Remarks for the Identity Theft Resource Center
Commissioner Terrell McSweeny
October 29, 2014

Good morning, it is great to be here as part of this event unveiling the Identity Theft Resource Center's "Identity Theft: The Aftermath" survey of victims of identity theft. I want to thank James Lee for those great welcoming remarks, and Eva Velasquez for inviting me to be here this morning. The FTC has a great partner in the ITRC in our joint efforts to protect consumers from identity theft.

Over the last two decades, we have quietly witnessed a remarkable turn of events regarding violent and property crime. Today streets are safer, crime is lower, and people have less of a chance of being a victim of a violent crime than at any other time in the last 50 years.

On Monday, Gallup released a new survey on the crime concerns of Americans. As most would expect, those surveyed had modest concerns about terrorism, car-jackings, and mass shootings. There was one crime which stood out across all ages, all races, and income levels.

Among all Americans, 69% were very concerned about their credit card information being hacked, 62% had similar worries about their smart phones or computers. Identity theft is really "the crime" of our interconnected technological world. In this new environment, the losses are staggering. The Bureau of Justice Statistics found that in 2012 the financial losses from identity theft totaled nearly $25 billion. The total loss from all property crime combined, by comparison, was $14 billion.

Identity theft, unlike a stolen wallet, can lead to years of financial loss and remediation. Last week, the FBI announced that in the last year nearly 519 million financial records were stolen from banks, retailers, and other businesses.

The Financial Services Roundtable, a leading trade association for the largest banks, estimates that 110 million American adults have had their data exposed by various breaches over the past year. At the FTC, over the same time period, we received some 290,000 complaints-almost 6,000 a week.

It seems that not a week goes by without another in a string of high-profile hacks. But, disturbingly, the news has seemed to desensitize many people to the real risks created each time an event occurs. Less than one-third of consumers, when learning of a breach, reset passwords or change other identifying information.

Unlike a pickpocketing, it might take a victim months to discover they have had their identity stolen. In the ITRC's own survey, over 40% of consumers did not know they were victimized until over a year after the crime first started. And, unlike a pickpocketing, the harm can be life altering:

Victims can lose the ability to get credit or apply for loans.

They might face continual harassment from collection agencies.

They might end up paying more to keep the credit they already have.

In some cases, victims of identity theft have lost jobs or homes.

Too often, people feel that they must face the daunting challenges of protecting their financial life, repairing their credit, and dealing with creditors and financial institutions alone.

The FTC has been in the vanguard of helping consumers deal with the problems, and going after bad actors and the bad practices, which enable this crime. We work with over 2,000 different American and Canadian law enforcement agencies, at every level of government, to find and prosecute the perpetrators and bring resources to consumers, community groups, and businesses.

The FTC is the lead agency protecting the privacy and data of American consumers. When companies do not have adequate security safeguards, or make misrepresentations about their security, the FTC is the frontline enforcement agency. Since we brought the first data security case in 2002, the FTC has brought more than 50 data security cases and continues to take each revelation of a breach very seriously. But more has to be done- particularly with easing the stress on people whose personal information has been stolen.

Consumers often don't know where to turn once they realize they are victims. Should they go to the police, or their bank, or their credit card company, or the credit bureaus, or the FTC? Should they cancel cards, initiate a fraud alert, or maybe even a credit freeze? Which accounts are safe and which are not?

Those questions are not always easy for those of us in this room to answer let alone the average person blindsided with the realization. And as we all know, the ease of resolving these matters varies greatly from person to person and business to business.

That is why I was thrilled to join President Obama two weeks ago when he unveiled the new "Buy Secure" initiative and signed an Executive Order giving the FTC new tools to help the American consumer. What the Buy Secure program will do for Americans is provide an easier way to report identity theft and begin to repair the damage.

For a long time now, the FTC has hosted the IdentityTheft.gov web site. The President has now directed the Departments of Justice, Commerce, and Homeland Security to provide us with their resources and information so that Americans can go to one site and one agency for the resources they need. We will expand IdentityTheft.GOV, making it a more functional clearinghouse for the combined resources of the Federal government.

Furthermore, and I'm very excited about this, we will be working with the credit bureaus to streamline the reporting and remediation process so that it is easier for victims of identity

theft to get their lives back on track. We hope to have all of this up and running by May, and I am committed to ensuring that this is done.

The efforts of the Buy Secure initiative I hope validate that the best way to combat identity theft is a rigorous and energetic public and private partnership. Retailers and banks have been improving their capabilities over the last year, and the President's initiative to speed up the adoption of chip-and-pin technology through Federal purchasing, will help even more.

Technology leaders like Google, eBay, Apple, and Amazon are all making their payment platforms more secure and consumers are becoming more savvy. But we have a long way to go, and criminals will always adjust.

That is why the FTC supports comprehensive data security and breach notification legislation that would create strong and consistent national standards; strengthen the FTCs enforcement capabilities; and provide consumers notice of when a breach occurs so they can better protect their information.

National data security and breach notification legislation is a win-win for consumers and businesses. National standards would simplify compliance for businesses, while also giving consumers greater security.

That is what makes the report the ITRC is unveiling today is so important. It helps enforcers and policy makers to put the focus back on the consumer. What can we be doing to make the marketplace a bit fairer? What can we do to promote better practices? What can we do to get victims the help they need? So that a breach doesn't mean years of endless phone calls with customer service representatives; or fighting creditors and debt collectors; or the inability to finance a car or a home.

At the FTC we will continue to help consumers with our enforcement and education efforts. I look forward to working with everyone here to make the fight a little easier.

Thank you.