Comments to Section 2, 4.F, 5, & 6
Peter Kochenburger, NAIC Consumer Representative

Section 2.G: at the end of the sentence add "….laws of this state, including licensed insurance producers."

Intent: While the current definition of licensee includes licensed producers – agents and brokers – adding this clause makes it explicit.

Section 4.F.(2): new sentence: "The licensee shall also confirm and document that the third-party service providers will comply with all relevant provisions of this Act, including all rights provided to affected consumers. The licensee shall be responsible for any failure by such third-party service providers to so comply."

Intent: I agree with Birny's comments filed on behalf of CEJ. This provision is both necessary and appropriate and reflects an appropriate shifting of risk of non-compliance from the policyholder/consumer, to the insurer, if the third-party service provider violates this Act. The insurer selects the third-party service providers, can monitor compliance with the Act both before and after a data breach, can set out appropriate indemnification language with the third-party service provider in the event of a breach, and price and shift the financial risks of non-compliance through appropriate indemnification language with the third-party service provider, or through its general pricing structure. In contrast, the consumer plays no role in selecting the third-party providers, cannot monitor or influence compliance with the Act, is not a party to any indemnification agreements, and cannot shift the risk.

The previous language that was struck out is fine; I offer the alternative language above simply to strengthen a licensee's argument that the third-party service provider bears primary responsibility for compliance.

Section 5: The use of "third-party service providers" to describe independent entities that are retained after a data breach is confusing, since a similar term is used to described licensee (pre-breach) vendors. There are a number of ways to fix this and several suggestions have already been made. The easiest method is probably creating a new definition for entities hired to address and remedy the breach, and then substitute that term throughout. One example of a definition: "an independent entity designed by the licensee to act on its behalf for purposes of the investigation of a data breach and other responsibilities under this Act."

Section 6.E: new clause in second sentence: "In the event that the third-party service provider agrees to send the notices, licensee will confirm and document that this was completed <u>as required in this Act, and if not, the licensee will be responsible for necessary additions or corrections to the notices."</u>

Intent: Director Dwyer noted that this section needed to be tightened up to make it clear that notices sent by third-party service providers must comply with all relevant provisions of this law.