Comments of the Center for Economic Justice and Peter Kochenburger

To the NAIC Cybersecurity Task Force Drafting Group

February 16, 2017

The Center for Economic Justice (CEJ) and Peter Kochenburger submit the following comments on Sections 5 through 13 of the second draft of the Insurance Data Security Model in preparation for the drafting group's February 21, 2017 call.

Section 5:

Section 5 requires a license to investigate a data breach or potential data breach. We believe using the taxonomy proposed previously – classifying events as either a "data breach" or a "data breach without use of personal information"[1] - significantly clarifies section 5B(3).

> Section 5. Investigation of a Data Breach
>
> 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 a data breach, a data breach without use of personal information or no loss of personal information has occurred~~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.

[1] "'Data Breach without Use of Personal Information" means a Data Breach for which the licensee has determined with a very high degree of certainty that the personal information acquired by the unauthorized person has not been used and has been returned or destroyed without further release or acquisition." CEJ comments submitted on January 23, 2017.

Section 6A

Section 6A also becomes clearer using our taxonomy of data breach versus data breach without use of personal information, As currently worded, Section 6A does not require a notification if the data breach involves[2]:

> 3H(2)(g) 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) 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) 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
>
> (j) 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.

As stated in prior comments, there should be one definition of personal information for purposes of data security and data breach notification. Any information deemed sufficiently important in Section 3 to require data protection should logically also trigger consumer notification under Section 6 in the event of a data breach. There is no purpose served or consumer benefit in separating these requirements. If an insurer learns through the application process (part i), sensitive information about the consumer's family status, health condition, hobbies, investments, criminal history, social media or web browsing activities, telematics information from vehicles, homes or wearable devices among countless other types of personal information, that information must not only be protected but trigger a data breach notice if that information is lost or stolen.

In 6A(1), we suggest replacing the vague phrase "to whom the personal information relates" with the clearer objective standard "whose personal information was acquired without authorization."

---

[2] "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 . . ."

In 6A(2), we suggest language tracking our taxonomy of data breach versus data breach without authorization, which would eliminate the need to use subjective phrases like information which "was or may have been compromised." In addition, the current draft's use of "compromised" introduces a previously unused (and undefined) term for data breach, injecting the potential for confusion. Our suggested language continues the use of consistent and objective phrasing.

In 6A(3), we have not offered any suggested edits, but note that the phrasing used – "The relevant Federal and state law enforcement agencies, as appropriate" – is ague. What makes a particular law enforcement agency relevant or appropriate for disclosure?

Section 6A(4) refers to a "payment card network," which should be defined in Section 3.

In section 6A(5), there is a "harm trigger" of 500 consumers before a licensee is required to notify a consumer reporting agency of a data breach. We object to this threshold requirement, which only serves to penalize consumers who happen to be part of a data breach involving 499 or fewer consumers – no matter how harmful the lost personal information may be to those consumers. Requiring notification of a data breach to a consumer reporting agency provides a critical consumer protection and its value is no less to a consumer in a data breach class of 499 than consumers "fortunate" enough to be in a data breach class of 500 or more. The "harm trigger" is completely unrelated to any measure of consumer harm.

In addition, there is no rationale for limiting notification to consumer reporting agencies based on alleged expense burden to licensees. The notification by the licensee will consist of a description of the data breach and the list of consumers whose personal information was lost or stolen. There is little or no difference in cost in preparing a description of a data breach with a list of affected consumers for a breach affecting 100 or 100,000 consumers.

Finally, regarding Section 6A(5), there are dozens of consumer reporting agencies,[3] some of which may not be relevant for data breach notification. For example, if the data breach involves health information, there would not seem to be a need to notify the consumer reporting agencies who manage property casualty all-claims databases like CLUE or A-Plus. The current phrasing simply refers to each consumer reporting agency. There should be some qualifier. We suggest the language below for purposes of discussion.

[3] The Consumer Financial Protection Bureau publishes a list of consumer reporting agencies. The 2016 list includes nearly 40 CRAs. http://files.consumerfinance.gov/f/201604_cfpb_list-of-consumer-reporting-companies.pdf

Section 6. Notification of a Data Breach

A. If following an investigation under Section 5, the licensee determines that a data breach~~n 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 whose personal information was acquired without authorization~~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 with residents whose personal information was part of the data breach~~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 in possession of the personal information acquired without authorization~~, if the data breach involves personal information relating to 500 or more consumers~~.

Section 6B

We suggest moving the last sentence about continuing obligation to the beginning of the section and cleaning up the introductory language of section 6B. We also suggest use of our taxonomy of data breach and data breach without use of personal information, including the addition of an item requiring the licensee to explain the determination that an incident was a data breach without use of personal information.

Hopefully, the remaining edits are transparent without further explanation. We will mention the edit to item 8 (item 7 before our edits) regarding types of information involved in the data breach. We strongly urge the addition guidance in our edit to ensure that the report to the commissioner set out the specific types of breached personal information and not simply broad categories. We will repeat this comment in the section setting out data breach notice requirements to 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 or a data breach without use of personal information has occurred, the licensee shall initially notify the commissioner that a data breach or data breach without use of personal information has occurred, including as much of the following information as available. . ~~The licensee shall provide as much of the following information as possible:~~ The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the commissioner concerning the data breach as additional information in this section is identified by the licensee.

(1) Date of the data breach or data breach without use of personal information;

(2) Description of ~~the data breach, including~~ how the information was exposed, ~~whether~~ lost, stolen, or breached, including the specific roles and responsibilities of third party service providers;

(3) How the data breach or data breach without use of personal information was discovered;

(4) If the licensee has determined the incident was a data breach without use of personal information, the basis for this determination.

(5) In the event of a data breach, w~~W~~hether any lost, stolen, or breached information has been recovered and if so, how this was done;

(6~~5~~) The identity of the source of the data breach;

(7~~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;

(8~~7~~) Description of the specific types of information ~~lost, stolen, or breached~~ acquired without authorization. Specific types of 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. ~~(equipment, paper, electronic, claims, applications, underwriting forms, medical records etc.);~~

(9~~8~~) Whether, if the information was encrypted, the specific encryption method used and whether the encryption, redaction or protection process or key was also acquired without authorization;

(10~~9~~) The period during which the information system was compromised by the data breach;

(11~~0~~) The number of total consumers and consumers of each state affected by the data breach; The licensee shall provide the best estimate in the initial report to the commissioner and states and update this estimate with each subsequent report to the commissioner pursuant to this section.

(12~~1~~) 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;

(13~~2~~) Identification of efforts being undertaken to remediate the situation which permitted the data breach to occur, including identification of employees or contractors who are investigating or remediating the data breach;

(14~~3~~) 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

(15~~4~~) 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.~~

Section 6C

It is unclear what Section 6C adds to the requirement to notify consumer reporting agencies in 6A(5). The proposed section provides no timeline for notification, only the vague "as expeditiously as possible and without unreasonable delay," which invites additional disputes over the timing. The section should set out a maximum time frame for such notification

We also oppose this section because it wrongly eliminates notification if certain sensitive personal information is part of the data breach, but the number affected consumers happen to be 499 or fewer consumers – no matter how egregious the data breach. We discussed these issues above.

This section might include guidance on which or what type of consumer reporting agencies must be notified in the event of a data breach.

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].