CENTER for ECONOMIC JUSTICE | FAIR ACCESS FAIR TREATMENT

Comments of the Center for Economic Justice

to the NAIC Cybersecurity Task Force Drafting Group

January 23, 2017

The Center for Economic Justice (CEJ) submits the following, reflecting comments made and issues discussed during the past few drafting group calls.

Data Breaches without Consumer Harm

In an earlier call, industry raised the concern of having to notify consumers in the event of data breaches/data losses for which no consumer harm can or would occur. In response to the examples raised by industry – consumer data was sent by the licensee to the wrong organization, but was recovered before the data was used or further distributed – CEJ suggested that this was an issue of whether a data breach had occurred as opposed to an issue of evaluating consumer harm.

We restate our position that consumers are in the best position to determine if lost or stolen data may endanger them. We strongly oppose a harm trigger, which leaves it up to insurers to determine if the damage from a data breach rises to the level of potential consumer harm. Consumer notification is the only way for consumers to learn about loss or theft of personal information which may endanger them. Insurers can never be in a position to evaluate the potential harm to a consumer of the loss or theft of that consumer's personal information. Just as having accounting and auditing procedures, processes and structures in place to ensure consumer premiums and payments are protected, so are data security and data breach notification policies and procedures essential in an era of insurers' collection and use of digitized personal information.

In an effort to address insurers' concern about data loss or theft for which there is no consumer harm, CEJ has proposed the following to ACLI, AHIP and IIABA for their consideration. The proposed language exempts from the definition of data breach (and related requirements for consumer notification), events in which the insurer can determine and demonstrate that the lost data has not been used and has not been further distributed.

C. “Data breach” means the acquisition of unencrypted personal information by an unauthorized person.

“Acquisition” does not include a data breach for which the licensee has determined with a very high degree of certainty that the personal information released to an unauthorized person has not been used and has been returned or destroyed without, further release.

The term “data breach” does not include "Data Breach without Use of Personal Information."

D. 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 that the personal information acquired by the unauthorized person has not been used and has been returned or destroyed without, further release or acquisition.
Inserted elsewhere in the model:

[An insurer must report all incidents of Data Breach without Use of Personal Information to the Commissioner with documentation of the investigation and determination that the incident was a Data Breach without Use of Personal Information]

[Data Breach notice requirements do not apply to incidents of Data Breach without Use of Personal Information.]

Third Party Service Providers

CEJ has the following comments and suggestions on the proposed edits regarding third-party service providers.

We support the following edit:

“Third-party service provider” means a person or entity, not otherwise defined as a licensee, that contracts with a licensee to maintain, process, store or otherwise have access to personal information used by the licensee or under the licensee’s possession, custody or control.

We oppose the changes to Section 4F which appear to remove licensee responsibility for third party data breaches. We have concern that the proposed language provides an incentive for a licensee to serve as a conduit for personal information from the consumer to the third party with the third party having possession custody or control instead of the licensee, but with the third party providing licensee access to the personal information as needed. For example, a licensee could collect personal information and pass to the third party, then access the information as needed for rating or claims or marketing without the licensee ever taking possession, custody or control.

In addition, the proposed changes change the requirements for a licensee utilizing a third party service provider from responsibility for outcomes to simply responsibility for pre-outcome procedures. We believe it is essential for licensees to be responsible for data breach outcomes – not only to ensure some entity is responsible to consumers, but to create the appropriate incentives for licensees to seek the best outcomes for consumers.

The edits to section 6F2 creates a requirement for a third party service provider, but the commissioner has no authority over such an entity --

There are two uses of the term "third-party." One is the use of a third party for dealing with data breach aftermath and the other is third party service provider's role in using or storing personal information. We find it confusing to use the same term "third party: for both. Further, it is unclear why "third party" needs to be included in all the data breach aftermath activities 5A, B, C and D as it seems obvious that a licensee can either investigate a breach itself or use a third party to investigate the breach as long as the investigation meets required standards. Stated differently, it is unclear why there is a concern about a licensee using a third party to fulfill the licensee's obligations in this section, since the licensee remains responsible whether the licensee performs these required tasks itself or through the use of a vendor.

Safe Harbors for Other State or Federal Requirements

Proposed new section 2B states the model is not intended to require a data breach notice when otherwise required and is not intended to establish a separate information security program. This proposed language is problematic for several reasons. First, it invites a lack of uniformity across licensees, with some licensees meeting the requirements of the model and others not. Second, the language incentivizes licensees to promote lowest-common-denominator alternative statutory requirements for information security and data breach notification. Third, there is no requirement that the "safe harbor" alternative to the insurance data security model requirements actually meet the standards of the insurance data security model.

The best way to achieve uniformity and consumer protection is to advance a model with strong consumer protections. Then, the licensee, in meeting the requirements of the insurance data security statute, will also meet the requirements of other state and federal data security statutes – while promoting uniformity across states for insurance licensees.

Private Cause of Action

We oppose the numerous changes that significantly weaken consumer protections. The proposal to add a harm trigger without a private cause of action and without disclosure requirements by the insurer or Commissioner of data breaches not meeting the harm trigger makes insurers and regulators unaccountable to consumers. We repeat our recommendation that the model create a private cause of action for violations of the consumer protection / data breach notification sections of the model.

Definition of Data Breach

We support a broad definition of data breach, without harm triggers, as discussed above.

"Data breach" means the acquisition of unencrypted personal information by an unauthorized person.

There should also be a definition of encryption, encrypted or unencrypted to ensure that the encryption is meaningful consumer protection. The current definition is weak because "low probability" is not defined and because it fails to account for theft of the encryption key.

The additional sections refer to "good faith" acquisition or belief. We oppose these sections because "good faith" is vague and unaccountable to consumers. We suggest an approach as discussed above in which the licensee can determine and demonstrate with a very high degree of certainty that the lost data has not been used and has not been further distributed.

Definition of Personal Information

We support a broad definition of personal information and oppose efforts to reduce consumer protection by virtue of unreasonable limits on the definition of personal information.

Section H2a defines personal information to exclude a consumer's name and "non-truncated social security number." This provision should be modified to "any three or more consecutive digits from a social security number. It is common for organizations to utilize the last four digits of a social security number as a means for identifying consumers. Consequently, the loss of a consumer's name and last four digits of a SSN could result in significant consumer harm.