CENTER for ECONOMIC JUSTICE | FAIR ACCESS FAIR TREATMENT

Comments of the Center for Economic Justice

To the NAIC Cybersecurity Working Group

On Version 4 of the Insurance Data Security Model Law

May 8, 2017

CEJ submits the following comments on version 4 of the proposed Insurance Data Security Model Law.

General Comments

The latest version of the model law has rewarded insurers and producers for their refusal to agree to, or compromise on essential personal consumer data protections, accountability or data breach obligations by eliminating anything industry has opposed. The current model has literally nothing for the consumers whose personal data insurers are mining, using, storing and selling. The current model provides zero accountability of licensees to consumers for data security or of insurance regulators to consumers for enforcement of the data security requirements. The current model provides no penalties for bad outcomes for consumers and is generally an exercise in Licensee self-regulation. The model borrows from the New York Cybersecurity Regulation, but omits that regulation's reliance on strong consumer data breach notification requirements in other New York law and creates harm triggers not found in the New York version.

Even assuming that consumer data protection and data breach notification and response issues will be addressed in a subsequent, companion model, version 4 requires, at a minimum, additions to create accountability to consumers of licensee data security practices and outcomes and for regulators' oversight and enforcement of licensee requirements. Towards this end, a section or sections are needed for independent assessment and publication of licensees' compliance with data security procedures. This information is essential to enable consumers to consider a licensee's data security procedures and competence when selecting a licensee with whom to do business.

Independent Assessment of Licensee Compliance and Data Security Program Effectiveness

Regulators and insurers urge consumers to select insurance providers based on their financial strength and consumer outcome performance in addition to shopping based on price. But, we are in an era where insurers mine, use and maintain vast amounts of consumers' personal information in the sale and administration of insurance products. Surely, one area for innovation – as well as fundamental accountability to consumers – is to develop a public grading system for licensees' protection of consumers' personal information to allow consumers to incorporate personal data protection into the decision to purchase from and do business with a licensee.

One likely response to this recommendation from insurers is that regulators will enforce the requirements of the model law and consumers are protected by that enforcement. There are several fatal problems with this rationale. First, the proposed model is largely a self-regulatory model with broad and vague requirements. For example, section 4A – Implementation of an Information Security Program

> Commensurate with the size and complexity of the Licensee, the nature and scope of the Licensee's activities and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody or control, each Licensee shall develop, implement, and maintain a comprehensive risk-focused written Information Security Program that contains administrative, technical, and physical safeguards for the protection of Nonpublic Information. The Licensee shall document, on an annual basis, compliance with its Information Security Program. The Licensee shall make this documentation available to the Commissioner upon request

Per this foundational provision of the model, the licensee determines what its risk is, designs a program based on its evaluation of its risk and evaluates itself on its performance in complying with a program it designed for a risk it assessed.

Second, the model includes procedural requirements only, presumably based on the belief that good policies and procedures will produce good (or better) outcomes, but no provisions based on actual data security program results. While such an approach is necessary for financial regulation since there are too few bad outcomes (financial failures) to create a statistically-valid methodology for correlating certain policies and procedures with certain outcomes, that is not the case with data security program. Problems with data security programs – small and large, data breaches and data security program failures not resulting in a breach – are numerous enough to measure the outcomes of data security programs. Stated differently, the model should require reporting and publication of data security program successes and failures and include monitoring and assessment of outcomes to inform and improve policies and procedures.

Third, in addition to the model creating no accountability to consumers from licensees, the model also contains no accountability to consumers from regulators charged with enforcing the vague provisions of the model. There are no provisions in the model – except for the

optional (!) rulemaking provision – to generate more specific regulatory practices for consistency across states. Not only is there no mechanism for regulators to agree upon the size and complexity of a Licensee or the nature and scope of a Licensee's activities or the sensitivity of the Licensee's Nonpublic Information or what the risk-focus of a Licensee should be, there is no accountability to consumers of regulators' performance. Consumer concern with uneven enforcement across the states is justified by uneven use of state-prescribed accounting practices and many states' commitment to insurance as an economic development strategy for their state.

Based on this analysis, we urge the working group to add provisions to the model allowing for independent assessment and publication of Licensees' performance meeting the data security requirements of the model. The independent assessment would grade the Licensee as not-meeting-requirements, meeting-requirements or exceeding-requirements for each of the requirements in Sections 4, 5 and 6 with the addition of a requirement to report the number and type of data breaches/data losses and the number of consumers affected. To ensure a consistent evaluation across states and to ensure the accountability of regulators to consumers, the assessment should be performed by an independent panel of cybersecurity experts.

Bias Against Consumers

In our comments on version 3 and in my colleague Peter Kochenburger's comments on version 4 of the model, we have identified a number of items in which regulators acquiesced to industry demands, creating a model biased towards Licensee interests over consumer interests. We discuss one more example here.

The definition of Cybersecurity Event excludes what we will call a "Non-Event" – a data loss by the Licensee for which the Licensee has determined that the Nonpublic Information released to an unauthorized person has not be used and has been returned or destroyed with further release. The new draft conspicuously omits the modifier "with a very high degree of certainty" for the Licensee's determination because industry opposed such a "vague" standard. Yet, the same vague standard remains with the definition of Encrypted – a low probability of assigning meaning with the key – because this vague standard was agreeable to industry.

Further, the requirement that all Cybersecurity Events be reported to the Commissioner – including those determined to by the Licensee to be "Non-Events" has been changed to eliminate reporting of the "Non-Events." The model also eliminates any requirement for the Licensee to document or justify its determination that the Cybersecurity Event was a "Non-Event." What was a limited exclusion for data breach notification when the Licensee could demonstrate with a high degree of certainty that the data loss did not result in consumer harm, has been transformed into a major loophole with no Licensee accountability to consumers or regulators.