

GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE ATTORNEY GENERAL
oag.dc.gov



FOR IMMEDIATE RELEASE: Tuesday, July 7, 2015

Contact: Rob Marus, Communications Director: 202.724.5646; robert.marus@dc.gov

Attorney General Racine Joins Colleagues in Letter Urging Congress to Preserve State Authority on Data-Security Laws

Attorneys General Urge Congress Not to Preempt State Laws That Protect Consumers

WASHINGTON, D. C. – In a bipartisan effort to protect consumers, Attorney General Karl A. Racine has joined his colleagues from 46 other state-level jurisdictions in urging Congress to maintain states’ authority to enforce data-security laws as well as their ability to enact new laws to address future data risks.

Citing recent efforts in Congress to pass a national data-security law, the attorneys general today sent a letter to members of Congress cautioning against federal preemption of state laws addressing data breaches and requiring notification of consumers whose data has been compromised. The letter argues that any federal law must not diminish the important role states already play in protecting consumers from data breaches and identity theft, particularly in states where state law provides greater protections for consumers than federal law does.

“As we have recently seen in multiple high-profile cases involving data breaches, this is an emerging and crucial frontier in consumer protection,” Attorney General Racine said. **“We want to ensure that the District and our peer states are able to protect our residents as robustly as possible.”**

The letter urges Congress to preserve existing protections under state law, so that states can continue to enforce their laws on notifying consumers about breaches and can continue enacting new laws to respond to new data-security threats. The letter also points out a number of concerns with federal preemption of these kinds of state laws:

- **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. Full-blown identity theft involving the use of a Social Security number costs the average victim \$5,100.
- **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 information entrusted to them by consumers, putting consumers’ personal data at unnecessary risk.

- **State officials play an important role in responding to data breaches and identity theft.** The states have been at the front lines in helping consumers deal with the repercussions of a data breach. State officials' role includes providing important assistance to consumers who have been affected by data breaches or who suffer identity theft or fraud as a result as well as investigating the causes of data breaches to determine whether the data collectors have had reasonable data security in place.

Today's letter, co-sponsored by Arkansas, Connecticut, Illinois, Indiana, Maryland, Massachusetts and Nebraska, was joined by the District of Columbia and by Alabama, Alaska, Arizona, California, Delaware, the 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, the Northern Mariana Islands, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Utah, Vermont, Virginia, Washington, and West Virginia.

A copy of the letter is attached.

###