CENTER for ECONOMIC JUSTICE | FAIR ACCESS FAIR TREATMENT

Comments of the Center for Economic Justice

to the NAIC Cybersecurity Task Force Drafting Group

February 6, 2017

The Center for Economic Justice (CEJ) has previously submitted comments to the drafting group. These comments reflect issues discussed during the January 24, 2017 drafting group call.

ACLI Recommendation: Create two categories of personal consumer information – one category for purposed of data protection and security and another for purposes of data breach notification.

CEJ opposes this recommendation. The premise behind the ACLI recommendation is that the category of data requiring data protection is broader than the category of data requiring notice to a consumer if the data are lost or stolen. We disagree. The purpose of data security requirements to protect data is to avoid the dissemination of consumers' sensitive personal information. Consequently, it is reasonable and necessary that the personal consumer information requiring data security protection is the same personal consumer information for a notice to a consumer in the event of a data breach.

In addition, the creation of two categories of personal consumer information – one for data security and one for data breach notices – is inherently arbitrary and will require some pre-determined harm trigger. For reasons already discussed in prior comments and below, we oppose any harm trigger. Further, the creation of two categories of personal consumer information will make the model unnecessarily complex and create more opportunities for variations among the states.

If uniformity across states is a goal – and we believe it should be – the model should contain a broad definition of personal consumer information with no harm trigger for data breach notices to consumers. As the definition of personal consumer information gets whittled down and/or harm triggers are introduced, the likelihood for individual states' to tweak the definitions grows rapidly. In contrast, a broad definition of personal consumer information without a harm trigger is a clear concept and definition which is less susceptible to individual state modifications.

Third Party Service Providers

Our January 23, 2017 comments discussed a number of issues related to the third-party service provider provisions of the model, including our concern over the proposed deletion of a number of provisions regarding licensees' responsibility for data breaches of the licensees' personal consumer information at the third party service provider. We offer an additional comment about regarding the assertion by the producers' trades and others that agents have limited or no ability to require their contracts with third party service providers adhere to the requirements of the proposed model.

The argument put forth by producers' trades is that agencies are small businesses who cannot dictate terms to third-party service provider giants like Google and Microsoft. (We assume that Google and Microsoft are offered as example of cloud services used by agencies.) Consequently, the producers' trades argue that licenses should have limited or no responsibility for the personal consumer information maintained by these third party service providers – a position reflected in the current proposed edits to the third party service provider sections of the model.

CEJ believes the producers' trades arguments are flawed in at least two significant ways. First, by including licensee responsibilities for third party service providers data security practices and data breach incidents, the model law changes the competitive dynamic between licensees and third party service providers. Instead of a small agency trying to convince a cloud services behemoth to change the standard contract, now it would be thousands of insurers and tens of thousands of agencies all requesting similar contractual features related data security and data breach response. The model law would create a market in which the entire insurance industry requires certain third party service contract features – features required by the insurance industry's regulators and which are not subject to negotiation.

Second, and equally important, is that while some insurers and agencies will certainly contract with very large companies for various third party services that involve personal consumer information, the vast majority of third party service providers and of third party service contracts utilized by insurance licensees will not be with Google or Microsoft, but with much smaller vendors, including a variety of insurance-specific vendors for marketing, underwriting, pricing and claim settlement services. The cybersecurity model should not be drafted to address the alleged exception which would create a loophole for licensee responsibility for third party service providers.

ALTA Comments – Harm Trigger

ALTA repeats the common industry refrain calling for a harm trigger to avoid consumers "receiving unnecessary and confusing notices for minor breaches." ALTA then repeats the canard about too many notices:

> The goal of the notification provision should be to ensure consumers get meaningful information to help them determine how to best protect themselves after a breach. Our worry is that consumers will become desensitized if they are inundated with notifications for incidental breaches where there is no reasonable likelihood of use of the data.

ALTA and industry are muddling several issues in their effort to gain a harm trigger. The purpose and result of a harm trigger is to eliminate notices to consumers for certain types of data breaches – breaches for which the insurer determines that the lost or stolen information is unlikely to result in consumer harm. As we have stated numerous times, the consumer is the entity in the best position to determine whether certain personal information poses actual or potential harm and that a data breach notice is the only mechanism to alert the consumer to this actual or potential harm and thereby empower the consumer to take necessary actions.

The result of a harm trigger will be that certain consumers suffering loss of personal consumer information by the licensee will not be alerted to this – based on either an insurers' arbitrary determination of what constitutes harm or because the consumer was unlucky enough to be part of a data breach affecting a total number of consumers below the arbitrary threshold. Clearly, the impact a harm trigger is profoundly anti-consumer.

The alleged harms of too many notices or conflicting notices claimed by ALTA and industry are not related to or addressed by a harm trigger, since both can occur with a harm trigger. We reject the assertion of "too many notices" and "desensitized because of data breach notice inundation," These claims are unsupported and without empirical basis. How many notices are too many, according to industry? More important, the issue of consumers responding to or ignoring notices is a function of the structure, format and presentation of the notice, not whether a consumer receives one, two or three notices. Further, where will this alleged avalanche of data breach notices be coming from? The fact is that the likelihood of situations in which multiple notices and/or conflicting notices are sent are those instances in which any harm trigger would be met because of large data breaches involving many, many consumers and multiple data breach parties.

Similarly, the solution to the alleged problem of conflicting notices is not a harm trigger. A harm trigger does not eliminate conflicting notices for events meeting the harm trigger threshold, but simply eliminates notices entirely for events not reaching the harm trigger.

ALTA Comments – Who Owns the Data?

During the January 24, 2017 call, ALTA argued, in their written comment that the lender providing the personal consumer information to the title agent might be considered a third party service provider of the title agent or title insurer and such an outcome would presumably be a problem.

CEJ does not see the problem suggested by ALTA. The model sets out responsibilities for licensees – title insurers and title agents – who collect, maintain or use personal consumer information to ensure that the licensee is protecting this personal consumer information and takes certain actions of these data are lost or stolen. Regardless of the source of the personal consumer information used by title insurers and title agents, it is unclear why a lender providing the title insurer or title agent with personal consumer information would be considered a third party service provider to the lender, since the title insurer and title agent are service providers to the lender.