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"

October 25, 2016

The Center for Economic Justice submits additional comments to the Task Force in response to industry comments on the revised draft Insurance Data Security Model Act. We submit these comments because the development and adoption of the model law is vitally important to insurance consumers and because the industry appears to be unified in their demands for little or no accountability to consumers for their collection, protection and loss of personal consumer information. The revised draft does balance the interests and protection of industry and consumers with regard to insurers' use and protection of personal consumer information. We and other consumer organizations will strongly oppose changes to the proposed model which skew that balance towards industry interests and will hold regulators accountable for favoring industry over consumers if such changes occur.

It has been evident for some time – and vividly on display at the Cybersecurity Task Force interim meeting earlier this year – that industry demands for "uniformity" are directed at establishing a low ceiling for consumer protection while encouraging regulators to use discretion for establishing data security practices among different industry participants. The industry demands for limiting disclosure of data breaches to consumers with "harm triggers" and no private cause of action would amount to insurers collecting and using personal consumer information without any accountability to consumers in the event of a loss of this information. The industry proposals are wildly unbalanced and we urge the Task Force to continue with a balanced approach.

We make the observation that the proposed cybersecurity model law involves both financial regulation – requirements for data security procedures and oversight of such procedures – and market regulation – treatment of consumers in the event of a data breach. Financial regulation has long had greater uniformity across states than insurance market regulation and for good reason. Financial regulation is premised on a lead state having responsibility for oversight of the financial condition of an insurer to avoid duplication of financial oversight activities by many states. In the case of cybersecurity, it makes sense for the lead financial oversight state to establish and monitor the data security policies and practices of an insurer instead of multiple states performing the same examination. On the other hand, market regulation has always had more diversity because states vary in the market performance requirements of insurers to reflect the various market differences among states. There is no lead state or domestic deference for market regulation for good reason – the market regulation issues vary across states.

It is vital to recognize that the proposed cybersecurity model law includes both financial and market regulation activities when the Task Force considers the role and extent of "uniformity." When it comes to the financial regulation aspect of the model law – requirements for data security policies and practices – uniformity is important and necessary. But when it comes to market regulation issues, like notification to and assistance for consumers in the event of a data breach, it is reasonable and necessary for individual states to respond to the issues facing their consumers. The personal information collected, obtained, used and/or maintained by insurers and agents can vary considerably across states because of fundamentally different approaches to structures for certain lines of insurance or state-specific prohibitions or permission to use certain types of personal consumer information. Consequently, the consumer protection aspects of the proposed cybersecurity model must be a floor with the ability of states to require greater consumer protections as the situations in those states dictate.

We strongly support the removal of the "harm trigger." As Commissioner Hamm has noted in numerous speeches, the nature of consumer harm from the theft of personal consumer information will vary by the nature of the lost information. The potential harm to a consumer form such information theft will vary due to the circumstances of the consumer and the nature of the lost data. It is inappropriate – inconceivably inappropriate – for an insurer or agent to decide what type of lost data might or might not cause consumer harm and, as a result, withhold notification to a consumer. The consumer is clearly in the best position to determine what harm he or she might suffer as a result of the specific lost personal information and to take the steps necessary to protect him or herself. But such action by the consumer requires knowledge by the consumer of the data breach and the content of the breach. Removing the so-called "harm trigger" – which is more appropriately described as insured-defined consumer accountability – is an essential consumer protection made even more important in the absence of a private cause of action.

Section 2: We continue to believe a private cause of action is appropriate for the consumer protection aspects of the model law. The current draft provides for notification to consumers in the event of a data breach – to empower the consumer to take the action necessary to protect him or herself. If an insurer fails to provide such notification in the absence of a private cause of action, a consumer who may have suffered grievous injury as a result of the insurer's or agent's failure to provide such notification is without recourse.

We recognize that the proposed draft is attempting to balance industry and consumer interests by removing the harm trigger for purposes of consumer notification coupled with limiting consumer access to courts in the event of insurer or agent failures to carry out their responsibilities. However, we suggest that prohibiting the private right of action should be limited to Sections 4, 5 and 6A, B, C and E of the model – the financial regulation sections – while permitting a private cause of action for activities required in Sections 6D and 7 – the consumer protection sections.

We fully support the provision in Section 2 that establishes the consumer protection provisions of the model as a floor, as discussed above. We would add that the world of cyberthreats and cybersecurity is changing rapidly. It would be illogical to prohibit a state from employing state-of-the-art consumer protections which provide greater protections than those included or currently imagined in the draft model.

Section 3C: the definition of a data breach excludes the loss of personal information if it is encrypted and the "encryption, process or key is not also acquired, released or used without authorization." Section 3D defines "Encrypted" as "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." Individually and combined, these definitions are vague and create a potentially large loophole. For example, how can a licensee know with authority that the encryption key has not been acquired or use? What does it mean to have a "low probability" of accessing encrypted data without the key?

We suggest that, as written, there is great potential for both lack of uniformity across the states and failure to identify data breaches due to encryption. On the first issue – uniformity across state financial regulators – Section 12 is reasonable and absolutely necessary. There are several aspects of the model – like Sections 3C and 3D – which are vague and/or open to significant differences in interpretation. As financial regulators work with licensees, best practices will emerge and those best practices can be memorialized in a model regulation.

Section 3H: We generally support the definition of Personal Information and urge the Task Force to reject industry calls to dramatically limit this definition. A broad definition of personal information is reasonable and necessary for both the financial regulation and consumer protection aspects of the model. In terms of consumer protection, the model has three basic

components – identification of a data breach, notification to the consumer of a data breach and assistance to the consumer in the event of a data breach. The proposed definition of Personal Information is appropriate because it limits this information to that not publicly available. Consequently, the scope of the model and required consumer protections apply appropriately to personal consumer information that is not publicly available.

Section 3I: It is essential that a licensee be responsible for the data security and consumer protection requirements of the model even if the licensee utilizes a third party service provider and that provider suffers a data breach of the personal information provided by or obtained on behalf of the licensee. While we do not object to industry requests to clarify that licensees covered by the law should not be considered third party service providers, we urge great caution in crafting this clarification to avoid creating a loophole or incentive for use of third-party providers by licensees to avoid responsibility.

Section 4A: We note that the section provides great latitude to regulators – "Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities and the sensitivity of the personal information in the licensee's possession, custody or control . . .." We also note that industry has not complained about the lack of uniformity that is likely to result from this section. We suggest that this provision requires further development through a model regulation – which is why section 12 of the model is reasonable and necessary. We would also note that there is zero accountability to the public of the regulator's action or decisions regarding Section 4A. Again, the development of a model regulation to establish objective criteria for implementing 4A would provide greater public accountability as well as promote greater uniformity.

Section 4: We strongly support the provisions in Section 4

Section 6C: This section requires notification of a data breach to a consumer reporting agency only if the breach affects 500 or more consumers. The section recognizes that notification by the licensee to consumer reporting agencies in the event of a data breach (of information maintained by the consumer reporting agency) is an important consumer protection. Consequently, it is unclear why there is a threshold for such reporting. What is the rationale for requiring such reporting if 525 consumers are affected, but not 475? Or even one consumer?

Presumably, the argument for including a threshold is to limit licensee expenses in the event of a data breach. We suggest that the cost of notifying a consumer reporting agency is minimal and does not vary significantly with the number of affected consumers. The notification will likely consist of a cover letter and a list of affected consumers – with such list generated by a report request of the licensee's data system. We submit that no evidence or logical argument has been provided to support any threshold for Section 6C.

Section 6D: We continue to question why Section 6D1 allows a licensee up to 60 days after the breach has occurred to notify consumers. Presumably, "occur" means the date the licensee discovered and confirmed the breach, since the actual breach could have occurred many months before discovery. Given that understanding, 30 days is a more reasonable time limit for consumer notification.

We strongly support the requirement in Section 6D2 for submitting the proposed notice to the Commissioner prior to sending the notice to consumers. Despite industry claims, this provision is not a hardship and need not delay such notification to consumers. The format of the notice and the majority of the text can be prepared as a template prior to any data breach. But the notice to consumers must have some breach-specific information – the date of the breach and the specific data types lost. It is this last item – a description of the specific data types lost – which requires regulatory review to ensure that the licensee is clearly and accurately describing the lost personal consumer information.

We suggest that the term "straightforward language" in 6D2 is both undefined and unclear. If the goal is to ensure that the consumer notification will be understood by and empower consumers, then the section should add a provision that the Commissioner shall establish a notification review group comprised of consumers, consumer representative and experts in consumer disclosures to assist the Commissioner in the review and offer advice regarding the effectiveness of the notification.

Section 7: We support the revisions to Section 7. As noted above, consumer protection needs in this area may vary because of differences in data lost across states and/or types of consumers affected. We would note that insurance regulators have a track record of working together for uniform approaches in the event of data breaches. Given this track record, we reject industry hyperventilation that allowing a Commissioner to address the specific needs of his or her affected consumers will lead to unreasonable outcomes. We also note that the flexibility in Section 7 matches the flexibility praised by insurers in Section 4A.

Section 12: As discussed above, Section 12 is essential. There is little doubt that best practices will emerge for both the financial regulation and consumer protection aspects of the cybersecurity model. These best practices – particularly in those areas for which flexibility is provided to the Commissioner – should be memorialized as quickly as possible to promote uniformity to the highest levels of license and consumer protection. The best tool for such improvements and clarifications is through a model regulation.