

**Opening Statement of the Honorable Fred Upton  
Subcommittee on Commerce, Manufacturing, and Trade  
Hearing on “What are the Elements of Sound Data Breach Legislation”  
January 27, 2015**

*(As Prepared for Delivery)*

This committee has a strong tradition of bipartisan cooperation and problem solving. In this spirit, today we continue our focus on the key elements to pass a federal data breach law – a priority the president identified in his State of the Union address last week. I look forward to working with the White House, Dr. Burgess, and members of this committee to accomplish that goal.

Criminal cyber hacking presents a serious risk of economic harm to consumers and businesses alike. From small mom-and-pop shops in Southwest Michigan to global fortune 100 companies – the unfortunate reality is that companies of all sizes are at risk of having information hacked.

This committee will be examining a series of issues relating to cybersecurity this new Congress. Where the conversation begins today is with a data breach bill, and I want to encourage members and the public to focus on getting that issue right before we try to tackle some of the other concerns. There are significant privacy issues in an online economy, and some of those will have to be addressed separately. Let’s also be clear that this isn’t a financial services bill. We cannot let data breach legislation be sunk by extraneous issues.

Today’s hearing will examine two discrete issues related to the complex effects of cyber crime: commercial data security and breach notification to consumers. There is a real opportunity this Congress to set a single, national standard for data security and breach notification.

I personally believe that a single, federal standard is the key to passing a solution. The trade-off is that it has to be a strong, consumer-friendly law – one that has real protections and real enforcement. Both the FTC and state AGs have shown that this is an area that they would police very effectively. Our role is to strike the right balance on when notification is required, how timely it needs to be, and what information leads to identity theft.

Setting a national standard benefits consumers by ensuring that every business must look at their activities and make sure they are taking reasonable security measures. A national standard allows businesses to focus on securing information and systems instead of trying to figure out how to comply with a host of different state laws with teams of lawyers. Consumers benefit from consistency in security and breach notification no matter what state they live in.

We are particularly concerned with the impact these criminal acts have on consumer confidence, economic growth, and job creation. The criminals are in this for the money, so we need to make it far harder to steal an identity or use stolen information to make purchases. The cost to consumers is well into the billions of dollars. No committee is more aware than this one about how central the online economy is to our future. A data breach bill is the first step to securing that future.

###