Opening Statement of Chairman Thomas R. Carper
Data Breach on the Rise: Protecting Personal Information from Harm
April 2, 2014

As prepared for delivery:

I would like to begin by thanking our panel of witnesses for joining us this morning to discuss a critical issue that is facing our nation. I'd also like to thank Senator Roy Blunt for joining us today to discuss his work on this issue.

There is no doubt that technology has evolved rapidly, particularly over the last decade. And these advances will continue to grow exponentially in the coming years. Technology that, 10 years ago, could have been something out of a science-fiction movie, is now a part of our daily lives.

As we embrace the latest technology both at home and in the workplace, there is little doubt that more of our sensitive personal information is at risk of being compromised. Whether it is stored on the electronic devices we use daily or on a company server, this data can be vulnerable to theft.

As the way we communicate and do business has evolved, so have the tactics used by criminals to steal our money and personal information. Today's cyber criminals run sophisticated operations and are discovering how to manipulate computer networks and make off with troves of personal data. These data breaches have become much more prevalent, with a new one seemingly being reported almost every day.

Data breaches can put our most valuable and personal information at risk, causing worry and confusion for millions of individuals and businesses. The impact of a data breach on the average American can be extremely inconvenient and sometimes results in serious financial harm. Data breaches can also be extremely expensive for banks and other entities to respond to and remediate.

Although several high-profile retailers have recently become the face of data breaches, they are not the only victims of these cyber intrusions. Hackers are targeting all types of organizations that people trust to protect their information – from popular social media platforms to major research universities. The pervasiveness of these incidents highlights the need for us to find reasonable solutions to prevent attacks and protect consumers and businesses if a breach occurs.

We will hear in testimony today that many retailers, financial institutions, payment processors and the groups representing them are coming together to find common sense solutions that the private sector can undertake proactively without the help of Congress. These are groups which often times find themselves on different sides of an issue.

I recognize though that there remain existing areas where Congress can and should play a constructive role. One important area where Congress can play a constructive role is answering the calls for implementing a uniform national notification standard for when a data breach occurs.

Currently, when a breach happens, notification occurs under a patchwork of 46 different state laws. While some of these laws may have common elements, creating a strong uniform standard will allow consumers to know the rules of the road and allow businesses to invest the money saved from compliance into important upgrades and protections.

That's why I have joined with Senator Blunt to introduce the Data Security Act of 2014.

This common-sense legislation would require a national standard for entities that collect sensitive personal information. It would require these entities to enact a cohesive plan for preventing and responding to data breaches, plans that would detail steps that will be taken to protect information, investigate breaches and notify consumers. I've referred to these steps with the acronym P-I-N.

Most importantly, these plans would provide consistency throughout the nation and allow consumers to have a greater level of confidence that their information will be protected, and that they will be notified if a breach occurs despite whatever protective measures have been put into place.

We are never going to be able to prevent every breach, but we owe it to the consumers and the businesses and other entities that have been and will be victims of breaches to put into place the best system possible to deal with this growing threat.

I look forward to hearing from our witnesses today who are the leading voices on cybersecurity and data breach in both government and the private sector. I am sure their insight will be valuable as we continue with our efforts to fix this problem.

I am encouraged that many of my colleagues share my interest in advancing our efforts to address data breaches. I hope we can embrace the 80-20 rule. That is -- set aside the 20 percent that we can't agree on and focus on the 80 percent on which we can agree.

It is in everyone's interest to ensure that we minimize the occurrence and impact of data breaches.

###