CENTER for ECONOMIC JUSTICE | FAIR ACCESS FAIR TREATMENT

Comments of the Center for Economic Justice
to the
NAIC Cybersecurity Task Force

Proposed "Insurance Data Security Model Act"

March 23, 2016

The Center for Economic Justice offers the following comments on the March 4, 2016 exposure draft of the "Insurance Data Security Model Act." ("Model Act").

The proposed Model Act has grave limitations on consumer rights and protections regarding licensees' collection and protection of consumer personal consumer information – limitations that fall far below the consumer protections provided in state or federal law for victims of theft of personal information. The impression we get from the Model Act is that the protection of insurers and jurisdiction of state insurance regulators is considered far more important than the protection of consumer personal information and licensee responsibilities to consumers in the event of a data breach.

Section 1: The Model Act states "The purpose and intent of this Act is to establish the exclusive standards for data security and investigation and notification of a breach of data security applicable to licensees in this state." However, the Model Act is clearly not limited to standards for licensees; it also specifies and limits the rights of consumers whose personal information is stolen or lost. It is unclear how the Model Act will work with other state laws regarding consumer rights for data breaches or why insurance consumers should have limited rights compared to other consumers in the event of loss or theft of their personal information. CEJ is concerned about the "exclusive" modifier in the purpose, particularly since many states' laws provide greater consumer protections. CEJ suggests the following changes:

"The purpose and intent of this Act is to establish the ~~exclusive~~ standards for data security and investigation and notification of a breach of data security applicable to licensees in this state, to the extent such standards do not already exist in and meet or exceed such standards in state or federal law."

Section 2: As noted in our comments on Section 1, there are existing state and federal laws setting out consumer rights in the event of theft or loss of personal consumer information by businesses which collect, use or maintain such personal information. Insurance consumers should have the same rights to notice, remediation and restitution as other consumers. ***Stated differently, the consumer rights in the Model Act should be the greater of consumer rights existing in state or federal law or the consumer rights set out in the Model Act.***

Section 3: The definition of data breach contains an exemption for stolen data that is "encrypted, redacted, or otherwise protected by another method that renders the information unreadable and unusable." The term "encrypted" is defined "rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security." This is a massive and unacceptable loophole. The definition of encrypted is immensely vague. What constitutes the "field of information security?" What does "generally acceptable" mean? This exemption could mean a password-protected spreadsheet containing sensitive personal information that is easily hacked to access that personal information. If there is going to be an exemption for "encrypted" data, then the exemption should be limited to data encrypted to specific standards which have been demonstrated to protect the data from access.

Section 3. The definition of personal information includes "non-truncated social security number." This definition would include a SSN truncated from 9 to 8 digits, the theft of which would continue to put the consumer at risk. The definition should be

"five or more consecutive digits of the consumer's ~~non-truncated~~ social security number."

Section 3: The definition of personal information contains an exclusion: "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." It is unclear if this exclusion applies to data obtained from data brokers, since insurers and other businesses are able to obtain and do obtain sensitive personal information from data brokers. The exemption is overly broad and vague and could easily be interpreted to include sensitive personal information obtained from such data brokers.

Section 3: The definition of "substantial harm" is woefully inadequate. Stolen personal consumer information can be used for stalking or otherwise inflicting physical or emotional harm on consumers. As noted below, there should be no "harm trigger" in the Model Act.

Section 4: The Model Act lists three objectives of the required information security system – security/confidentiality of personal information, protection against anticipated threats, and protection against unauthorized access. These objectives are insufficient. Additional objectives should include:

- Destruction of personal consumer information no longer needed for the provision of services by the licensee.
- Initial and routine disclosure of to consumers of personal consumer information collected and maintained by the licensee.

Section 4: The Model Act limits the "scale and scope of a licensee's information security program" to be "appropriate to" (1) The size and complexity of the licensee; (2) The nature and scope of the activities of the licensee; and (3) The sensitivity of the consumer information to be protected. It is unclear what this section means or how it would be implemented consistently across states and licensees. Does it mean that small licensees need not protect personal consumer information because the licensee's small size? We are extremely troubled by a limitation based on the nature and scope of the activities of the licensee. Why would the same personal consumer information be treated to different security standards or consumer rights in the event of a breach because two licensees use these personal data in different ways? Finally, how is "sensitivity" of consumer information evaluated? The Model Act has a definition of personal information; it follows that any of the information so defined is "sensitive." Consequently, it is unclear why or how an information security program of a licensee would or should vary based on "sensitivity" of the consumer information.

Section 4: CEJ supports sections A and D through H.

Section 5: This section requires the licensee to provide information to the consumer about the "types: of personal information collected and stored by a licensee. There is no definition of "stored" in the Model Act. This definition would seem to exclude, for example, personal consumer information obtained through and used for the underwriting process, but not maintained after the underwriting is completed. But, if that personal consumer information is stolen from the licensee during the period in which the data are used that data breach is clearly just as serious and harmful to a consumer as data theft of personal information maintained by the licensee. Further, providing "types" of information has not been shown to inform or empower consumers. Consumers should have the right to see the actual personal information collected by the licensee. This is particularly relevant given the consumer right in Section 5b to "review and correct their data if needed." A consumer cannot review and correct types of data collected; she can only review and correct actual data collected. We suggest the following changes to 5a.

> The licensee shall periodically, no less frequently than annually, offer ~~provide~~ consumers the opportunity to view or obtain a list of all the ~~with information regarding the types of~~ personal information collected ~~and stored~~ by the licensee or any third-party service providers it contracts with and whether that personal information is maintained by the licensee or third-party.

Section 7: The notification provisions in the event of a data breach are based on the licensee's determination that the theft or loss of the personal consumer information is reasonably likely to cause substantial harm or inconvenience. This section is problematic and anti-consumer in a number of ways.

First, it includes a harm "trigger." Several states have notification laws without harm triggers because consumers have the right to know if their personal information has been stolen so the consumers can take the steps need to protect themselves. It is totally inappropriate and unacceptable for a licensee to be determining whether to incur the cost of notification of data breach based on the licensee's evaluation of harm.

Second, the defined trigger of substantial harm is shockingly inadequate, as discussed above.

Third, the limitation on notifying consumer reporting agencies of the data breach to only those situations in which 1,000 or more consumers are affected is illogical and without justification. There is no rationale for a licensee not notifying a consumer reporting agency if personal information of 100 or 500 consumers are affected. The number of consumer reporting agencies is limited and likely fewer than the number of state and federal regulatory and law enforcement agencies to be notified.

Fourth, Section 7a identifies parties to be notified "without unreasonable delay" in the event the licensee determines a data breach has occurred (which will cause "substantial harm.") Section 7b sets out a specific time frame for such notification to insurance commissioners – 5 days – and such notification must include 15 types of information. The list of information to be submitted to the commissioner – within 5 days of identifying the data breach – is substantial, relevant and appropriate. But the short time frame for notifying the commissioner is wildly at odds with the time frames for other notifications in Section 7 as well as the "without unreasonable delay" provision in Section 7a. Section 7c not only inappropriately limits notification to consumer reporting agencies to instances involving 1,000 or more consumers, but allows up to 60 days for such notification. If the licensee has identified a data breach, there is no reason to allow 60 days to notify consumer reporting agencies. Even assuming that the initial work after the data breach will be to prepare the required information for notification to the commissioner, notification to consumer reporting agencies should be no longer than 15 days following identification of the breach.

Similarly, it is unclear why up to 60 days is permitted before notification to consumers. Significant consumer harm can occur within 60 days and significant consumer harm can be avoided with prompter notification. Given the detailed list of information to be included in the notification to the consumer, it is unclear why such notification needs to delayed 15 days by submission to the commissioner. This notification letter can and should be prepared prior to any data breach as part of the licensee's information security program with a few pieces of information to be filled in if a data breach occurs – the description of the data stolen and actions taken by the licensee.

Notification to affected consumers should be provided within no more than 15 days from the date of identification of the data breach and the submission to the commission 15 days prior to sending notification to consumers should be eliminated. The proposed consumer notification should be included in the list of information provided to the commissioner pursuant to 7b.

Section 8: We have commented previously that "identity theft" protection, generally, is a near worthless "consumer protection" and have provided studies documenting this. Further, "identity theft" protection is not defined and could include simply credit monitoring – already provided by most credit card issuers. Identity theft protection is woefully inadequate, but if it is to be provided, then such protection should be defined to include costs associated with responding to and remediating identity theft, such as legal and other fees, and not simply identity theft as credit monitoring.

But, identity theft protection, as demonstrated in our prior comments, does not materially help or protect consumers who are victims of data breaches or enable consumers to exercise pro-active measures to prevent identity theft or other harm from the theft of their personal information. We strongly recommend that consumer protection following a data breach include free security freeze and substantial identity theft protection for at least three (3) years following the notification to the consumer of the data breach. The current language simply states 12 months of protection and does not specify when that period starts.

Section 15. This section unreasonably and without justification limits private rights of action against licensees who fail to comply with the provisions of the Model Act. In particular, Section 15D inexplicably precludes any "remedy or recovery available to consumers, in law or equity, for occurrences constituting a violation of any provision of this Act." By what logic should a licensee be immune from a consumers' private cause of action if that consumer's personal information was collected by the licensee – likely without the knowledge or consent of the consumer – and which personal information was lost or stolen due to lax and irresponsible practices of the insurer?