 2 modified to read in pertinent part as follows *(Language proposed to be deleted is in **[bold and brackets.]**)*:

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 .... and the manner in which it asserts compliance.

A licensee subject to and compliant with the privacy and information security requirements under [under Pub.L. 106-102, 113 Stat. 1338, enacted November 12, 1999, or to] Pub. L. 104-191, 110 Stat. 1936, enacted 21, 1996, and 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.

A licensee subject to and compliance with data breach notification requirements under [Pub. L 106-102, 113 Stat. 1338, enacted November 12, 1999, or to] Pub. L. 104-191, 110 Stat. 1936, enacted August 2, 1996, and such statues 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.~~

C. This Act may not be construed to create or imply any new private causes of action for violation of its provisions that don not already exist in 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

Comparison of Insurance Data Security Model Law (proposed v.3) "Data Breach" Definition/Harm Trigger with HIPAA and California Laws

Comments on Definitions of "Data Breach" and "Harm or Inconvenience" in 11/22 draft of Model Law

As previously stated, ACLI believes it is fundamentally important that all notices required under the Model Law, including notices to the commissioner, be subject to a harm trigger.

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 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.

Accordingly, ACLI believes it is very important and much appreciates that the definition of "Data breach" proposed in the 11/22 draft includes a harm trigger, that refers to the likelihood of harm or inconvenience to a consumer.

At the same time, ACLI is very concerned by the proposed modifications to the definition of "Harm or inconvenience" in the 11/22 draft. These modifications could completely undercut the harm trigger provided in the definition of "Data breach." ACLI respectfully submits that any unauthorized acquisition, release, or use of personal information may be construed to be a "loss of privacy;" and the legal meaning or effect of the phrases "Other types of fraud" and "reputational damage" are very unclear. ACLI urges that the definition of "Harm or inconvenience" be as clear as possible and focus on identity theft and financial fraud, in line with primary concern with security breaches.

In addition, ACLI is concerned that the definition of "Data breach" in the 11/22 draft:

(i) refers to the unauthorized acquisition of "Personal information," rather than sensitive personal information (or personal information listed under Sections 3.H.(1)(b)(i)-(iv) and Section 3.H.(1)(c), as the definition of "Personal information," is proposed to be modified below);

(ii) is not limited to unauthorized acquisition of sensitive personal information that is likely to compromise the confidentiality, security and integrity of the information, in line with the majority of existing state breach notification laws and the HIPAA definition of "breach."

(iii) does not exclude the good faith acquisition of the information or disclosure by an agent (in addition to an employee) of a licensee if the information is not subject to further disclosure; and

(iv) does not exclude unauthorized disclosures of sensitive personal information in connection with which the recipient did not actually acquire or view the information or the risk to the information has been mitigated.

In view of the above, ACLI urges that the definitions of "Data breach" and "Harm or inconvenience" in the 11/22 draft be modified to read as follows *(Language proposed to be added is **in bold and underlined;** Language proposed to be deleted is in **[bold and brackets.]**):*

C. "Data breach" means the unauthorized acquisition, release or use of encrypted personal information **listed in Sections 3.H.(1)(a)(i)–(iv) and Section 3.H.(1)(c)** that is reasonably likely to **compromise the confidentiality, security and integrity of the information and to** result in harm or inconvenience to a Consumer.

The term "data breach" does not include:

(1) the unauthorized acquisition, release or use of ~~encrypted~~ personal information **listed in Sections 3.H.(1)(a)(i)–(iv) and Section 3.H.(1)(c)** 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) good faith acquisition by an employee **or agent** if not subject to further disclosure; **[or]**

(3) unauthorized disclosure to an employee **or agent** of another licensee if no further disclosure**; or**

(4) unauthorized disclosure where the information is not actually acquired or viewed or the risk to the information has been mitigated.

D. "Harm or inconvenience" means either [any] of the following or the reasonable likelihood thereof:
   (1) Identity theft; or
   (2) Financial fraud. [Other types of fraud, or;} ~~Fraudulent transactions on financial accounts; or~~
   (3) [Any act that results in financial or reputational damage or loss of privacy to the consumer;] ~~(3) Other misuse as defined by [insert definition of misuse or comparable term, if applicable.]~~

ACLI believes a breach notification statute that reflects the approach and includes definitions of "Data breach" and "Harm or inconvenience," as proposed above, will most effectively protect against desensitization of consumers and unnecessary resource strain on state insurance departments.

Comments on definition of "Data Breach" and Harm Trigger in HIPAA Privacy Rule

Use of the definition of "Breach" and the harm trigger(s) in the HIPAA privacy rule at 45 CFR Section 164.402, modified as necessary to refer to licensees, sensitive personal information (or personal information listed in Sections 3.H.(1)(a)(i)–(iv) and Section 3.H.(1)(c)) and as otherwise technically necessary, may be acceptable: (i) provided the language in the definition referring to compromise of the privacy and security of the information, the exclusions in subsection (1), and the specific exclusions from the presumption of a breach when there is a low probability of compromise to the information in subsection (2) are included; and (ii) depending on other requirements in the draft relating to breach notification.

Comments on definition of "Data Breach" and Harm Trigger in California Statute

A determination of whether the California approach may be acceptable would be based on the definition of "breach of the security of the system," set forth in 1798.82(g) as well as the language in section 1798.82(a) (provided in the comparison); and would be particularly dependent on other requirements in the Act relating to breach notification, including, but not limited to, thresholds of numbers of affected consumers for notice.

Comments on the definition of "Personal Information" in the 11/22 draft

As previously indicated, ACLI believes that the Model Law's security requirements should be applicable to "personal information," and that its breach investigation and notice requirements should be applicable to a subset of personal information, sensitive personal information (i.e. "personal information listed in Sections 3.H.(1)(a)(i)-(iv) and Section 3.H.(1)(c)), as the term is proposed to be modified below), the unauthorized acquisition of which may render the subject of the information vulnerable to identity theft or fraud.

ACLI very much appreciates the apparent effort, reflected in the 8/17/2016 (version 2) draft, to make this distinction in the applicability of the security and the notice requirements, by making the

notice requirements in Sections 6.A., 6.C., and 6.D. applicable only to personal information "listed in Section 3.H.(1), (2)(a)-(f), (3), or (4)."

ACLI also appreciates the proposed modifications to the definition reflected in the 11/22 draft to eliminate the consumer's date of birth and to associate health information with the name of an individual. Unfortunately, however, ACLI continues to have a number of concerns with the definition of "Personal information" as proposed in the 11/22 draft.

The definition is not limited to information of residents of the state in which the Act is enacted. This gives rise to significant concern that the Act may be construed to be extraterritorial in effect. It also is likely to cause confusion in the implementation and enforcement of the Act's security and breach investigation and notice requirements.

Notwithstanding the language in Sections 6.A., 6.C., and 6.D., of the 8/17 draft, discussed above, ACLI is concerned by the definition as proposed in the 11/22 draft for purposes of the Model Law's security as well as its investigation and breach notification requirements for the following reasons:

(i) The continued inclusion of "any information of the consumer that the licensee has a legal or contractual duty to protect …" in Section 3.H.(2)(d) is unnecessary given the breadth of information that may fall within the scope of Sections 3.H.(2)(e) – (g), that is required to be protected under the GLBA and state regulations tracking the NAIC Standards for Safeguarding Customer Information (Model Safeguards Regulation). Also, it is unclear what information may fall within the scope of Section 3.H.(2)(d) given the difficulty of determining what information is or may be required to be protected under any other federal or state laws.

(ii) It is not clear what information may be construed to fall within the scope of Section 3.H.(4). It seems likely to be very difficult, if not impossible, to determine in the abstract which, if any, of the data elements described in Section 3.H.(2)(a)-(f), when not in combination with an individual's name, would be sufficient to permit the fraudulent assumption of the individual's identity.

In addition, while notice is not required under Sections 6.A., 6.C., and 6.D.of the 8/17 draft in connection with data breaches involving personal information listed in Sections 3.H.(2)(g) – (i), notice still is required in connection with data breaches involving "any information of the consumer that the licensee has a legal or contractual duty to protect …" (Section 6.H.(2)(d)). As indicated above, the latter includes the information described in Sections 3.H.(2)(e) – (g), that includes almost any personal information of a consumer obtained by a licensee in connection with the provision of insurance products or services.

Finally, ACLI also has the following technical concern: Financial account number, described in Section 3.H.(1), should be associated with an individual's name and should not include an insurance policy number.

In view of the above, ACLI urges that the definition of "Personal information" in the 11/22 draft be modified to read as follows *(Language proposed to be added is **in bold and underlined;** Language proposed to be deleted is in **[bold and brackets.]**):*

H. "Personal information" means:

(1) ~~A financial account number relating to a Consumer, including a credit 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~~

(1) Any following information of a consumer who is a resident of this state, whether in paper or electronic form, that is in the possession, custody or control of a licensee: ~~Information including~~**:**

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

(i) the consumer's non-truncated social security number;

(ii) the consumer's driver's license number, passport number, military identification number, or similar identification number issued by the federal or a state government;

~~(c)A user name or email address, in combination with a password or security question and answer that would permit access to a financial account of the consumer~~

(iii) Biometric data of the consumer that would permit access to financial accounts of the consumer;

(iv) the consumer's financial account number, other than an insurance policy number, 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 consumer's financial account;

(v) Information that the consumer provides to a licensee to obtain an insurance product or service to be used primarily for personal, family, or household purposes

(vi) Information about the consumer resulting from a transaction involving an insurance product or service used primarily for personal, family, or household purposes;

(vii) 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

(viii) A list, description, or other grouping of consumers, and other publicly available information pertaining to them, that is derived using the information described in subsections (i) – (vii), that is not publicly available;

(b) **[(~~3~~)]** A user name or email address, in combination with a password or security question and answer that would permit access to a financial account of the consumer; **or**

~~[(4) Any of the data elements identified in Section 3H2)(a) through (f) ...]~~

(c) [~~(5)~~] The first name or first initial and last name of the consumer in combination with information, except age or gender, that relates to:

(i) the past, present, or future physical, mental, or behavioral health or condition of the consumer;

(ii) the provision of health care to the consumer; or

(iii) payment for the provision of health care to the consumer.

(2) Does not mean information that is:

(i) publicly available, except as included on a list described in subsection (1)(b)(vii) or

(ii) any list, description, or other grouping of individuals (and publicly available information pertaining to them) that is derived without using any information that is not publicly available.

Comments from Steve Gottheim (ALTA)

1. On 2(b), our focus is to ensure that this model law both helps to promote uniformity among the states and federal law and doesn't create a conflict between the requirements that title insurance agents/settlement companies must comply with under the different state and federal laws. This is why we favor the deemed compliance language. I have a question about the last sentence of the first paragraph of 2(b). When is the the notification to the commissioner of reliance on the federal law provision meant to occur? After a breach when asserting that no duplicative notice is required? Before the breach or during an examination?

2. On 2(c), should the new addition say, "that do not already exist UNDER THE LAWS of this state,"? I am not sure if the NAIC has any drafting styles or conventions, but this would be more consistent with the style promoted by the Uniform Law Commission.

3. Should the language that you added to (c)(1) just be incorporated into the definition of encryption? We agree with the comment that the law should try to be more evergreen by not relying on current technology.

4. While I think a harm trigger is a good idea, what is more important is cleaning up the definition of personal information. Our view is that even if a breach occurs, if the information obtained could also have been obtained by an unauthorized person through publicly available source (both governmental and commercial), then a notification should not be required. The example that I think best undercuts this is 3(H)(3)(f) or (g). In most applications for insurance, the consumer will provide or the licensee will obtain the consumers address or birth date along with their name. If those are the only pieces of data obtained during a breach, the model suggests a notice may be required. However, that information is also publically available in government records, the phone book, or social media. The potential harm to the consumer is not increased by the breach in this instance.

5. On the California language, would you propose to also keep the exceptions to the term breach as found in the current model? Combining the two may be the best way to thread both needles.

6. If we go away from a harm trigger, then it would be helpful to consider an exception to the definition of a breach where the licensee reasonably believes that the unauthorized person will not use the personal information to cause harm or inconvenience to the consumer. This would be an attempt to address the scenario where the spouse of an employee of the licensee happens to see one consumer's information on a computer screen while the employee is working from home.

Insurance Data Security Model Law
[CA Proposed Revisions to Version 2 – for discussion on Nov. 29 Drafting Group Call]

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~~ minimum standards in this state for data security and investigation and notification of a data breach applicable to licensees, as defined in Section 3G. 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.

~~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.~~

Comment [DD1]: Relocated in part to Section 6(D)(4); intention is to avoid duplicative notice issue.

~~A licensee subject to and compliant with the privacy and information security program requirements under Pub.L. 106–102, 113 Stat. 1338, enacted November 12, 1999, or to Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996, and 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. A licensee subject to and compliant with data breach notification requirements under Pub.L. 106–102, 113 Stat. 1338, enacted November 12, 1999, or to Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996, and 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.~~

B~~C~~. This Act may not be construed to create or imply any new private causes of action for violation of its provisions that do not already exist in 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~~ enacting 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.~~

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) good faith acquisition by an employee if not subject to further disclosure; or
(3) unauthorized disclosure to an employee of another licensee if no further disclosure.

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 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.~~

E~~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.

F~~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.

G~~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;~~
(c) Biometric data of the Consumer that would permit access to financial accounts of the Consumer;
(d) Any information of the Consumer that the licensee has a legal or contractual duty to protect from unauthorized access or public disclosure;
(e) The Consumer's date of birth;
(f) 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;
(g) 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;
(h) 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) 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;
(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.
(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.

Section 6 (Edits to selected subdivisions)

(A) If the licensee determines that a data breach has occurred, or is reasonably believed to have occurred, the licensee, or a third party acting on behalf of the licensee shall notify, without unreasonable delay:

Comment [DD2]: This content is not entirely new, but is a clarification of the exposure draft text.

(D)(4) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivisions (A)(1) and (D) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5; 42 U.S.C. 17932). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

Comment [DD3]: This Section 6(D)(4) is all new content.

(D)(5) If Federal or State statutes require a licensee to send notices duplicative of those required by Section 6(A)(1) and this section (D), the licensee may petition the Commissioner on a case-by-case basis for exemption from the notice requirements of Section 6(A)(1) and this section (D). Upon a showing of good cause by the licensee that notices submitted as an alternative to notice under this Act will both: (1) contain substantially similar information as that contained in notices required by this Act and, (2) be sent to all consumers required to be notified by this Act, the Commissioner may waive the notice requirements of Section 6(A)(1) and this section (D). However, nothing in this subdivision shall be construed to exempt a licensee from any other provision of this section.

Comment [DD4]: This Section 6(D)(5) is all new content.

Comments Ben Yardley (ME)

Just a couple of short edits, with underlining or ~~strikethrough,~~ to section 2:

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 under Pub.L. 106–102, 113 Stat. 1338, enacted November 12, 1999, or to Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996, and ~~such statutes, or~~ rules, regulations, procedures or guidelines established ~~there~~under either statute, 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 format maintained by that licensee.

   A licensee subject to and compliant with data breach notification requirements under Pub.L. 106–102, 113 Stat. 1338, enacted November 12, 1999, or to Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996, and ~~such statutes, or~~ rules, regulations, procedures or guidelines established ~~there~~under either statute, is deemed compliant with Section 6D, Notification to Consumers.

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 in this state nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

From: Texas Department of Insurance

Modified Harm Trigger Suggested Language

Remove the harm trigger from the definition of "data breach" by amending Section 3 as follows:

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~~.

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) good faith acquisition by an employee if not subject to further disclosure; or

(3) unauthorized disclosure to an employee of another licensee if no further disclosure.

Add the harm trigger to the notification paragraph in Section 6A:

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

(1) All consumers to whom the personal information relates, unless the licensee determines that no harm or inconvenience to the consumer is reasonably likely to result from the data breach; *

(2) ...

*The model could add a drafting note or include in the provision factors to be considered in the determination of harm or inconvenience: the nature and extent of the personal information involved, the unauthorized person who used the personal information or to whom the disclosure was made, whether the personal information was actually acquired or viewed, the extent to which the risk to the personal information has been mitigated, and other factors as appropriate. (These factors were taken from HIPAA privacy regulations.)

Provide for timely notice to the commissioner of the harm or inconvenience determination and that the commissioner can override this determination such that consumers must be notified by adding the following after the language in the current version of the draft in Section 6B:

The licensee shall within 15 business days of its initial notification to the commissioner notify the commissioner of any determination under Section 6A(1) that no harm or inconvenience to consumers is reasonably likely to result from the data breach and provide factors considered in reaching the determination. If the commissioner, in coordination with the commissioner of other affected states, if any, finds that such determination is not sufficiently supported by the known facts, the commissioner may require the notification of consumers under Section 6D.