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 10 percent of all reported incidents, and consumers purchased fraudulent goods or services by telephone in 30 percent of reported incidents.[2]

Consumer complaints to the FTC tell a similar story: the FTC receives tens of thousands of complaints about illegal calls every week. A number of these complaints are about imposter scams that target seniors. In these scams, the caller pretends to be a friend or relative of the call

[2] Staff Report of the Bureau of Economics, FTC, *Consumer Fraud in the United States, 2011*, at i, 18-19, 33-40 (2013), http://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey_0.pdf.

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] These figures exclude Do Not Call registry and identity theft complaints.

To put the numbers set forth in the table numbers in context, during the same time period, complaints about imposter scams made up 4.9% of the total number of complaints the FTC received (excluding Do Not Call Registry complaints), and the total amount consumers reported losing in imposter scams was 5.8% of the total amount consumers reported as having been paid to fraudsters. Nonetheless, it is important to note that most consumers who are victims of frauds do not file complaints with the FTC, so the actual numbers of consumer victims and amounts lost in imposter scams will be higher than the amounts reflected in the FTC's complaint data.

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 litigation.[4]

Complementing these enforcement actions against the fraudsters, the FTC also has taken steps to cut off access to the money transfer services commonly used by perpetrators of imposter phone scams to obtain payments from consumers. For example, in 2009 the Commission reached a settlement with MoneyGram, which paid $18 million in restitution to settle the FTC's charges that it allowed telemarketers to bilk U.S. consumers out of tens of millions of dollars using its money transfer system.[5] Moreover, the FTC is currently investigating whether another

---

[4] *FTC v. Worldwide Info Services, Inc.*, No. 6:14-cv-8-ORL-28DAB (M.D. Fla. Jan. 6, 2014), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3175/worldwide-info-services-inc.

[5] *FTC v. MoneyGram Int'l, Inc.*, No. 1:09-cv-06576 (N.D. Ill. Oct. 19, 2009). The FTC charged that MoneyGram knew that its system was being used to defraud people but did very little about it. For example, the FTC alleged that MoneyGram knew, or avoided knowing, that about 131 of its more than 1,200 agents accounted for more than 95 percent of the fraud complaints MoneyGram received in 2008 regarding money transfers to Canada. The Commission further alleged that MoneyGram ignored warnings from law enforcement officials

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 network.[6] In addition to its enforcement efforts, the FTC has worked cooperatively with money transfer companies, reloadable prepaid card services, retailers, financial institutions, and other private sector entities on an informal, ongoing basis to improve their fraud-prevention practices.

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

---

and its own employees that widespread fraud was being conducted over its network, and even discouraged its employees from enforcing its own fraud prevention policies or taking action against suspicious or corrupt agents. *See* Press Release, FTC, *MoneyGram to Pay $18 Million to Settle FTC Charges That it Allowed its Money Transfer System To Be Used for Fraud* (Oct. 20, 2009), *available at* http://www.ftc.gov/news-events/press-releases/2009/10/moneygram-pay-18-million-settle-ftc-charges-it-allowed-its-money.

The Department of Justice subsequently negotiated a deferred prosecution agreement, pursuant to which MoneyGram paid an additional $100 million to victims of fraud. *See United States v. MoneyGram Int'l, Inc.*, No. 1:12-CR-00291, D.E. 3 (M.D. Pa. Nov. 9, 2012); *Pending Criminal Division Cases – United States v. MoneyGram International*, U.S. Dep't of Justice, http://www.justice.gov/criminal/vns/caseup/moneygram.html (last visited July 20, 2014). In addition, in 2008 forty-five state attorneys general entered into a $1.2 million multi-state settlement with MoneyGram. *See* Press Release, Office of the Vermont Attorney General, *Attorney General Announces $1.2 Million Settlement With MoneyGram* (July 2, 2008), *available at* http://www.atg.state.vt.us/news/attorney-general-announces-1.2-million-settlement-with-moneygram.php.

[6] *FTC v. The Western Union Co.*, No 13-3100, Brief of Appellant [D.E. #49] at 1 (2d Cir. Nov. 27, 2013) (filing in litigation to enforce FTC civil investigative demand served on Western Union). In 2005, forty-eight state attorney generals entered into a $8.1 million multi-state settlement with Western Union to resolve charges that the company failed to take steps to stop fraudsters from using its money transfer system to defraud consumers. *See* Press Release, Office of the Vermont Attorney General, *Western Union Enters Into Settlement With Attorneys General* (Nov. 14, 2005), *available at* http://www.atg.state.vt.us/news/western-union-enters-into-settlement-with-attorneys-general.php.

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]

C. Impersonating Businesses

The FTC also targets fraudsters that impersonate legitimate companies in an attempt to steal consumers' money.[10] For example, the FTC brought a series of cases against telemarketers operating overseas whom the agency alleged were calling consumers and falsely claiming an affiliation with major computer or Internet security companies.[11] The FTC charged that the telemarketers in these cases falsely claimed that consumers' computers were riddled with viruses and malware and then offered to "fix" these non-existent problems for several hundred dollars.

---

[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.*, 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] *FTC v. Broadway Global Master, Inc.*, No. 2:12-CV-00855-JAM-GGH (E.D. Cal. Apr. 3, 2012), *available at* http://www.ftc.gov/enforcement/cases-proceedings/1123215/broadway-global-master-inc-also-dba-bgm-et-al.

[9] The district court stayed the FTC's civil action in *Broadway Global* due to the subsequent criminal indictment of Mr. Patel. *Id.*, D.E. 48 (Sept. 12, 2012).

The FTC's actions resulted in federal court orders permanently halting these schemes and freezing the perpetrators' assets.

D. Coordinating with Criminal Law Enforcement

The Commission, through its Criminal Liaison Unit ("CLU"), coordinates extensively with criminal law enforcement agencies in combatting phone scams, including referring perpetrators of phone scams to criminal law enforcement authorities for prosecution.[12] Since the

---

[10] *See, e.g.*, *FTC v. AFD Advisors, LLC*, No. 13-CV-6420 (N.D. Ill. Sept. 9, 2013) (alleging defendants pretended to be affiliated with medical insurance providers in addition to government entities) *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3138-x130058/afd-advisors-llc; *FTC v. A+ Fin. Ctr., LLC*, No. 2:12-CV-14373-DLG (S.D. Fla. Oct. 23, 2012) (alleging defendants implied an affiliation with consumer's bank or credit card company), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3197/financial-center-llc; *FTC v. Universal Premium Servs., Inc.*, No. 2:06-CV-00849-GW-OP (C.D. Cal. Feb. 14, 2006) (alleging defendants impersonated gasoline companies, government entities, financial institutions, and well-known retailers such as Wal-Mart and Home Depot), *available at* http://www.ftc.gov/enforcement/cases-proceedings/052-3153/universal-premium-services-inc-also-known-premier-benefits.

[11] *FTC v. Pecon Software Ltd.*, No. 12-CV-7186 (S.D.N.Y. Sept. 24, 2012), *available at* http://www.ftc.gov/enforcement/cases-proceedings/1123118/pecon-software-ltd-et-al; *FTC v. Marczak*, No. 12-CV-7192 (S.D.N.Y. Sept. 24, 2012), *available at* http://www.ftc.gov/enforcement/cases-proceedings/1223246/virtual-pc-solutions-mikael-marczak-aka-michael-marczak-et-al; *FTC v. Finmaestros, LLC*, No. 12-CV-7195 (S.D.N.Y. Sept. 24, 2012), *available at* http://www.ftc.gov/enforcement/cases-proceedings/1223247/finmaestros-llc-et-al; *FTC v. Lakshmi Infosoul Servs. Pvt Ltd.*, No. 12-CV-7191 (S.D.N.Y. Sept. 24, 2012), *available at* http://www.ftc.gov/enforcement/cases-proceedings/1223245/lakshmi-infosoul-services-pvt-ltd; *FTC v. PCCare247 Inc.*, No. 12-CV-7189 (S.D.N.Y. Sept. 24, 2012), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3243-x120057/pccare247-inc-et-al.

[12] In the *Broadway Global* case, the CLU referred the principal of the scheme, Kirit Patel, for criminal prosecution. A grand jury subsequently indicted Mr. Patel on 21 criminal counts of wire fraud and mail fraud. *See* Press Release, FTC, *California Man Previously Sued by FTC Is Indicted on Criminal Charges for Phony Debt Collection Scam* (Aug. 27, 2012), *available at* http://www.ftc.gov/news-events/press-releases/2012/08/california-man-previously-sued-ftc-indicted-criminal-charges. The trial is scheduled to begin October 20, 2014. *United States. v. Patel*, 2:12-cr-00306-JAM, D.E. 46 (E.D. Cal. June 24, 2014).

creation of the CLU in 2003, hundreds of fraudulent telemarketers have faced criminal charges and prison time as a result of FTC referrals.

Given the cross-border nature of phone fraud, the Commission also partners with foreign agencies to combat phone scams. For example, the Commission is a member of the Centre of Operations Linked to Telemarketing Fraud ("Project COLT"), a joint operation involving U.S. and Canadian agencies to combat cross-border telemarketing fraud.[13] Through its participation in Project COLT, the FTC coordinates law enforcement efforts and receives and shares intelligence relating to phone scams with Canadian authorities. The FTC's involvement in Project COLT has resulted in at least ten recent indictments of individuals involved in grandparent[14] and other types of telemarketing scams.[15] In connection with Project COLT, the 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.

---

[13] Project COLT members include the Royal Canadian Mounted Police, Sureté du Québec, Service de Police de la Ville de Montréal, Canada Border Services Agency, Competition Bureau of Canada, Canada Post, U.S. Homeland Security (U.S. Immigration and Customs Enforcement and the U.S. Secret Service), the U.S. Postal Inspection Service, the FTC, and the FBI.

[14] *See, e.g., U.S. v. Kirstein, Buchan, El Bernachawy, Iacino, & Kamaldin*, No. CR 13 00469 (C.D. Cal. July 9, 2013); Press Release, FBI, *Alleged Operator of "Grandparent 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.

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]

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

---

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

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]

In addition to providing guidance about phone scams relevant to all consumers, the FTC recently created Pass It On, an innovative education effort aimed at active, older adults. Pass It On seeks to arm older people with information that they can "pass on" to family and friends who might need it. The materials and videos available at www.ftc.gov/PassItOn are direct and to the point, with a friendly and respectful tone informed by research about the target community's

---

[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-alert-systems.

[21] *See Government Imposter Scams*, FTC, http://www.consumer.ftc.gov/articles/0048-government-imposter-scams (last visited July 10, 2014); *Government Imposter Scams*, FTC, http://www.consumer.ftc.gov/media/audio-0053-government-imposter-scams (last visited July 10, 2014); Amy Hebert, *Scammers Continuing to Pose as IRS Agents*, FTC (May 29, 2014), http://www.consumer.ftc.gov/blog/scammers-continuing-pose-irs-agents; Lisa Lake, *Fake IRS Collectors Are Calling*, FTC (Apr. 7, 2014), http://www.consumer.ftc.gov/blog/fake-irs-collectors-are-calling.

preferences. The materials cover topics such as imposter and health care scams, charity fraud, and identity theft,[22] all of which are available in print in both English and Spanish.

The Commission seeks to reach older adults through the facilities where they gather or live: libraries, social and civic clubs, senior centers, adult living communities, and veterans' facilities. The FTC recently mailed information to three thousand such facilities and within three days had orders from around the country for more than two thousand copies of the Pass It On printed materials. This confirmed the demand for clear, friendly, respectful education materials for older Americans. The Commission looks forward to sharing these materials with public and private sector organizations.

The Pass It On resource works hand-in-hand with other outreach and coordination activities that have been crucial to the FTC's efforts on behalf of older people. For instance, we work extensively with the Elder Justice Coordinating Council to identify cross-agency initiatives to protect seniors from abuse, neglect, and exploitation, and other crimes.[23] The Commission also entered into an innovative program with the AARP Foundation in 2012. As part of the program, the FTC refers for individual peer counseling consumers over the age of 60 who have called the FTC's Consumer Response Center to complain that they have been victims of certain

---

[22] The FTC's Pass It On materials include a folder containing one-page articles and bookmarks that explain, in easy-to-understand terminology, how six of the most popular scams work and steps consumers can take to avoid falling victim to these schemes.

[23] The Secretary of the Department of Health and Human Services ("DHHS") convened the Elder Justice Coordinating Council in accordance with the Elder Justice Act of 2009. The Council consists of heads of federal departments and other government entities, including the FTC, identified as having responsibilities, or administering programs, relating to elder abuse, neglect, and exploitation. The Council's mission is to develop recommendations to the DHHS Secretary for the coordination of relevant activities. *See* Elder Justice Coordinating Council, *Facts*, http://www.ltcombudsman.org/sites/default/files/norc/elder-justice-coordinating-council-factsheet.pdf (last visited July 10, 2014).

frauds, including lottery, prize promotion, and grandparent scams.[24] Last year, the AARP Foundation peer counselors successfully communicated with more than a thousand people referred by the FTC, providing one-on-one advice and guidance to consumers to help them avoid future fraud.[25]

III. Policy and Technology Initiatives

In addition to the FTC's law enforcement and outreach efforts, the agency is heavily involved in exploring and addressing technological issues that have facilitated the proliferation of fraudulent calls. The convergence between our phone system and the Internet has made phone fraud easier and created significant challenges in the investigation of these scams. In today's world of Voice over Internet Protocol ("VoIP") technology, it is not only much cheaper to send fraudulent calls; it is also easier to hide one's identity when doing so.[26]

First, the typical call now takes a complex path, traversing the networks of multiple different VoIP and legacy carriers before reaching the end user. Each of these carriers can identify which carrier passed a particular phone call onto its network, but likely knows little else about the origin of the call. Such a path makes it difficult to trace a call back to its inception. In fact, tracing the call often fails because one of the carriers in the chain has not retained the

---

[24] The FTC only refers consumers who have consented to being contacted by the AARP.

[25] The consumers from whom the Foundation gathered data reported having lost more than $15 million.

[26] *See* Prepared Statement of the Federal Trade Commission, *Stopping Fraudulent Robocall Scams: Can More Be Done?* at 10-17 (July 10, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-entitled-%E2%80%9Cstopping-fraudulent-robocall-scams-can-more-be/130710robocallstatement.pdf; *Robocalls All the Rage: An FTC Summit*, FTC, http://www.ftc.gov/bcp/workshops/robocalls (last visited July 10, 2014); *How Does a Robocall Work?*, FTC, http://www.consumer.ftc.gov/sites/default/files/pictures/0381-robocalls-infographic.png (last visited July 10, 2014).

records that would further an investigation. Alternatively, the process often fails to identify a perpetrator because calls can be initiated using web-based dialing software using difficult to trace payment methods, or "burner" cell phones and SIM cards that are active only for a few days and then replaced.

Second, new technologies allow callers to manipulate the caller ID information that appears with an incoming phone call. Such "caller ID spoofing" allows scammers to deceive consumers by pretending to be an entity with a local phone number or a trusted institution such as a bank or government agency. In addition, fraudsters can change their phone numbers frequently in an attempt to avoid detection.

Finally, new technologies help fraudsters operate outside the jurisdiction where they are most likely to face prosecution and move around frequently to any location in the world with an Internet connection. Indeed, all of the many different entities and companies involved in the 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 solutions to fight phone scams. As one example, the Commission held its first public contest to spur American innovators and entrepreneurs into developing short-term solutions that could help consumers block illegal calls. The 2012 "Robocall Challenge," hosted on the challenge.gov platform, offered a $50,000 prize to the individual or small team that could propose the best call-blocking solution – *i.e.*, a spam filter for the phone.[27]

---

[27] *See* Press Release, FTC, *FTC Challenges Innovators To Do Battle With Robocallers* (Oct. 18, 2012), *available at* http://www.ftc.gov/news-events/press-releases/2012/10/ftc-challenges-innovators-do-battle-robocallers.

The FTC received 798 eligible submissions, many of which were extremely sophisticated technical proposals. As a result of the Challenge, a wide array of people with technical expertise spent countless hours working on these issues; in fact, all of the winning proposals were submitted by people who had never previously worked on the problem of illegal calls. In addition, the Challenge received overwhelming public attention and interest, helping the FTC spread the word about the steps consumers can take to fight, and prevent, illegal calls. Finally, less than six months after the Commission announced the challenge winners, one of the winners launched a new product that reportedly has already blocked more than five million unwanted calls for U.S. consumers.[28] While the FTC does not endorse any products or services, we are gratified that the Challenge stimulated the marketplace to develop innovative solutions.

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

---

[28] *See* www.nomorobo.com.

[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.

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 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

[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.

[31] Participants in M3AAWG VTA SIG include academics, law enforcers and regulators from the U.S. and Canada; the major U.S. and Canadian carriers; entrepreneurs with smaller technology companies; and other experts.

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-generation honeypot, or perhaps even to join the growing international community of experts fighting fraudulent and unwanted calls.

IV. Conclusion

The Commission will continue its battle to protect consumers from phone scams and looks forward to working with the Committee on this important issue.

[32] DEF CON is one of the largest annual conferences of experts in computer technology.