

Opening Statement of the Honorable Lee Terry
Subcommittee on Commerce Manufacturing and Trade
Hearing on “Protecting Consumer Information: Can Data Breaches Be Prevented?”
February 5, 2014

(As Prepared for Delivery)

Welcome to our subcommittee’s first hearing of 2014 and the 20th meeting of the 113th Congress.

Today, we are turning our focus to an important issue that has affected nearly one-quarter of American consumers: a string of recent data breaches at nationwide retailers, which resulted in the loss of consumer payment card data and personal information for millions of consumers.

Millions of consumers are seeking answers to questions about their personal and financial security. I’m grateful to both Target and Neiman Marcus for agreeing to appear before our subcommittee today. It is my hope that they will be able to give the subcommittee as clear a view as possible of what transpired, what was being done to protect consumer information before these breaches, what steps have been taken to mitigate the harm to consumers in the wake of these breaches, and what more is being done to prevent such breaches in the future.

We will also hear from public and private sector entities who participate in developing security standards, protecting consumer data, and taking enforcement actions against the criminals who perpetrate these crimes.

Our objective today is not to cast blame or point fingers—just like you don’t blame the homeowner whose home is broken into. Nevertheless, we must ensure that breaches like these do not become the “new normal.”

The private sector has worked to try and prevent these crimes to different degrees, including cooperation with government entities. Clearly, there is more than can be done, which is the reason for convening today’s hearing.

Already, the U.S. accounts for 47 percent of the fraudulent credit and debit losses worldwide, while only accounting for 30 percent of the transactions.

We need to be realistic and recognize there is no “silver bullet” that is going to fix this issue overnight. If we are to seriously address the problems surrounding consumer data security, it will take thoughtful and deliberate actions at all stages of the payment chain.

I do not believe that we can solve this whole problem by codifying detailed, technical standards or with overly cumbersome mandates. Flexibility, quickness, and nimbleness are all attributes that are absolutely necessary in cyber security but run contrary to government’s abilities.

I do believe that information sharing is an area that we can be involved with. I would like to explore with our witnesses today a role for Congress in information sharing and analysis centers (ISACs).

We must encourage the private sector to keep improving on its consensus-driven standards, which are built to adapt over time to changing threats to data security.

There are areas where Congress can take action and lead in a way in protecting consumers and combating fraud. One such area is a uniform data breach notification standard. Right now, national retailers have to comply with as many as 46 different state and territory notification rules, which can slow down how quickly a business can notify customers of a breach by creating confusion over who must be notified, how they must be notified, and when they must be notified. Consumers need to know quickly if their information is breached so that they protect themselves. I am working on legislation that would

foster quicker notification by replacing the multiple – and sometimes conflicting – state notification regimes with a single, uniform federal breach notification regime.

The security of data itself is paramount in this conversation, but as I have said, cumbersome statutory mandates can be ill equipped to deal with evolving threats. Nonetheless, I think this subcommittee would benefit from hearing about how companies are dealing with this issue now, as well as in the future.

I understand that the four largest credit card companies have put a deadline of October 1, 2015, for merchants to adopt point-of-sale portals that accept EMV-enabled cards — the so-called chip-and-PIN. I am interested in hearing about how this technology could benefit consumers, as well as what Congress' role should be with regard to data security in general.

I look forward to hearing from these stakeholders and officials on our panel today and I thank them for appearing.

###