Cybersecurity & Data Breach

We appreciate the NCSL's efforts to confront the omnipresent cybersecurity threat. We want to stress our desire to work with legislators on the ever advancing cybersecurity danger which is targeted against public and private entities alike.

Stakeholders should be working together in a collaborative way to prevent and defend against cyber assaults. The cyber attacks are designed to obtain confidential company informational as well as sensitive personal information. If an attack surmounts the defenses of a government organization or company, we should have a uniform system of informing the public and tools for them to protect themselves and limit the negative effects of their exposure.

Cybersecurity is a serious concern for ACLI member companies. They are working diligently and expeditiously to protect their systems against these vicious illegal cyber attacks. ACLI member companies are and will continue to protect the sensitive consumer and company information in their possession and want to partner with regulators and law enforcement professionals to protect our businesses and our customers.

The NCSL is uniquely positioned to rationalize the universe of random and uncoordinated state requirements and create a uniform environment for the insurance industry and the millions of consumers they serve. Currently we have 47 different state breach notification laws. Uniformity in this complicated, frequently changing cyber environment is in the best interest of all involved when a cyber-breach occurs.

It is safe to presume that the cyber climate is guaranteed to evolve in the coming years. The ACLI has developed a preliminary draft of a single comprehensive cybersecurity model that incorporates both front-end protection of data requirements and back-end breach notification standards. We believe that the NCSL should consider our state-directed proposal as you move forward in examining this issue.