**Prepared Statement of**
**The Federal Trade Commission**

**Before the**
**United States Senate**
**Special Committee on Aging**

**on**

# Hanging Up on Phone Scams: Progress and Potential Solutions to this Scourge

**Washington, DC**
**July 16, 2014**

Chairman Nelson, Ranking Member Collins, and members of the Committee, I am Lois Greisman, Associate Director of the Division of Marketing Practices, Bureau of Consumer Protection at the Federal Trade Commission ("Commission" or "FTC").[1] I appreciate the opportunity to appear before you today to provide an overview of the Commission's initiatives to fight phone scams that target seniors, with a particular focus on imposter scams. My testimony today will discuss the Commission's initiatives to fight these phone scams, including our law enforcement, consumer outreach, and efforts to spur policy and technological solutions.

Phone scams are a scourge that have harmed millions of Americans, including many elderly citizens. Seniors, in particular, are a frequent target of many phone scams, including imposter scams where callers trick seniors into sending them money by pretending to be a friend or relative in distress or an employee or official of a government agency or well-known business.

The Commission dedicates significant resources to identify emerging phone scams, locate the culprits, and file enforcement actions to stop the fraud and return money to consumer victims. These efforts have stopped fraudsters responsible for billions of illegal calls, and the agency will continue to pursue aggressively those engaged in imposter and other types of phone scams.

The FTC also disseminates an array of educational materials to help consumers spot and avoid phone scams. Among these materials is our recently created Pass It On package – an innovative education effort that arms older people with information about phone scams that they can "pass on" to friends or family members who might need it.

---

[1] The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or any individual Commissioner.

Finally, the agency has embarked on an ambitious plan to catalyze technological innovation that will hopefully lead to a telephone network that will minimize phone scammers' ability to hide from law enforcement by using fake caller ID information.

The FTC is fighting phone scams with every tool at its disposal, and this testimony briefly describes those efforts, with a particular focus on imposter scams.

## I. Law Enforcement

The FTC has aggressively combatted deceptive and abusive telemarketing for decades. In the past decade, the Commission has brought more than 130 cases involving telemarketing fraud against more than 800 defendants. Although some of these cases are still in litigation, the Commission has obtained judgments of more than $2 billion from the cases that have been resolved. Moreover, we also work closely with our foreign and domestic counterparts to help ensure that fraudsters are held criminally accountable.

Despite the Commission's efforts, the prevalence of phone scams remains unacceptably high. The most recent report by the Commission's Bureau of Economics on consumer fraud in the United States estimated that 10.8 percent of U.S. adults – 25.6 million people – were victims of fraud during 2011 alone. The phone is a commonly used tool in many frauds – the phone was the initial means of contact in nearly c 3 T d 2 ( e ) 6 (

recipient or someone who works for a government agency or well-known business. In 2013, 91 percent of consumers filing complaints about imposter scams reported that the fraudster initially made contact by phone. The economic impact of such schemes is severe. Consumers who complained to the FTC of imposter scams from the beginning of 2012 until May 31, 2014 reported the following monetary losses[3]:

| Product Service Description | Number of Complaints | Reported Amount Paid |
|---|---|---|
| Imposter: Family/Friend | 30,441 | $42,079,331 |
| Imposter: Government | 145,835 | $150,532,421 |
| Imposter: Business | 82,293 | $34,284,556 |
| **Total** | **257,396** | **$223,582,881** |

Set forth below are examples of each of the three categories of imposter fraud and the Commission's enforcement efforts in each area.

### A. Impersonating Family and Friends

The FTC has worked diligently to combat scams in which fraudsters call consumers and claim to be a friend or family member in distress. A prevalent example is the "grandparent scam," in which an individual receives a call from someone claiming to be a grandchild in need of immediate financial help, such as money to get out of jail or to cover hospital costs. One difficulty in shutting down this scam is that many perpetrators are located overseas, and the vast

3

majority of victims are told to send funds through wire transfers, which are very difficult to trace. Nonetheless, the FTC continues to do the work necessary to identify and bring cases against the perpetrators of these scams.

Our recent action in FTC v. Worldwide Info Services, Inc., is an example of our efforts to combat a variant of a friend and family imposter scam. The FTC has charged that telemarketers made phone calls to consumers with prerecorded messages informing them that a friend, family member, or other acquaintance had purchased a medical alert system for the consumer. The recording indicated that consumers would receive the system at no cost. In reality, no friend, family member, or other acquaintance purchased the system, and the company charged consumers, many of whom were elderly, $34.95 per month for monitoring. The FTC's action against the company resulted in a court order shutting down the telemarketing operation and freezing the defendants' assets pending the outcome of the

money transfer service company – Western Union – has used effective procedures to stop consumers from sending funds to perpetrators of fraud, here and abroad, using its money transfer

### B. Impersonating Government Agencies

The FTC also has sued companies claiming false affiliation with the Social Security Administration, the Medicare Program, the FBI and other law enforcement officers, state and federal financial agencies, and even the FTC itself, in calls to consumers.[7]

In one such case, FTC v. Broadway Global Master, Inc., the caller ID information on consumers' phones tricked consumers into believing that the calls were from the FBI.[8] When consumers answered the phone, the caller would pretend to be a law enforcement agent and claim that the consumer owed a debt, often threatening to sue consumers or have them arrested. The fraudsters managed to collect more than $5 million from consumers for debts they did not owe to the defendants, or did not owe at all. The FTC's civil action against mastermind Kirit Patel and his two companies shut the operation down.[9]

---

[7] See, e.g., FTC v. Fed. Check Processing, Inc., No. 1:14-CV-00122-WMS (W.D.N.Y. Feb. 24, 2014) (alleging impersonation of state and federal financial agencies), available at http://www.ftc.gov/enforcement/cases-proceedings/122-3273/united-check-processing-inc; FTC v. The Cuban Exch., Inc., No. 1:12-CV-05890-NGG-RML (E.D.N.Y. Nov. 28, 2012) (alleging impersonation of the FTC), available at http://www.ftc.gov/enforcement/cases-proceedings/132-3046/cuban-exchange-inc; FTC v. 6554962 Canada Inc., No. 1:08-CV-02309 (N.D. Ill. Apr. 23, 2008) (impersonating the Social Security Administration, Medicare program officials, or the consumers' bank), available at http://www.ftc.gov/enforcement/cases-proceedings/082-3118/6554962-canada-inc-also-dba-union-consumer-benefits-naeem.

[8]

### C. Impersonating Businesses

The FTC also targets fraudsters that impersonate legitimate companies in an attempt to steal consumers' money.[10] For example

FTC has also provided sworn victim statements to Canadian authorities that were used to help extradite and prosecute perpetrators of phone fraud. Since its inception in 1998, Project COLT has recovered over $26 million for victims of telemarketing fraud.

In addition, the FTC is also a member of the Jamaican Operations Linked to Telemarketing taskforce ("Project JOLT"). Project JOLT is a multi-agency task force consisting of U.S. and Jamaican law enforcement agencies working cooperatively to combat Jamaican-based fraudulent telemarketing operations that target U.S. consumers.[16] The FTC, through its involvement in Project JOLT, shares information, investigative resources, and complaint data with other JOLT members. The Commission has supported multiple prosecutions in partnership with Project JOLT, including prosecutions for phone scams that targeted the elderly and impersonated government agencies to promote fake lottery schemes.[17]

---

Scam" Indicted (Oct. 26, 2012), available at http://www.fbi.gov/losangeles/press-releases/2012/alleged-operator-of-grandparent-scam-indicted.

[15] See, e.g., Press Release, FBI, Owner of Timeshare Telemarketing Fraud Sentenced to 20 Years in Prison (Jan. 29, 2014), available at http://www.fbi.gov/miami/press-releases/2014/owner-of-timeshare-telemarketing-fraud-sentenced-to-20-years-in-prison; Press Release, United States Attorney's Office for the Northern District of Georgia, Adams Sentenced to Over 17 Years in Prison for Multi-Million Dollar Telemarketing Fraud Scheme (Feb. 9, 2012), available at http://www.justice.gov/usao/gan/press/2012/02-09-12.html.

[16] JOLT members include the FTC, Immigration and Customs Enforcement, the Department of Homeland Security, the Department of Justice, the Postal Inspection Service, the FBI, and Jamaican law enforcement agencies.

[17] For example, on April 29, 2014, a federal judge sentenced Jamaican citizen Oneike Barnett to 60 months in prison for his role in a fraudulent lottery scheme that targeted elderly victims in the United States. Barnett, who pled guilty, acknowledged that he was a member of a conspiracy that called elderly victims, informing them that they had supposedly won a large amount of money in a lottery. The fraudsters induced victims to pay bogus fees in advance of receiving their purported lottery winnings. In an effort to convince the victims that the lottery winnings were real, the conspirators sent written and electronic communications that claimed to be from the IRS and the Federal Reserve. See Press Release, U.S. Dep't of Justice, Jamaican Citizen Sentenced in Connection With International Lottery Scheme That Defrauded

The above examples provide snapshots of some of the numerous ways in which the FTC uses the tools at its disposal to enforce consumer protection laws against perpetrators of phone scams. Because of the ubiquity of and harm caused by these scams, the FTC continues to make phone fraud an enforcement priority.

## II. Consumer Education and Outreach

Public outreach and education is an essential means to advance the FTC's consumer protection mission. The Commission's education and outreach programs reach tens of millions of people a year through our website, the media, and partner organizations that disseminate consumer information on the agency's behalf. The FTC delivers actionable, practical, plain language materials on dozens of issues, and updates its consumer education whenever it has new information to share. For example, the Commission's library of articles in English and Spanish includes pieces specifically describing grandparent scams,[18] prize and lottery fraud,[19] medical alert system robocalls,[20] and government imposter fraud.[21]

---

Elderly Americans (Apr. 29, 2014), available at http://www.justice.gov/opa/pr/2014/April/14-civ-454.html.

[18] See Family Emergency Scams, FTC, http://www.consumer.ftc.gov/media/audio-0052-family-emergency-scams (last visited July 10, 2014); Family Emergency Scams, FTC, http://www.consumer.ftc.gov/articles/0204-family-emergency-scams (last visited July 10, 2014).

[19] See Prize Scams, FTC, http://www.consumer.ftc.gov/articles/0199-prize-scams (last visited July 10, 2014).

[20] See Colleen Tressler, To Robocall Scammers Who Lied About Free Medical Alert Devices: We've Got Your Number, FTC (Jan. 13, 2014), http://www.consumer.ftc.gov/blog/robocall-scammers-who-lied-about-free-medical-alert-devices-weve-got-your-number; Bridget Small, Robocall Scams Push Medical Alert Systems, FTC (July 18, 2013), http://www.consumer.ftc.gov/blog/robocall-scams-push-medical

In addition to providing guidance

path of a call – including lead generators, telemarketers, dialing platforms, and phone service providers – can be located in different countries, making investigations even more challenging.

The FTC has responded directly to the new technological reality by working to identify and support a variety of short-, medium-, and long-term technical

On the other end of the spectrum, the FTC encourages solutions that would fundamentally shift the playing field in the fight against phone scams. A working group of the Internet Engineering Task Force ("IETF") called "Secure Telephone Identity Revisited" ("STIR")[29] is working to specify changes to existing telephone protocols and processes that would combat the problem of caller ID spoofing that is employed in the vast majority of fraudulent calls. No method exists on the present-day phone network infrastructure to "authenticate" the caller ID that accompanies a call – i.e., prove that the person placing that call is authorized to use the displayed caller ID number. Although significant changes to the VoIP technologies will be required to make caller ID authentication a reality, the IETF continues to work on the issue, and the FTC strongly supports these efforts and stands ready to assist in any way possible.

Finally, the FTC is pursuing potential medium-term solutions identified in coordination with our many expert partners. For example, FTC staff has spearheaded a new working group of the London Action Plan International Do Not Call Forum to address caller ID spoofing from an international perspective, with an emphasis on law enforcement, policy, and technological solutions.[30] The FTC also has become actively involved in an industry-led working group to tackle technological issues contributing to telephony abuse – the Voice and Telephony Abuse

---

[29] The STIR working group involves members from government, major carriers, technology companies, and other subject-matter experts. IETF working groups are open to all who want to participate, and hold discussions on an open mailing list or at IETF meetings.

[30] The London Action Plan is comprised of government and public agencies, and anti-spam technologists from 27 countries that cooperate through law enforcement, training, information sharing, and educational initiatives to combat email and text message spam, viruses, do not call violations, and malware.

Special Interest Group ("VTA SIG") of the Messaging Malware Mobile Anti-Abuse Working Group ("M3AAWG").[31]

One of the approaches of particular interest that has emerged from Commission staff's work with experts around the world is the development of honeypots. Intelligence about illegal calls is currently limited, and a phone honeypot – i.e., an information system consisting of phone lines that are designed to attract malicious callers – can help experts and authorities understand and combat their tactics. The FTC launched such a honeypot in the fall of 2012, and since then we have been working with academics, industry, and law enforcement partners who are in various stages of creating their own honeypots. To further this promising work, the FTC will hold a contest at DEF CON 22 in August of this year,[32] offering prizes for insights about the design of robust, cutting-edge telephony honeypots. Information security specialists have used honeypots extensively, but we have seen limited overlap between their expertise and the efforts to fight phone scams. The FTC hopes to inspire some of the experts at DEF CON to apply their knowledge and creativity to create a next-gener-ou (-)Tj 0.eite12(een0.004 Tc 0.)-3(C)a0.004(ef)-1(e an) -0.