Press Releases

July 7, 2015

MADIGAN URGES CONGRESS TO PRESERVE STATE'S AUTHORITY TO ENFORCE DATA BREACH & DATA SECURITY LAWS

Attorneys General Oppose Federal Preemption of States' Ability to Legislate & Enforce Laws that Protect Consumers from Data Breaches & Identity Theft

Chicago — Attorney General Lisa Madigan today urged Congress to pass a federal data security law that allows states to continue to enforce their own state data breach and data security laws in the interest of better protections for consumers across the country.

Citing recent efforts in Congress to pass a national law on data breach notification and data security, Madigan argued that any federal law must not diminish the important role of states in addressing data breaches and identity theft, especially in states like Illinois that has laws that provide greater protections than federal counterparts.

"Data breaches are increasingly threatening our financial security," Attorney General Madigan said. "States absolutely must maintain their authority to serve as a frontline responder to assist residents in the wake of data breaches to help minimize the threat of identity theft."

The letter, which was joined by 44 other states and the attorney generals of the District of Columbia and the Northern Mariana Islands, urged Congress to preserve existing protections in 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.

The attorneys general point 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 over 815 million records containing sensitive information about consumers – primarily financial account information, Social Security numbers or medical information. Identity theft involving the use of a Social Security number can cost a consumer an average of $5,100 in losses.

- **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 customers, putting customers' 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 address 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.

In Illinois, Attorney General Madigan recently drafted legislation to strengthen the state's Personal Information Protection Act (PIPA). Originally passed in 2005 at Attorney General Madigan's direction, PIPA made Illinois among the first states in the country to require entities that suffer a data breach to notify Illinois residents if the breached information included residents' drivers' license numbers, social security numbers, or financial account information. Since the law's enactment, the extent of sensitive information collected about consumers has expanded and the threat of data breaches has increased significantly, necessitating the need to update and strengthen the state's law.

Madigan's bill, Senate Bill 1833, which has been endorsed by Illinois PIRG, Citizen Action Illinois, the Heartland Alliance and more, will expand the type of information that triggers a breach notification to consumers, including medical information outside of federal privacy laws, biometric data, contact information when combined with identifying information, and login credentials for online accounts. The bill also requires entities holding sensitive information to take "reasonable" steps to protect the information, to post a privacy policy describing their data collection practices, and to notify the Attorney General's office when breaches occur. Entities will also be required to notify the Attorney General's office in the event of a breach of geolocation information or consumer marketing information, making Illinois the first state in the country with such a requirement. Madigan has said her office would create a website that lists every data breach that affects Illinois to increase awareness among residents.

To help Illinois residents, Madigan's office has an Identity Theft Unit and Hotline (1-866-999-5630), run by a team of experts who provide one-on-one assistance to victims of identity theft and data breaches. Since the creation of the hotline, the Attorney General's office has helped over 38,000 Illinois residents remove more than $27 million worth of unauthorized charges on their accounts.

-30-

Return to July 2015 Press Releases

TOP