Project GOAL – Internet Safety for Older Adults: Challenges and Solutions
Washington D.C.
February 10, 2015
Keynote Remarks of Commissioner Terrell McSweeny[1]

Good morning, and thank you for that wonderful introduction. I want to thank Google for hosting us today and Debra Berlyn for her leadership on behalf of older Americans, and for highlighting what policy-makers and industry should be doing to make sure the benefits of our new, digital age, can be shared with people of all ages.

As a mom of a four and six year old, I'm constantly amazed by the digital fluency of my kids. My kids will never remember a day without smart phones and tablets, much less the Internet. The other day I asked my six year old to pause the game he was playing on my iPhone to answer our wireline phone, only to discover he had no idea how to do that.

As my parents will attest, their grandchildren's fluency with new technology can be very helpful – such as when my four year old taught my dad how to text. For the record, my parents and my in-laws are both savvy Internet and technology users. They use smartphones and tablets and laptops. They bank online, buy tickets online, video chat with their grandkids, and check in with friends on social networks.

And while sometimes they still find it helpful to have a six year old around to explain how Netflix works, for the most part my parents have enjoyed the innovations made possible by our mobile and networked world. But all these benefits do come with risks – some of these risks are ubiquitous to all Internet users, while others seem to target particularly older Americans.

Perhaps the most widespread risk to all consumers – not just seniors – in our interconnected world is data breach and the fraud and identity theft that can follow. Just last week we learned of another high-profile breach of consumer information: Anthem. At the FTC, we have seen an increase in complaints around Tax ID theft, medical identity theft and even identity theft of children. It's no surprise that after the breaches at Target, Home Depot, Neiman Marcus and other high profile retailers, 2014 was termed "The Year of the Breach."

Here are some statistics:

The Financial Service Roundtable estimates that in the past year, 110 million Americans had personal data exposed by a breach. At the Federal Trade Commission over the same period, we received some 290,000 breach complaints – almost 6,000 a week.

The Bureau of Justice Statistics found that in 2012 the financial losses from identity theft and data breach totaled nearly $25 billion. The total loss from all property crime combined, by comparison, was $14 billion.

[1] The views expressed in this speech are my own and do not necessarily reflect those of the Commission or any other Commissioner.

Unfortunately, many breaches aren't discovered until well after the data is sold and fraudulent transactions are made in a consumer's name. Many people, including older consumers, don't know what to do once they realize they are victims.

Should they go to the police or the credit bureaus? Should they replace all of their credit cards or just the one affected? Should they put an alert on their credit reports or freeze them altogether? These are complicated issues even for the most vigilant consumer.

That's why I was glad that President Obama announced a new effort to make reporting and repairing a data breach easier for all consumers. Under his "Buy Secure" initiative, the Federal Trade Commission is working to consolidate all of the government's breach resources into one helpful site, www.identitytheft.gov. Once built out, the new IdentityTheft.gov will make it easier for victims to get the help and resources they need.

The President has also asked that the credit reporting agencies – Experian, TransUnion, and Equifax – work with us so that IdentityTheft.gov can be a portal where credit alerts, freezes, and the process of credit repair can begin. Once the revamped and expanded IdentityTheft.gov is ready, Project GOAL's work will become enormously valuable as you reach seniors with the resources and materials they need to take control of their online security and personal data.

Additionally, the FTC continues to use its enforcement power to bring data security cases serving notices to scammers – and to businesses that leave sensitive data exposed – that they have an obligation to improve their security practices.

Unfortunately, we are finding many old scams are now being repackaged to fit the online marketplace. For example, some scams prey on people's fear of becoming a victim of ID theft. Following an announcement of a large breach, it is common to see scams purporting to offer assistance with identity protection that are in fact just ways to gather personal information.

Just as older Americans were frequently the targets of unscrupulous salespeople and con artists in years passed, they are again the preferred victims of the new breed of Internet fraudster. The Internet has replaced the telephone and mailbox as the preferred medium to communicate scams and lure in victims.

Some of the most effective ploys we see are the ones largely dependent on a user's inexperience with the Internet itself. For example, in the last few years, the FTC has tracked an explosion of so-called "tech support" scams. This fall, we brought a case against one such fraudster who brought in over $2 million in a matter of months. In that case, consumers would receive a call from someone claiming to represent Microsoft or Google informing them that they had a computer virus on their home computer. The caller would then gain remote access to the computer and activate dormant, innocuous files. The consumer presumably didn't recognize the files, and would agree to a pricy security monitoring plan. Other tech-support scams have used remote access to steal personal information, or to insert malware directly into a user's home computer.

We are also tracking an exponential rise in IRS imposter scams and tax ID fraud. Complaints about IRS imposter scams have shot up. These scams involve someone who usually calls you purporting to represent the IRS and then gets you to "confirm" your personal information for them over the phone. It is important to remember that the IRS will *not* call you – they will only contact you by mail.

Tax ID fraud happens when a real Social Security number is used to get a job or file for a tax refund. You may have seen the story last week in which Turbo Tax stopped transmitting state returns when their system noticed a spike in questionable filings.

Unfortunately, people only find out they've been victimized after they receive notice from the IRS for taxes owed for a job they didn't work at, or that multiple returns have been filed in their name.

Somewhat relatedly, one of the longstanding frauds of our data-driven world has been the credit card or consumer credit repair scam. Often a consumer will receive a phone call from someone purporting to be from their credit card company with news that the consumer's credit card has been breached. The caller claims they can protect or repair their credit if the consumer provides some information. The criminal then uses the information to open new cards and lines of credit, or just steal and use the consumer's identity in its entirety.

As with many other schemes we prosecute, this and other long-standing frauds have migrated online where the Internet has given them new life. For instance, many of our sweepstakes frauds, where "winners" have to pay an upfront fee to obtain their prize, now operate as pop-up ads and unsolicited emails rather than as calls from a telemarketer or junk mail in a mailbox. Similarly, fraudulent Medicare and prescription-drug discount cards are marketed in online ads and appear in keyword searches on search engines.

As enforcers, we recognize that stopping frauds and scams can be like a game of whack-a-mole – which is why we are preparing new materials to help people protect themselves.

Last fall we announced a new campaign directed to active older Americans called "Pass it On." I love this effort because it is so different from earlier consumer education programs. Instead of seemingly nagging people into action or vigilance, the Pass it On message recognizes older Americans for the experience and wisdom they have.

Previously, education materials looked to adult children to bring their parents information and to make sure they understood it. Pass it On instead empowers people to educate their friends and their social networks about online safety, and also provides straightforward information about how to recognize scams that may be targeting them specifically because of their demographic.

To make all of our online interactions safer, we need more than enforcement and education; we need strong national standards for data security and breach notification. I know that there are serious, bipartisan efforts to pass legislation by the end of this year, and the FTC stands ready to work to support those efforts.

It is my hope that the final legislation contains strong requirements on security and gives the Federal Trade Commission enhanced penalty and rulemaking authority so that we can send appropriate signals to business and keep pace with rapid technological change.

The benefits of the Internet, connected devices, and more individualized technology offer today's older adults a world of choice, convenience, and safety that would have been unimaginable just twenty years ago. But for all the promise technology brings, there are risks. The risks are manageable, but by no means are they irrelevant. Helping everyone, including older people, understand the risks of technology so that they can better access – and have faith in – the benefits of technology is incredibly important.

I want to thank Project GOAL for doing just that, and I look forward to working with you to continue to spread that message.