

# **Testimony of Commissioner Terrell McSweeney**

## **Before the Committee on Commerce, Science, and Transportation**

### **Subcommittee on Consumer Protection, Product Safety, and Data Security**

**March 21, 2017**

Chairman Moran, Ranking Member Blumenthal: thank you for holding this important hearing. I am Terrell McSweeney, and along with Acting Chairman Ohlhausen, we are the current members of the Federal Trade Commission.

The work of protecting American consumers from frauds and scams is bipartisan – in fact, I would call it non-partisan. For more than 100 years, the FTC has protected consumers from dishonest practices, although the particular scams we see in the marketplace change over time.

In 2016, we received more than three million consumer complaints and the top three categories were debt collection, impostor frauds, and identity theft. Since not all victims file complaints, these statistics understate the problem. The FTC's most recent national survey of fraud victimization estimated that 10.8% of all Americans over age 18 – or 25.6 million people – had been a victim of fraud in 2011.

The growth in impostor scam complaints is striking; they surpassed the number of identity theft complaints for the first time ever last year. In impostor scams someone poses as a friend, family member, romantic interest, legitimate company, or government agency, in order to obtain money or personal information.

Government impostor scams – the most common type of impostor scam reported last year – run the gamut from callers claiming to be from the IRS and demanding payment for back taxes to debt collectors claiming to be from a law enforcement agency.

Other impostors purport to be calling on behalf of a company such as Microsoft or Apple. They convince consumers that their computers are infected with malware. In reality no virus exists, but consumers pay for costly “technical support” services with little, if any, value.

We are taking action to stop these scams. Last year we brought multiple cases against tech support scams, as well as an action against an entity that was impersonating the Department of Transportation.

Stopping fraud is a core FTC priority. This includes not just pursuing bad actors who are directly perpetrating the frauds, but also others whose facilitate scams. One example is our recent case

against Western Union, which paid \$586 million to settle charges that it failed to stop scammers from using its money transfer system to collect payments for numerous types of fraud.

Protecting consumers is too big a job for the FTC to do alone. That's why we partner with other government agencies, states, and civic organizations in our anti-fraud work -- and why we invest in consumer and business education.

Educating American consumers is one of the best ways we can combat fraud. We produce materials in multiple languages for almost every demographic and make them available across platforms to reach the broadest possible audience. We hold Ethnic Media Roundtables around the country to help diverse communities highlight frauds affecting them.

We also have a campaign to help older people learn about common scams and pass that information on to their peers. And we work closely with the Department of Defense and others to help the military community avoid fraud.

It is vital that we continue this important outreach -- and ensure that we have the resources to meet the demand for our materials. This is especially true for our educational materials for parents and children, which help parents keep their kids safe online. It's critical that we keep these materials relevant and up to date, including optimizing them for mobile platforms.

The FTC must continue to stay abreast of emerging consumer protection issues. Our always-on, always-connected digital world is full of marvelous innovations - but it also creates some new opportunities for bad actors.

I'm particularly concerned about the growth in ransomware attacks. Ransomware attacks on computers -- both for individuals and businesses -- are unfortunately already well known. But I worry that attacks on connected consumer devices will soon become more common -- especially given wide-ranging industry data security practices. In the not-too-distant future a consumer might turn on her smart TV only to see a message that asks for \$50 in Bitcoin if she wants to watch television again.

In a world of new cyber threats, the FTC must keep pace with changing technology. We have been doing that by engaging with stakeholders -- and, most importantly, bringing technologists on board. The FTC's Office of Technology Research and Investigation, or OTech, is in its second year.

OTech is a talented inter-disciplinary team of lawyers and computer scientists who provide us with in-house research capabilities and the expertise to understand cutting-edge technology -- like cross-device tracking, or how algorithms impact consumer choice. As more of these technologies come into the marketplace, it is vital that the FTC continue to expand these capabilities.

Unlike many other enforcement agencies, the Federal Trade Commission sends refund checks to individual consumers who are harmed by unfair and deceptive business practices. Last year, we obtained orders that will return more than \$11 billion in redress to consumers.

Our enforcement actions not only provide American consumers with justice, they help to strengthen consumer trust in the marketplace, strengthening the dynamism of the American economy itself.

Thank you again for holding this hearing. I look forward to answering your questions.