

**Chairman Patrick Meehan**  
**Opening Statement as Prepared for Delivery**  
**Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies**  
**Field Hearing: “Protecting Your Personal Data: How Law Enforcement Works with the**  
**Private Sector to Prevent Cybercrime”**  
**April 16, 2014**  
**Paul Peck Alumni Center, Drexel University, Philadelphia, Pennsylvania**  
**10:00 a.m.**

Recent cyber breaches at retailers including Target, Neiman Marcus and Michaels have once again brought the public’s attention to the threat of criminals accessing their personal information. Unfortunately, such data breaches are neither new nor rare. The Target attack alone compromised the information of approximately 110 million consumers and it could be months or years before we know how many of those customers will eventually be the victims of fraud. In 2012, an estimated 16.6 million Americans experienced identity theft costing consumers nearly \$25 billion. This problem is not going away, either. Just last week, many people learned about the so-called “Heartbleed” vulnerability that affects the encryption software used in many e-commerce sites.

While fraud is nothing new, the techniques and scope have risen to a new level. Our increasingly interconnected world and the advancement of online shopping and banking has made our lives much more convenient but it also means that a sophisticated criminal can steal your account information without ever being in the same country. In fact, the biggest hotbed of hackers is in Eastern Europe, where criminals can buy, sell and trade various pieces of software used to attack systems and steal information.

The question then becomes, “what is being done about it?” From the retailers responsible for protecting the information on their systems, to the banks who are liable for fraudulent charges, to law enforcement at every level- local, state and federal- who are charged with going after the criminals, all of the stakeholders here play a role and are working hard to counter cyber fraud and identity theft.

Consumers must also do their part to protect themselves. Simple steps to increase cyber hygiene include creating strong passwords and changing them regularly, using antivirus software and keeping it updated and most importantly, keeping an eye out for suspicious activity on your computer and in your bank accounts. I’m looking forward to hearing from all of our witnesses about the outreach they do to inform consumers to better protect themselves.

Our first panel of witnesses is directly responsible for investigating cyber crimes at the federal and local level. In addition to its role as the lead agency investigating the recent retail breaches, we will hear from the Secret Service about the tools at their disposal including the National Computer Forensic Institute, which trains local law enforcement officials to investigate and prosecute cyber crimes, the Cyber Intelligence Section that collects, analyzes and disseminates data and the Electronic Crimes Task Forces that brings together law enforcement, academia and

the private sector to combat computer-based threats to our financial payment systems and critical infrastructures.

Similarly, the FBI will testify about their role in investigating cyber related crimes and about the National Cyber Investigative Joint Task Force, which was created in partnership with the Department of Defense, the intelligence community, law enforcement and the private sector to coordinate and share information.

We will also hear from Delaware County District Attorney Jack Whelan, who will tell us about local efforts to fight cyber crime, the effects on the community and how we are doing at the federal level in coordinating with and helping local law enforcement.

Our second panel will discuss efforts in the private sector to prevent and respond to cyber attacks. They are the ones on the front lines fighting the problem and continue to suffer significant financial losses. I am particularly interested in hearing from them about how they interact with law enforcement and how we can better help them protect their customers.

I look forward to hearing from all of our witnesses today and again thank everyone for their attendance.

With that, I yield the balance of my time.