NATIONAL CYBER SECURITY ALLIANCE
TWO STEPS AHEAD: PROTECT YOUR DIGITAL LIFE
Arlington, Virginia
December 14, 2015
Remarks of Commissioner Terrell McSweeny[1]

Good morning, and thank you Michael Kaiser, for that kind introduction. I also want to thank the National Cyber Security Alliance for inviting me to be here today and for organizing this terrific event, along with the Better Business Bureau.

The NCSA has been an incredibly valuable partner to the FTC and has played an important role in our efforts to educate consumers and businesses about data security, and we are grateful for your work in this area. The Two Steps Ahead education campaign is a wonderful way to spread the word about the steps you can take to protect your data and identity online.

For those of you who don't know the Federal Trade Commission or our work, we are the nation's consumer protection agency. A core part of our mission is to protect consumers' privacy, including by making sure that companies keep consumers' data secure. The FTC is primarily a law enforcement agency, so one way we protect consumer privacy and data security is by bringing law enforcement actions when we believe a company has failed to take reasonable steps to secure consumers' data – as we've now done on more than 50 separate occasions.

But an equally important part of our efforts to promote data security involves educating consumers on how to keep themselves safe online – and we have a lot of resources available on www.OnGuardOnline.gov and www.identitytheft.gov. We have also distributed millions of copies of our "Net Cetera" guide, which provides advice to parents and caregivers about talking to children about being online. It includes tips on talking to kids about computer security and how you can protect your child's privacy online.

Having conversations about data security is critically important as we move more and more of our lives online. I am a mom of a seven and five year old who will never remember a day without smart phones, much less the Internet, and much of their future social and work life will revolve around connected devices and online interactions.

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

For all of us, online technologies have transformed our everyday lives, giving us access to a wider variety of goods and services; a greater awareness for new opportunities and experiences; and easier ways to stay connected to loved ones and friends.

But these benefits do come with risks. We've all heard recent news reports about attacks on financial and highly personal data, or even connected children's toys. It has never been clearer that we must secure the software underpinning our modern life.

The risk of data breaches and identity theft looms large. The FTC has received more than 474,000 identify theft complaints to date in 2015. It is by far our most common complaint. According to the Bureau of Justice Statistics, 17.6 million Americans – or 7% of the U.S. population – were victims of identity theft in 2014.[2] The Bureau of Justice Statistics also 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.[3]

In addition to reaching out to consumers, we also need to reach out to the businesses that are collecting and storing our data. Together, we can think creatively about how best to solve the security challenges that technology companies and others are facing in today's connected world.

This is why the FTC recently unveiled our "Start with Security" initiative, which focuses on promoting better online security by educating businesses about best data security practices. It's critical that we get the message out to businesses of all sizes – from the startups to the mom and pop store that's moving online from the brick and mortar world for the first time, to the most sophisticated technology companies – that security cannot be an afterthought.

Security has to be an integrated part of each business's culture, from the very beginning, and it has to be valued from the ground up all the way to the C-Suite. In the rush to innovate and offer the newest, coolest product, privacy and security cannot be overlooked.

Our Start with Security guide for business distills ten lessons learned from our more than 50 data security settlements. For example, the guide encourages companies to think through the implication of their data decisions. By making conscious choices about the kinds of information

[2] Erika Harrell, U.S. DEPT. OF JUSTICE, BUREAU OF JUSTICE STATISTICS, "Victims of Identity Theft, 2014" (Sept. 2015) at 1, http://www.bjs.gov/content/pub/pdf/vit14.pdf.

[3] Erika Harrell and Lynn Langton, U.S. DEPT. OF JUSTICE, BUREAU OF JUSTICE STATISTICS, "Victims of Identity Theft, 2012" (Dec. 2013) at 6, http://www.bjs.gov/content/pub/pdf/vit12.pdf.

they collect, how long they keep it, and how they use it, companies can reduce the risk of a data compromise down the road. The guide also emphasizes the necessity of requiring secure passwords and authentication, including having policies that require complex hard-to-guess passwords, making sure that passwords are stored securely, and restricting access after a number of unsuccessful login attempts.

Our guide condenses a lot of information into a succinct form, and to complement the guide, we are also producing a series of short videos about each of the ten Start with Security principles. Today I have the pleasure of debuting our latest video, which reminds business to think critically about who has access to the data on their systems. By restricting access to networks and databases to only those who need it for their job, companies can reduce the risk that a compromise of any particular employees' credentials could result in a serious breach. Let me play the video for you now – it's about two minutes long.

Our Start with Security guide reminds companies that security isn't a one-time effort, but rather an ongoing process that requires continuous evaluation and updating. We encourage businesses to put procedures in place to keep security current and address vulnerabilities that may arise. For example, we have brought cases against companies that didn't update their anti-virus software, increasing the risk that hackers could exploit known vulnerabilities or overcome the businesses' defenses. It serves an important reminder to businesses that outdated software undermines security. The Start with Security guide can help businesses identify, and possibly prevent, these and other security pitfalls.

Besides our Start with Security Guide and videos, we have other resources available to help companies bake privacy and security into their products and services – otherwise known as implementing privacy by design – from general guidance on protecting personal information, to specific resources for those building mobile apps and connected devices.

For all these efforts, we recognize that increasingly more consumers will confront the unfortunate consequence of data insecurity: ID Theft. So, I am pleased that we are continuing to update and expand our www.identitytheft.gov, which is a one-stop shop where victims of identity theft can get information and checklists to start taking concrete steps to begin the recovery process.

Right now, the site helps consumers generate an affidavit, learn what actions to take following different types of ID theft, and obtain sample letters for credit bureaus, businesses, and debt collectors. Soon, we will be unveiling enhancements that will allow consumers to register and create an account so that they can update affidavits and track their progress over time, obtain a personal recovery plan that walks consumers through each step they need to take, and get customized, pre-filled letters that they can print out and send to companies. The improvements will make it easier than ever for consumers who have been affected by identity theft to address the damage and regain control.

Additionally, the FTC continues to bring data security cases serving notice to scammers and to businesses that leave sensitive data exposed, demonstrating that we take seriously the rights of consumers and will use all the tools available provided by law to enforce those rights.

I want to emphasize one thing: the FTC alone cannot make security a priority. It takes partnerships – with other agencies, with experts, and with members of the business community, just like you. By being here today, we are demonstrating our commitment to work together to make security a priority. So thank you for sharing in this work. We hope that you will continue to spread the word about the importance of security.