

Statement of Chairman Fred Upton
Commerce, Manufacturing, and Trade Subcommittee Hearing on “Protecting
Consumer Information: Can Data Breaches Be Prevented?”
February 5, 2014

The recent data thefts of consumer information at well-known companies are a reminder of the challenges that we face in a digital, connected economy. We are well aware of the benefits to consumers and businesses of instant communication and e-commerce. The rapid evolution of technology allows consumers to purchase goods and services on demand –whenever and wherever they want. Despite the many new conveniences and efficiencies, the unfortunate reality is that technology also facilitates the ability of criminals to commit identity theft or other crimes that can potentially injure far more consumers.

What originated as paper-based fraud or identity theft gathered from a dumpster or mailbox has changed with the times and adapted to the Internet and the digital economy. Today, most transactions we conduct are either transmitted or stored in a connected environment, ensuring almost every citizen has some digital footprint or profile. If the most sophisticated cybercriminals are successful in infiltrating digital databases, they can gain access to data on millions of individuals. As long as the risk-reward payoff is sufficient to attract criminals, the problem will not go away.

Congress recognized the importance of protecting our personal information as the crimes of identity theft and financial fraud became more pervasive in our economy. It is the reason we enacted laws specifically to address sensitive consumer data that can be used by criminals for identity theft or financial fraud, including the Gramm Leach Bliley Act for financial institutions and HIPAA (Health Information

Portability and Accountability Act) for healthcare industry participants.

Additionally, we also have empowered the FTC to address data breaches through the use of Section 5 of the FTC Act, under which they have settled 50 data security cases.

The federal government is not the only layer of protection. A handful of state laws mandate security for the data of their citizens, and the private sector has developed extensive standards through the PCI Security Standards Council.

Yet breaches, identity theft, and financial fraud continue, affecting every sector from the federal government to merchants, banks, universities and hospitals. We must consider whether the current multi-layer approach to data security – federal, state, and industry self-regulation – can be more effective, or whether we need to approach the issue differently.

In short, the title of today’s hearing is an appropriate question to ask: “Can Data Breaches be Prevented?” This is the right venue to discuss what businesses can reasonably do to protect data. Equally important, we need to find ways to minimize or eliminate the ability of criminals to commit fraud with data they acquire. Americans deserve to have the peace of mind that the government, law enforcement officials, and private industry are doing everything necessary to protect the public from future breaches.