

FOR IMMEDIATE RELEASE:

Contact: James Hallinan

July 7, 2015

(505) 660-226

Attorney General Balderas Urges Congress to Preserve Authority to Enforce State Data Breach and Data Security

New Mexico Joins Multistate Letter against Federal Preemption of States' Ability to Legislate and Enforce Laws that Protect Consumers from Data Breaches and Identity Theft

Las Cruces, NM – Joining a bipartisan effort to ensure that New Mexico keeps its authority to enforce and enact data breach and data security laws, New Mexico Attorney General Hector Balderas today signed onto a letter to the U.S. Congress that emphasized maintaining states' rights and rejecting any efforts to allow federal preemption of state legislation.

Citing recent efforts in Congress to pass a national law on data breach notification and data security, Attorney General Balderas, joined by 46 other attorneys general, cautions against federal preemption of state data breach and security law and argues that any federal law must not diminish the important role states already play in protecting consumers from data breaches and identity theft, especially in states like Massachusetts whose laws provide greater protections than federal counterparts.

“Consumers' personal information and business data are constantly at risk of being hacked. It is crucial that we are able to aggressively protect New Mexicans, both through the preemptive enactment of laws and through enforcement,” said **Attorney General Balderas**. “Data breaches and identity theft devastate working families in New Mexico and threaten our economy; we must have all the necessary tools at our disposal to protect New Mexicans.”

“Preempting state law would make consumers less protected than they are right now,” **reads the letter signed by 47 state and territorial attorneys general**. “Our constituents are continually asking for greater protection. If states are limited by federal legislation, we will be unable to respond to their concerns.”

The letter points out a number of concerns with federal preemption of state data breach and security laws, including:

- **Data breaches and identity theft continue to cause significant harm to consumers.** Since 2005, nearly 5,000 data breaches have compromised more than 815 million records containing sensitive information about consumers – primarily financial account information, Social Security numbers or medical information. Full-blown identity theft involving the use of a Social Security number can cost a consumer \$5,100 on average.

- **Data security vulnerabilities are too common.** States frequently encounter circumstances where data breach incidents result from the failure by data collectors to reasonably protect the sensitive data entrusted to them by consumers, putting consumers' personal information at unnecessary risk. Many of these breaches could have been prevented if the data collector had taken reasonable steps to secure consumers' data.
- **States play an important role responding to data breaches and identity theft.** The States have been at the frontlines in helping consumers deal with the repercussions of a data breach, providing important assistance to consumers who have been impacted by data breaches or who suffer identity theft or fraud as a result, and investigating the causes of data breaches to determine whether the data collector experiencing the breach had reasonable data security in place. Forty-seven states now have laws requiring data collectors to notify consumers when their personal information has been compromised by a data breach, and a number of states have also passed laws requiring companies to adopt reasonable data security practices.

The letter urges Congress to preserve existing protections under state law, ensure that states can continue to enforce breach notification requirements under their own state laws and enact new laws to respond to new data security threats, and to not hinder states that are helping their residents by preempting state data breach and security laws.

In 2005, 44 state attorneys general wrote a similar letter to Congress calling for a national law on breach notification that did not preempt state enforcement or state law.

Today's letter, co-sponsored by Arkansas, Connecticut, Illinois, Indiana, Maryland, Massachusetts and Nebraska, was also joined by the following states and territories: Alabama, Alaska, Arizona, California, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Iowa, Kansas, Kentucky, Louisiana, Maine, Michigan, Minnesota, Mississippi, Missouri, Montana, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, North Mariana Islands, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Utah, Vermont, Virginia, Washington, and West Virginia.

Click here for copy of the letter delivered to Congress

- <http://www.naag.org/assets/redesign/files/sign-on-letter/Final%20NAAG%20Data%20Breach%20Notification%20Letter.pdf>.

###