NATIONAL CONSUMER REPORTING ASSOCIATION 23RD ANNUAL CONFERENCE
Washington D.C.
November 4, 2015
Remarks of Commissioner Terrell McSweeny

Good morning, thank you for having me here for your national conference. I want to thank Terry Clemans for helping to put this event together and Bill Bower for that nice introduction. The Federal Trade Commission has a valuable relationship with NCRA, and many of our most important issues are your most important issues. Before I begin, I will give the standard disclaimer that the views I express are my own and do not reflect the Commission's views or the views of any other Commissioner.

We both see first-hand how consumers are susceptible to identity theft and how big data and technology are transforming the world of credit risk and prediction models. And I think we both find ourselves in a rapidly changing world and have to make sure new tools comply with hard fought public policy goals – like non-discrimination and consumer protection.

That is why it is important you have come to Washington this week. Policymakers at the FTC, the Consumer Financial Protection Bureau, in Congress, and in the Administration need to hear from you to understand how the marketplace of consumer reporting is changing. We need to make sure that our policy goals are not just empty pronouncements in Washington, but can actually work when a renter walks into a leasing office or a family wants to buy a new home.

This is a fascinating time to be a Commissioner at the FTC. The explosion of how we can collect data and what is done with it is transforming society. The financial crisis and its aftermath highlighted many problems in how consumers are offered, apply for, receive, and treat credit. Electronic and online transactions have brought efficiency gains to our economy and improved the quality of life for consumers. Those gains are tempered by an increased risk of fraud and the exposure of personal information to scammers. Between the sensors we use to track our steps, the Internet connected devices we have in our homes and cars, and the amount of information we are inputting into computers each day, we are producing more data than ever before.

How that data is used and how it is secured are central to what we do at the FTC. Cisco recently released a report that we will soon generate more than 400 zetabytes of data a year by 2018. How much is a Zetabyte, you might ask? Well, a Zetabyte is one trillion gigabytes. One gigabyte is approximately the amount of data in 4,500 books. Very roughly, we will soon be generating more data in one year from all our devices and transactions than all the data created from the dawn of the written word over 5,000 years ago to the creation of the Internet. That is a heck of a lot data.

All of that data has had an immeasurable impact on our world. It is has helped launch businesses, improve our public health, and allow access to educational and commerce opportunities that were impossible a generation ago. But it has also unleashed a wave of criminal activity that exists online but has devastating real world impacts.

The theft and misuse of personal data is an issue of increasing concern to Americans. Last year, Gallup released a survey on the crime worries of Americans. As most would expect, those surveyed had modest concerns about terrorism, car-jackings, and mass shootings. There was one crime, however, which stood out across all ages, all races, and all 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.[1]

Last week, Chapman University released a poll on what Americans fear most. Credit card fraud and identity theft actually caused more concern than illness, job loss, or death.[2] For each of the last fifteen years, identity theft generated the largest number of consumer complaints to the FTC – about 300,000 last year.[3]

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

[1] Rebecca Riffkin, Gallup, "Hacking Tops List of Crimes Americans Worry About Most" (Oct. 27, 2014), http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx.

[2] Sheri Ledbetter, Chapman University Blog, "America's Top Fears 2015" (Oct. 13, 2015), https://blogs.chapman.edu/wilkinson/2015/10/13/americas-top-fears-2015/.

[3] *See* Fed. Trade Comm'n, Consumer Sentinel Network Data Book for January – December 2014 at 6 (Feb. 2015), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2014/sentinel-cy2014-1.pdf.

the past year.[4] The Bureau of Justice Statistics found that in 2012 the financial losses from identity theft totaled nearly $25 billion.[5] The total loss from all property crime combined, including arson, burglary, and vandalism, by comparison, was $14 billion.

I am sure that everyone in this room has seen this problem up close. Stolen personal information, fraudulently opened lines of credit, and unpaid yet never-known-about debts plague honest consumers and make the process of getting a mortgage or approval for a lease or a job more expensive and time consuming. For many of you, it has meant hours spent with consumers correcting their credit reports or with the credit bureaus or creditors finding out more information. For the unfortunate consumer who was a victim of identity theft, it often means being victimized yet again because a mortgage might fall through or a job offer might not be extended.

The FTC has been in the vanguard of helping consumers deal with the problems, and going after bad actors and the bad practices that enable this crime. In the last year, there have been developments that promise to bring about long-term benefits for consumers. Two months ago, the Third Circuit issued an important ruling that reaffirmed our role in enforcing data security. For years, the FTC has been leading enforcement actions against companies who did not have adequate security in place to prevent a breach. Some argued that since Congress did not grant us explicit authority to police inadequate security, our actions were not justified or our jurisdiction was overbroad. One of the arguments made in court was that having the FTC enforcing against a data breach was akin to having the FTC police a supermarket for having a banana peel on the floor.[6] The Court pushed back against this assertion. They said that the breach in question was not merely one banana peel on the floor, but rather for that case the equivalent of 619,000 banana peels on the floor.[7]

---

[4] *See* Erin Kelly, USA TODAY, "Officials warn 500 million financial records hacked" (Oct. 20, 2014), http://www.usatoday.com/story/news/politics/2014/10/20/secret-service-fbi-hack-cybersecuurity/17615029/.

[5] 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.

[6] Reply Br. of Appellant, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-JAD (D.N.J. filed Dec. 8, 2014) at 6.

[7] Memorandum Op., *FTC v. Wyndham Worldwide Corp.*, No. 2-13-cv-01887 (D.N.J. filed Aug. 24, 2015). https://www.ftc.gov/system/files/documents/cases/150824wyndhamopinion.pdf

The Court's decision validated one prong of our data security and identity theft program. The first tactic is to use our enforcement authority against bad actors. Since our first data security case a decade ago, we have brought over 50 cases. Each has helped to develop an enforcement program that is flexible for businesses to meet but has also helped to institute best practices across industries.

Second, we educate businesses on what they need to do in order to provide reasonable security for their customers. We have issued a "Start with Security" guide that uses the various cases in order to help businesses understand the basics of protecting customer and employee information.[8] We understand that there is no such thing as perfect security. Hacks happen and information gets compromised, but what we want to see is reasonable security hygiene. We want information encrypted, access to sensitive information to be limited to those who need it, and for passwords not to be kept in files named "password." The Start with Security guide is free and can be downloaded at www.ftc.gov/business. We are taking our Start with Security message on the road and are hosting a series of events geared to entrepreneurs to help get companies thinking about security at the outset.

Third, we want to make sure consumers have the resources they need if they do have a problem. Last year, the President came to the FTC to unveil the Buy Secure Initiative. As part of that effort, the FTC was charged with creating a one-stop shop for Americans who have been a victim of identity theft through our IdentityTheft.gov website. We recently unveiled a new IdentityTheft.gov web site. Currently, the site provides an easy to follow checklist for consumers on what to do if they are a victim of a hack or breach. Eventually, we want IdentityTheft.gov to be the trusted place where all Americans can go to set up credit and fraud alerts, freeze their credit, report ID theft, and engage with law enforcement.

If you visit the site, you'll notice that we have a section devoted to some of the fastest growing frauds – tax identity. Tax ID theft is the fastest growing fraud that we monitor. Last year, it accounted for one-third of all ID theft complaints we received. In January, the FTC will be holding our third annual Tax ID theft awareness week. Raising awareness is just one part of

[8] *See* Fed. Trade Comm'n, Start with Security: A Guide for Business (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

our strategy. We are also working with the IRS, state tax agencies, and national tax preparers on efforts to limit fraud at the point of filing.

We are also keeping our eye on issues related to Big Data and the impact it is having on consumers. Last year, we held a workshop entitled "Big Data: A Tool for Inclusion or Exclusion?" which focused on the opportunities and pitfalls of using big data as an input. As new tools like data and social media mining become more prevalent, there is a growing concern that some entities will try to skirt the consumer protections of existing laws like the Fair Credit Reporting Act.

While we have overlapping jurisdiction with the Consumer Financial Protection Bureau over the FCRA, our enforcement activity has not waned. Three years ago, the FTC took its first action in this regard when we entered into a consent agreement with Spokeo. In that matter, we determined that Spokeo was acting as a consumer reporting agency and was in violation of the FCRA.

Just recently, we announced another consent agreement, this time with Sprint for violating the FCRA when they used credit reports to place customers with poorer credit into a higher cost program without their knowledge or consent. Sprint failed to provide customers with the credit information so that they could challenge the findings, and oftentimes did not even inform customers until after the contract period commenced, making it challenging for consumers to go to another service.

Another problem that I think everyone in this field is wrestling with is how to ensure that the best decisions are actually being made with the data available. As my colleague Commissioner Maureen Ohlhausen has said, "Data is a tool, it is not a substitute for wisdom."[9] Sometimes data might be incomplete and might not paint a comprehensive picture of a situation. Sometimes entire groups of consumers might not be measured, or inhabit what one recent paper on the problem termed a "data desert." Other times, advanced algorithms might reflect our own

[9] Maureen K. Ohlhausen, Commissioner, Fed. Trade Comm'n, Remarks at the Center for Data Innovation: The Social Impact of Open Data (July 23, 2014) at 4, https://www.ftc.gov/system/files/documents/public_statements/571281/140723socialimpactofopendata.pdf.

unwitting biases, or, as the programs self-propagate and auto-correct, exclude vulnerable or underrepresented groups.

The challenge for us as policymakers, and you as practitioners, is to approach these technologies with an understanding that they are merely tools and that individuals lie behind these data sets. We have come a long way from when banks and governments used racial and economic data to redline and isolate entire communities, when mortgage decisions were made by how someone looked or where they prayed rather than their ability to pay back the loan.

Your industry is one of the key remedies to those past abuses. Using data properly, with the fair and empathetic human oversight, will go a long way to ensuring we continue our progress on that path.

I want to thank you again for having me here. I hope we have some time for questions.