BRIAN E. FROSH
ATTORNEY GENERAL

MEDIA CONTACTS:
Press@oag.state.md.us
410-576-7009

PRESS RELEASE

AG Frosh Urges Congress to Preserve States' Authority to Enforce Data Breach and Data Security Laws

47 Attorneys General sign letter opposing federal preemption of laws protecting consumers from data breaches and identity theft

Baltimore, MD (July 7, 2015) - Attorney General Brian E. Frosh today urged the U.S. Congress to preserve states' authority to enforce data breach and data security laws, while also allowing states to continue enacting laws that address future data security risks.

Frosh, joined by the Attorneys General of 46 other states and territories, wrote in a letter to members of Congress that recent efforts to pass a national law on data breach notification and data security should neither preempt state laws nor diminish the important role states already play in protecting consumers from data breaches and identity theft.

"Maryland has passed laws to protect consumers from data breaches and identity theft, and it would be ill-advised if Congress passed a law that prevented the state from continuing to protect its residents," said Attorney General Frosh. "We have seen in recent years how widespread data breaches have become, which is why our enforcement efforts cannot be constrained in any way." Under Maryland law, businesses are required to take reasonable steps to protect sensitive consumer data. When a date breach occurs, timely notice must sent both to affected consumers and to the Office of the Attorney General. Many of the bills being currently considered by Congress would take some or all of these protections away from Marylanders and would prevent the state General Assembly from enacting new protections.

Maryland was among the lead drafters of the letter, which 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.
Separately, Attorney General Frosh also sent a letter to Maryland's Congressional delegation expressing concern about the potential impact a national data breach law would have in Maryland.
"Our constituents want more protection of their personal information, not less," wrote Attorney General Frosh, adding that the large number of breaches would overburden any one federal agency and that some breaches may be deemed minor on a national scale, even if its impact is more severe in a given state or region. "State attorneys general must have the authority to

investigate such breaches, and they should be able to continue to require notification to their offices." The letter to Maryland Delegation can be viewed here

Attorney General Frosh noted that his office has regularly investigated the causes of data breaches and has taken enforcement action against businesses that have failed to adequately protect the sensitive data entrusted to them by consumers. The Office of the Attorney General Identity Theft Unit received more than 1,000 inquiries in the past year. The multistate letter, which can be viewed at here, 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 on 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. 47 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 2005, 44 state attorneys general, including then-Maryland Attorney General J. Joseph Curran Jr., wrote a similar letter to Congress calling for a national law on breach notification that did not preempt state enforcement or state law.

See a video of Attorney General Frosh speaking on this topic here:
https://youtu.be/DKGfGrKMESo