

Rep. Jan Schakowsky

Opening Statement

Subcommittee on Commerce, Manufacturing, and Trade

“Protecting Consumer Information: Can Data Breaches Be Prevented?”

February 5, 2014

Thank you Mr. Chairman for holding this important hearing on data security and breach notification. As we’ve discussed previously, I hope and expect we will work together to address these issues.

I thank all of our witnesses for being here, but I’d like to take a moment to pay a special thanks to my friend, Illinois Attorney General Lisa Madigan. She has been at the forefront of this issue since taking office in 2003, leading several efforts at the state level to defend against cyber crime and prosecute those responsible. She is also co-leading an investigation into the Target, Neiman Marcus, and Michaels data breaches. I look forward to gaining from her perspective about how we can better protect data and inform consumers in the future.

The threat of data breaches isn’t new: the Privacy Rights Clearinghouse has identified over 650 million records containing consumers’ personal information that have been compromised through thousands of data breaches since 2005. Nonetheless, the recent attacks at some of this country’s most popular retail stores should give us all renewed motivation to address data security and breach notification.

I think every one of our witnesses today and every member of this subcommittee wants to make sure that we do everything we can to reduce the risk of future massive data breaches. Tens of billions of dollars each year are lost to cyber fraud and identity theft, threatening consumer credit and stretching law enforcement resources. The Target breach alone could cost as much as \$18 billion, and analysts suggest the company itself could be on the hook for more than \$1 billion in costs from fraud.

It is important to note that there is no foolproof regulatory scheme or encryption program to prevent data breaches. Cyber criminals are incredibly innovative, and as soon as we invent and implement new technologies, they are hard at work looking for vulnerabilities.

But just because we can’t absolutely guarantee the protection of consumer data doesn’t mean we shouldn’t try. There is currently no comprehensive federal law that requires companies to protect consumer or user data. Nor is there a federal requirement that companies inform their customers in the event of a data breach.

I believe it is critical that this subcommittee move forward with legislation that will ensure that best practices are followed at all retailers and that consumers are informed as soon as possible

after cyber theft is discovered. That legislation should be technology-neutral, allowing the FTC and other regulatory agencies to update requirements at the speed of innovation.

In the 111th Congress, I was one of 4 original cosponsors of HR 2221, the Data Accountability and Trust Act, offered by Mr. Rush. The bill was bipartisan and counted Chairman Emeritus Barton as a cosponsor. The bill had two main provisions: (1) an entity holding data containing personal information had to adopt reasonable and appropriate security measures to protect such data; and (2) that same entity had to notify affected consumers in the event of a breach. Those basic requirements should be the basis for data security and breach legislation coming out of this committee.

Our constituents can't afford another massive data breach that threatens their credit and the protection of their identity. We owe it to them to take steps to limit the likelihood of data breach and ensure that they are informed when that happens.

I thank our witnesses for appearing today, and I look forward to hearing from them about how we can better protect against cyber theft in the future and ensure that consumers are informed as soon as possible when those protections fail.