Prepared Statement of
The Federal Trade Commission

Before the
United States Senate
Committee on Commerce, Science and Transportation
Subcommittee on Consumer Protection, Product Safety, and Insurance

on

Stopping Fraudulent Robocall Scams: Can More Be Done?

Washington, DC
July 10, 2013

Chairman McCaskill, Ranking Member Heller, and members of the Subcommittee, 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 discuss the Commission's initiatives to fight illegal robocalls.

In 2003, the FTC responded to enormous public frustration with unsolicited sales calls and amended the Telemarketing Sales Rule ("TSR") to create a national Do Not Call Registry.[2] The Registry, which currently includes more than 221 million telephone numbers,[3] has been tremendously successful in protecting consumers' privacy from the unwanted calls of tens of thousands[4] of legitimate telemarketers who participate in the Registry each year.[5] More recently, changes in technology led to a new source of immense frustration – the blasting of prerecorded messages using Voice over Internet Protocol ("VoIP") technology.[6] In 2008, the Commission

---

[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.

[2] 68 Fed. Reg. 4580 (Jan. 29, 2003); 16 C.F.R. Part 310. The FTC issued the TSR pursuant to the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101-6108.

[3] *See* Appendix A, National Do Not Call Registry Active Registrations and Complaint Figures.

[4] For example, in fiscal year 2012, more than 28,000 telemarketers accessed the Do Not Call Registry. National Do Not Call Registry Data Book FY 2012 at 8 (Oct. 2012), *available at* http://www.ftc.gov/os/2012/10/1210dnc-databook.pdf.

[5] Humorist Dave Barry called the Do Not Call Registry "the most popular federal concept since the Elvis stamp." *See* Dave Barry, *Idea for telemarketers: Hang up and go away*, DESERET NEWS, Aug. 31, 2003, *available at* http://www.deseretnews.com/article/1006979/Idea-for-telemarketers-Hang-up-and-go-away.html.

responded by amending the TSR to address this problem, prohibiting the vast majority of prerecorded sales calls unless the recipient has provided express written consent to receive them.[7]

Illegal robocalls are still a significant consumer protection problem today, because they repeatedly disturb consumers' privacy and many of them peddle fraudulent goods and services that cause significant economic harm. Therefore, the FTC is using every tool at its disposal to fight them.[8] This testimony describes the Commission's efforts to stop telemarketer violations, including our aggressive law enforcement, initiatives to spur technological solutions, and broad consumer and business outreach.

I. Do Not Call and Robocall Law Enforcement

Since the Do Not Call Registry was established in 2003,[9] the Commission has fought vigorously to protect consumers' privacy from unwanted calls. Indeed, two weeks ago on the

---

[6] *See* Section II(A), *infra*.

[7] 73 Fed. Reg. 51164 (Aug. 29, 2008); 16 C.F.R. Part 310.4(b)(1)(v). The FTC had already brought robocall-related enforcement actions prior to 2008, alleging that defendants made illegal "abandoned calls," because their robocalls did not "connect the call to a sales representative within two seconds of the completed greeting of the person who answer[ed]." 16 C.F.R. Part 310.4(b)(1)(iv). Any telemarketing campaign consisting solely of prerecorded messages would always violate that provision, and would not meet the abandoned call safe harbor requirements under the TSR. *See* 16 C.F.R. Part 310.4(b)(4). Nonetheless, the Commission amended the TSR to explicitly prohibit unsolicited robocalls, considering it beneficial to make the prohibition more prominent.

[8] *See* FTC Robocall Action Plan, http://www.ftc.gov/robocalls.

[9] In 2003, two different district courts issued rulings enjoining the Do Not Call Registry. *See* Press Release, FTC Files Motion to Stay Pending Appeal in Oklahoma DNC Ruling (Mar. 24, 2003), *available at* http://www.ftc.gov/opa/2003/09/dncok.shtm; Press Release, Statement of FTC Chairman Timothy J. Muris (Sept. 26, 2003), *available at* http://www.ftc.gov/opa/2003/09/dnc030926.shtm. Congress addressed the first decision in summary fashion by enacting HR 3161 in one day. *See* "HR 3161 (108th) Do-Not-Call-Registry bill," http://www.govtrack.us/congress/bills/108/hr3161; Press Release, Statement of FTC Chairman Timothy J. Muris (Sept. 25, 2003), *available at*

10th anniversary of the Do Not Call Program, the Commission announced that Mortgage Investors Corporation, one of the nation's leading refinancers of veterans' home loans, will pay $7.5 million, the largest Do Not Call fine the FTC has ever collected.[10] This case is the 105th enforcement action since the Commission began enforcing the Do Not Call provisions of the TSR in 2004.[11] Through these enforcement actions, the Commission has sought civil penalties,[12] restitution for victims of telemarketing scams, and disgorgement of ill-gotten gains from the 298 companies and 234 individuals involved. Although a number of cases remain in litigation, the 81 cases that have concluded thus far have resulted in orders totaling more than $126 million in civil penalties and $741 million in redress or disgorgement. In the first several years of the Registry's existence, consumers reported that the Do Not Call program was highly effective in reducing the number of unwanted telemarketing calls they received.[13]

---

http://www.ftc.gov/opa/2003/09/dnc030926.shtm. The 10th Circuit reversed the second district court decision on February 17, 2004. *See* Press Release, Appeals Court Upholds Constitutionality of National Do Not Call Registry (Feb. 17, 2004), *available at* http://www.ftc.gov/opa/2004/02/dncappeal.shtm.

[10] *See* Press Release, Mortgage Broker Targeting U.S. Servicemembers Will Pay Record $7.5 Million to Settle Alleged Telemarketing Violations (June 27, 2013), *available at* http://www.ftc.gov/opa/2013/06/donotcall.shtm.

[11] The 105 Do Not Call actions include cases that involve the rule provisions prohibiting unauthorized robocalls, which also invade consumers' privacy and may be deceptive as well.

[12] As is true of for all TSR violations, telemarketers who violate the Do Not Call provisions are subject to civil penalties of up to $16,000 per violation. 15 U.S.C. § 45(m)(1)(A); 16 C.F.R. 1.98(d).

[13] For example, in October 2007, an independent study by Harris Interactive® found that of the 72% of Americans who had registered their telephone numbers for the Do Not Call Registry, 18% reported that they currently received no telemarketing calls, 59% reported that they still received some, but far fewer than before they signed onto the Registry, and 14% said they received some, but a little less than before they registered. Previous surveys had similar results. *See* Annual Report to Congress for FY 2007 Pursuant to the Do-Not-Call

On September 1, 2009, new TSR provisions went into effect prohibiting the vast majority of sales robocalls,[14] unless the telemarketer has the consumer's prior written authorization to transmit such calls.[15] The robocall provisions cover prerecorded calls to all consumers, including those who have not registered their phone number on the Do Not Call Registry. The Commission has been aggressive in enforcing prohibitions on robocalls, bringing 34 cases involving illegal prerecorded calls against 97 companies and 77 individuals.[16] These actions have shut down entities responsible for *billions* of illegal robocalls, and the 22 cases that have concluded thus far have resulted in orders totaling more than $51 million in civil penalties and $202 million in redress or disgorgement. Some of the Commission's early robocall cases were against companies with household names such as Dish Network, DIRECTV, and Talbots.[17]

Yet increasingly, robocalls that plague consumers are initiated by fraudsters, who often hide out in other countries in an attempt to escape detection and punishment. One example is the

---

Implementation Act on Implementation of the National Do Not Call Registry, at 4-5, n.10 (July 2008), *available at* http://www.ftc.gov/os/2008/07/P034305FY0dncreport.pdf.

[14] Like the other provisions of the TSR, the robocall provisions do not apply to non-sales calls, such as calls placed by charities or those that are pure political, informational, or survey calls. *See generally* "Complying with the Telemarketing Sales Rule" (Feb. 2011), *available at* http://business.ftc.gov/documents/bus27-complying-telemarketing-sales-rule.

[15] 16 C.F.R. Part 310.4(b)(1)(v). Limited exceptions exist for calls that deliver a healthcare message made by an entity covered by the Health Insurance Portability and Accountability Act, 16 C.F.R. Part 310.4(b)(1)(v)(D), and for certain calls placed by telemarketers who solicit charitable contributions, 16 C.F.R. Part 310.4(b)(1)(v)(B).

[16] The FTC filed 12 of the 34 cases before the rule change went into effect on September 1, 2009.

[17] *See U.S. v. The Talbots, Inc*., No. 10-cv-10698 (D. Mass. Apr. 27, 2010), *available at* http://www.ftc.gov/opa/2010/04/talbots.shtm; *U.S. v. Dish Network, LLC*, No. 3:09-cv-03073 (C.D. Ill. Feb. 4, 2010), *available at* http://www.ftc.gov/opa/2009/03/echostar.shtm; *U.S. v. DIRECTV, Inc*., No. 09-02605 (C.D. Cal. Apr. 23, 2009), *available at* http://www.ftc.gov/opa/2009/04/directv.shtm.

defendants in *FTC v. Navestad*, who the Commission successfully traced and sued even after they attempted to hide their identities through fake caller IDs, shifting foreign operations, and name changes. The court found that the defendants made in excess of eight million robocalls, and ordered them to pay $30 million in civil penalties and give up more than $1.1 million in ill-gotten gains.[18] Unfortunately, the two defendants are currently in hiding overseas.

A. Coordination with Law Enforcement Partners

1. State, Federal, and International Coordination

As the law enforcement challenges associated with illegal telemarketing have increased, the FTC's relationships with other agencies have become ever more important. The Commission has robust collaborative relationships with state law enforcers, including through the National Association of Attorneys General Do Not Call working group. In addition, the FTC regularly works with the Federal Communications Commission ("FCC"), the Department of Justice, the U.S. Postal Inspection Service, and U.S. Attorneys' Offices across the country. The Commission also coordinates with its counterparts in other countries on particular cases and broader strategic matters such as caller ID "spoofing" – the practice of faking a call's identifying information.

The FTC's collaboration with its partners takes many different forms, including sharing information and targets, assisting with investigations, and working together on long-term policy initiatives. The agency also coordinates with various partners to bring law enforcement "sweeps" – multiple simultaneous law enforcement actions – that focus on specific types of telemarketing fraud.[19] One recent example is a concerted attack on illegal robocalls purporting

---

[18] *FTC v. Navestad*, No. 09-CV-6329 (W.D.N.Y. Mar. 23, 2012), *available at* http://www.ftc.gov/opa/2012/04/cashgrant.shtm.

[19] The following describe some of the telemarketing and robocall sweeps that the FTC and its law enforcement partners have conducted over the past several years: Press Release, FTC Leads Joint Law Enforcement Effort Against Companies that Allegedly Made Deceptive

to be from "Rachel" or others from "Cardholder Services," which pitch a supposedly easy way to save money by reducing consumers' credit card interest rates. The FTC brought five cases against companies that were allegedly responsible for millions of these illegal calls. The Commission simultaneously announced that state law enforcement partners in Arizona, Arkansas, and Florida had filed separate law enforcement actions as part of the same sweep.[20]

2. Referrals for Criminal Prosecution

Although the Commission does not have criminal law enforcement authority, it recognizes the importance of criminal prosecution in deterrence. Accordingly, the Commission routinely works with federal and state criminal law enforcers through its Criminal Liaison Unit ("CLU"). Since CLU's launch in 2003, hundreds of fraudulent telemarketers have found themselves facing criminal charges and prison time. One example is the *Voice Touch* case, which involved the use of robocalls to advertise an auto warranty scam. The FTC case shut down the scam and resulted in almost $3.2 million in redress to consumers,[21] and the Office of

---

"Cardholder Services" Robocalls (Nov. 1, 2012), *available at* http://www.ftc.gov/opa/2012/11/robocalls.shtm; Press Release, FTC Settlements Put Debt Relief Operations Out of Business (May 26, 2011), *available at* http://www.ftc.gov/opa/2011/05/amsdynamic.shtm; Press Release, FTC Sues to Stop Robocalls with Deceptive Credit Card Interest-Rate Reduction Claims (Dec. 8, 2009), *available at* http://www.ftc.gov/opa/2009/12/robocall.shtm; Press Release, FTC Cracks Down on Scammers Trying to Take Advantage of the Economic Downturn (July 1, 2009), *available at* http://www.ftc.gov/opa/2009/07/shortchange.shtm; Press Release, FTC Announces "Operation Tele-PHONEY," Agency's Largest Telemarketing Sweep (May 20, 2008), *available at* http://www.ftc.gov/opa/2008/05/telephoney.shtm.

[20] *See* Press Release, FTC Leads Joint Law Enforcement Effort Against Companies that Allegedly Made Deceptive "Cardholder Services" Robocalls (Nov. 1, 2012), *available at* http://www.ftc.gov/opa/2012/11/robocalls.shtm.

[21] Press Release, FTC Returns Almost $3.2 Million to Auto Warranty Robocall Victims (Aug. 31, 2011), *available at* http://www.ftc.gov/opa/2011/08/voicetouch.shtm; *FTC v. Voice Touch, Inc.*, No. 09CV2929 (N.D. Ill. Aug. 23, 2010), *available at* http://www.ftc.gov/os/caselist/0823263.

the U.S. Attorney for the Southern District of Illinois subsequently brought criminal charges. Three of the fraud's principals have pleaded guilty and gone to prison, with the two leaders of the scheme each sentenced to five years.[22]

Another example is Kara Singleton Adams, the leader of a scam that used robocalls to sell worthless credit card interest rate reduction services. Not only did the Commission act to shut down the operation,[23] a federal jury in Atlanta subsequently convicted Adams on charges of wire fraud and conspiracy, among other things. In 2012, the court sentenced her to more than 17 years' imprisonment. Three of her associates in the scheme also went to prison.[24]

B. Strategic Targeting for Maximum Impact

The Commission constantly seeks innovative ways to maximize its resources and its impact on those responsible for illegal robocalls.[25] Often, telemarketers' deceptive and abusive practices are facilitated by third parties, such as auto-dialers, which provide the software needed to blast out millions of calls, and payment processors, which enable fraudulent telemarketers to reach into consumers' bank accounts. The FTC has increasingly targeted gatekeepers that have

---

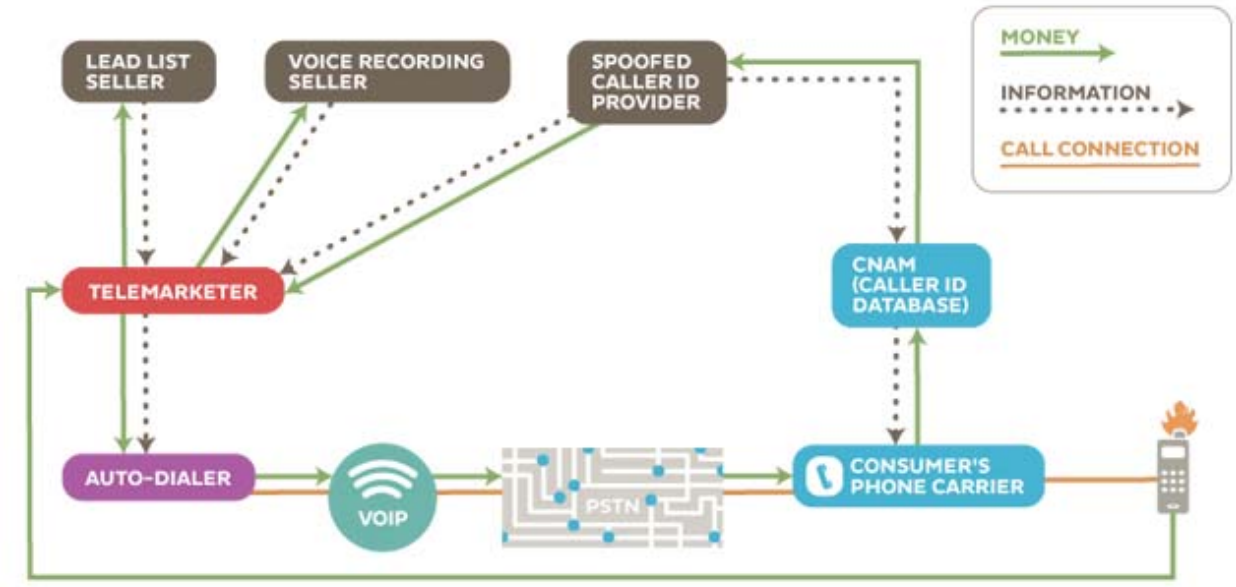
[22] Department of Justice ("DOJ") Press Release, "Auto Warranty" Telemarketer Pleads Guilty (June 15, 2012), *available at* http://www.justice.gov/usao/ils/News/2012/Jun/06152012_Dolan%20Press%20Release.html; DOJ Press Release, Update on Transcontinental Warranty Case (Oct. 31, 2011), *available at* http://www.justice.gov/usao/ils/Programs/VWA/transcontinental.html.

[23] *FTC v. Econ. Relief Techs., LLC*, No. 09-CV-3347 (N.D. Ga. July 22, 2010), *available at* http://www.ftc.gov/os/caselist/0923118.

[24] DOJ Press Release, 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.

[25] As an example, the FTC recently created a robocall "honeypot," which is a group of phone numbers from around the country that the Commission controls, permitting it to receive robocalls directly. This allows the Staff to quickly amass information about who is making the calls and to have recordings in-house, thus facilitating a more rapid law enforcement response.

tended to service large numbers of rogue telemarketers and therefore offer a way to strike a blow to many law-breakers with only one case.



Money flows in many directions within a robocall operation.[26]

First, the Commission aggressively pursues companies that provide the equipment and software necessary to send out millions of calls, sometimes referred to as "voice broadcasters" or "autodialers."[27] One example is *FTC v. Asia Pacific Telecom, Inc.*, in which the FTC alleged that defendants were responsible for violating the TSR by placing billions of prerecorded phone

[26] The PSTN is the "Public Switched Telephone Network." It consists of transmission facilities (e.g., phone lines, fiber optic cables, microwave transmission links, cellular radios, communication satellites, etc.) and switching facilities (central office switches, databases for 800 number translation, gear for cellular handoffs, multiplexors, etc.).

[27] *U.S. v. Skyy Consulting, Inc., also d/b/a CallFire*, No. 13-CV-2136 (N.D. Cal. May 14, 2013), *available at* http://www.ftc.gov/os/caselist/1223011; *FTC v. Asia Pac. Telecom, Inc.*, No. 1:10-3168 (N.D. Ill. Mar. 28, 2012), *available at* http://www.ftc.gov/os/caselist/1023060; *U.S. v. Brian Ebersole*, No. 3:12-cv-00105 (D. Nev. Feb. 29, 2012), *available at* http://ftc.gov/os/caselist/0923174; *U.S. v. Sonkei Commc'ns*, No. SACV11-1777 (C.D. Cal. Nov. 22, 2011), *available at* http://ftc.gov/os/caselist/1123060; *U.S. v. Voice-Mail Broad. Corp.*, No. cv-08-00521 (C.D. Cal. Jan. 29, 2008), *available at* http://www.ftc.gov/os/caselist/0523182; *U.S. v. The Broadcast Team, Inc.*, No. 6:05-cv-01920 (M.D. Fla. Feb. 2, 2007), *available at* http://www.ftc.gov/os/caselist/0523025/0523025.shtm.

calls on behalf of unscrupulous telemarketers. These robocalls pitched worthless extended auto warranties and credit card interest rate reduction programs while using spoofed Caller ID names – such as "SALES DEPT" – and phone numbers registered to companies with overseas offices in the Northern Mariana Islands, Hong Kong, and the Netherlands. In 2012, the Commission reached a settlement under which the defendants are banned from all telemarketing, from misrepresenting any good or service, and from selling or otherwise benefitting from customers' personal information. The order imposed a $5.3 million judgment that was suspended, based on the defendants' inability to pay, after they had surrendered assets valued at approximately $3 million.[28]

Second, the FTC has increasingly taken action against payment processors when they assist and facilitate telemarketers engaged in deceptive practices, providing access to the financial system and, in turn, consumers' money.[29] Two amended complaints the FTC filed in June provide examples of the agency's enforcement in this area. In both cases, the Commission sued telemarketing operations allegedly peddling bogus credit card interest rate reduction services. After obtaining temporary restraining orders against the defendants and beginning discovery, the FTC moved to amend both complaints to include the defendants' payment processors. The Commission alleges that the payment processors knew, or consciously avoided

---

[28] *FTC v. Asia Pac. Telecom, Inc.*, No. 1:10-3168 (N.D. Ill. Mar. 28, 2012), *available at* http://www.ftc.gov/os/caselist/1023060. The full judgment will become due immediately if the defendants are found to have misrepresented their financial condition.

[29] *See, e.g.*, *FTC v. Automated Elec. Checking, Inc.*, No. 3:13-cv-00056 (D. Nev. Mar. 13, 2013), *available at* http://ftc.gov/os/caselist/1223102; *FTC v. Landmark Clearing, Inc.*, No. 4:11-cv-00826 (E.D. Tex. June 27, 2013), *available at* http://www.ftc.gov/os/caselist/1123117.

knowing, key facts about the illegal telemarketing,[30] and chose to continue profiting from the illegal activity by processing consumers' payments to the original defendants.[31]

In sum, the Commission seeks to identify and attack chokepoints for illegal telemarketing.

II. Policy and Market Stimulation Initiatives

Despite the 2008 prohibition of unauthorized robocalls and the Commission's vigorous enforcement efforts, technological advances have permitted law-breakers to continue to profit from illegal robocall campaigns. In the fourth quarter of 2009, the FTC received about 63,000 complaints about illegal robocalls each month.[32] That number ballooned in three years, to an average of approximately 200,000 complaints per month in the fourth quarter of 2012.[33]

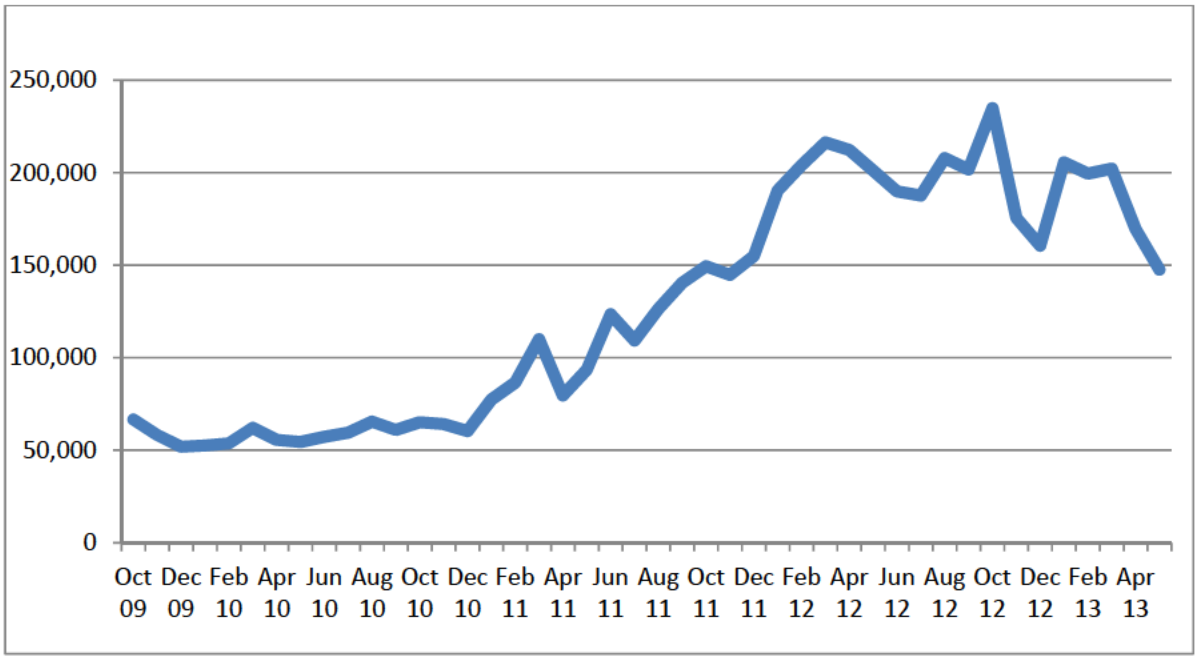
---

[30] 16 C.F.R. Part 310.3(b).

[31] *FTC v. Innovative Wealth Builders, Inc.*, No. 13-cv-00123 (M.D. Fla. June 5, 2013), *available at* http://www.ftc.gov/os/caselist/1223127; *FTC v. WV Universal Mgmt., LLC*, No. 6:12-CV-1618 (M.D. Fla. June 21, 2013), *available at* http://www.ftc.gov/os/caselist/1223190.

[32] National Do Not Call Registry Data Book FY 2010 at 5 (Nov. 2010), *available at* http://www.ftc.gov/os/2010/12/101206dncdatabook.pdf. Since that time, the FTC began separately tracking Do Not Call complaints and robocall complaints based on information provided by the consumer.

[33] National Do Not Call Registry Data Book FY 2012 at 5 (Oct. 2012), *available at* http://www.ftc.gov/os/2012/10/1210dnc-databook.pdf.



Number of robocall complaints filed with the FTC each month[34]

The public's anger has increased with the number of illegal robocalls.[35] Robocalls propagate harmful frauds; indeed, the estimated consumer harm associated with the 22 FTC lawsuits against robocallers that have concluded thus far amounts to more than $202 million.[36] Illegal

---

[34] While this chart suggests recent positive trending of self-reported complaints, it has in no way diminished the Commission's law enforcement efforts.

[35] *See generally* FTC Workshop, *Robocalls: All the Rage* (Oct. 18, 2012). A webcast of the workshop, a transcript of the event, PowerPoint presentations, and other related materials are available at http://www.ftc.gov/bcp/workshops/robocalls. References to the workshop transcript ("Tr.") identify the speaker and the transcript page. *See, e.g.,* Zoeller, Tr. at 86-87; Bash, Tr. at 88-89; Maxson, Tr. at 89-90.

[36] This estimate is based on the FTC's equitable monetary relief awards, and excludes civil penalties ordered in the same cases. In addition, it only includes cases that involved robocalls. The estimated consumer harm associated with the FTC's 81 concluded Do Not Call actions amounts to more than $741 million.

robocalls also have a significant impact on quality of life by repeatedly invading the privacy and peace of consumers' homes.[37]

A. Coordinating with Technical Experts, Industry, and Other Stakeholders

Convinced that law enforcement alone is not enough to solve the problem, FTC Staff has aggressively sought new strategies in ongoing discussions with academic experts, telecommunications carriers, industry coordinating bodies, technology and security companies, consumers, and counterparts at federal, state, and international government bodies. To that end, on October 18, 2012, the Commission hosted a public summit on robocalls to explore these issues (the "Robocall Summit").[38]

The Robocall Summit made clear that convergence between the legacy telephone system and the Internet has given rise to massive, unlawful robocall campaigns. The telephone network has its origins in a manual switchboard that allowed a human operator to make connections between two known entities.[39] A small group of well-known carriers were in control and were highly regulated.[40] Placing calls took significant time and money, and callers could not easily conceal their identities.[41]

Now, communications technology is universal and standardized such that entrepreneurs

---

[37] *See, e.g.*, Maxson, Tr. at 90-92; Zoeller, Tr. at 86-88; *see also* FTC, *Robocall Challenge Comments* [hereinafter *Public Comment*], *available at* http://www.ftc.gov/os/comments/robocallchallenge; Michelle Block, *Public Comment*, cmt. #565017-00015, at 1 (explaining how robocalls can cause her to lose desired assignments as a substitute teacher).

[38] *See generally* FTC Workshop, *Robocalls: All the Rage* (Oct. 18, 2012), http://www.ftc.gov/bcp/workshops/robocalls.

[39] Bellovin, Tr. at 12.

[40] Schulzrinne, Tr. at 22; Rupy, Tr. at 46-47; Diggs, Tr. at 55.

[41] Bellovin, Tr. at 12-17.

can build up a viable telephone services business wherever they find an Internet connection.[42] As a result, the number of service providers has grown exponentially and now includes thousands of small companies all over the world.[43] In addition, VoIP technology allows consumers to enjoy high-quality phone calls with people on the other side of the planet for an affordable price.[44] With this efficiency came other changes: instead of a voice path between one wire pair, the call travels as data; identifying information can be spoofed; many different players are involved in the path of a single call; and the distance between the endpoints is not particularly important.[45] As a result, it is not only much cheaper to blast out robocalls; it is also easier to hide one's identity when doing so.

1. New Technologies Have Made Robocalls Extremely Inexpensive

Until recently, telemarketing required significant capital investment in specialized hardware and labor.[46] Now, robocallers benefit from automated dialing technology, inexpensive long distance calling rates, and the ability to move internationally and employ cheap labor.[47] The only necessary equipment is a computer connected to the Internet.[48] The result is that law-breaking telemarketers can place robocalls for less than one cent per minute.[49] In addition, the

---

42 Herrman, Tr. at 60-61; Maxson, Tr. at 96.

43 Schulzrinne, Tr. at 22.

44 *See, e.g.*, Bellovin, Tr. at 16-17.

45 *Id*. at 17.

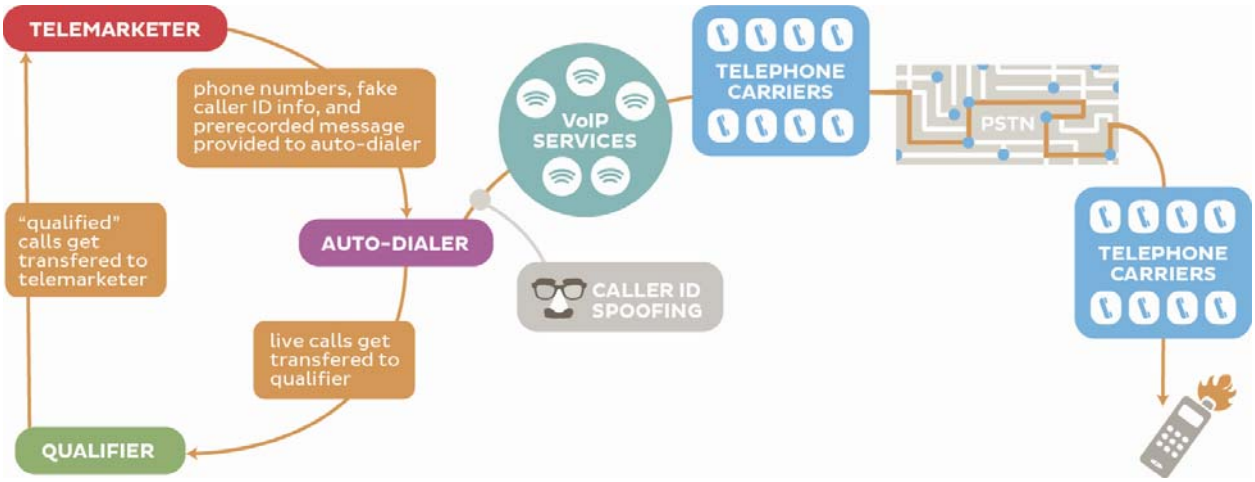
46 Herrmann, Tr. at 58-59; Schulzrinne, Tr. at 24.

47 Schulzrinne, Tr. at 24.

48 Herrmann, Tr. at 59-61.

49 *See* Dan Weber, Alan Basinger, Dean Willis, and David Schwartz, *Public Comment*, cmt #565017-00014, at 3.

cheap, widely available technology has resulted in a proliferation of entities available to perform any portion of the telemarketing process, including generating leads, placing automated calls, gathering consumers' personal information, selling the products, or doing all of the above.[50] Because of the dramatic decrease in upfront capital investment and overall cost, robocallers – like email spammers – can make a profit even if their success rate is very low.[51]



Technology enables a cheap and scalable model for robocalls.

2. New Technologies Have Made It Easier for Robocallers to Hide

Technological changes have also affected the marketplace by enabling telemarketers to conceal their identities when they place calls. First, direct connections do not exist between every pair of carriers, so intermediate carriers are necessary to connect the majority of calls. Thus, the typical call now takes a complex path, traversing the networks of multiple different VoIP and legacy carriers before reaching the end user.[52] Each of these carriers knows which carrier passed a particular phone call onto its network, but likely knows little else about the

---

50 Schulzrinne, Tr. at 20-21; Maxson, Tr. at 95-98.

51 Schulzrinne, Tr. at 21; Bellovin, Tr. at 16-17.

52 Panagia, Tr. at 130-32; Bellovin, Tr. at 17.

origin of the call.[53] Such a path makes it cumbersome to trace back to a call's inception.[54] All too often, this process to trace the call fails completely because one of the carriers in the chain has not retained the records that would further an investigation.[55]

Second, new technologies allow callers to manipulate the caller ID information that appears with an incoming phone call.[56] This "caller ID spoofing" has beneficial uses; legitimate companies adjust their caller ID information regularly so that customers will see the most useful corporate number or name, rather than the phone number from which an agent actually placed the call.[57] However, the same functionality allows robocallers 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.[58] In addition, robocallers can change their phone numbers frequently in an attempt to avoid detection.[59] It is generally illegal to transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value, but many robocallers flagrantly violate this law.[60]

---

53 Panagia, Tr. at. 132; Maxson, Tr. at 100.

54 Schulzrinne, Tr. at 24-25; Maxson, Tr. at 100; Bash, Tr. at 104.

55 Panagia, Tr. at 160-61; *see also id*. at 132-133; Schulzrinne, Tr. at 21.

56 Schulzrinne, Tr. at 24-26.

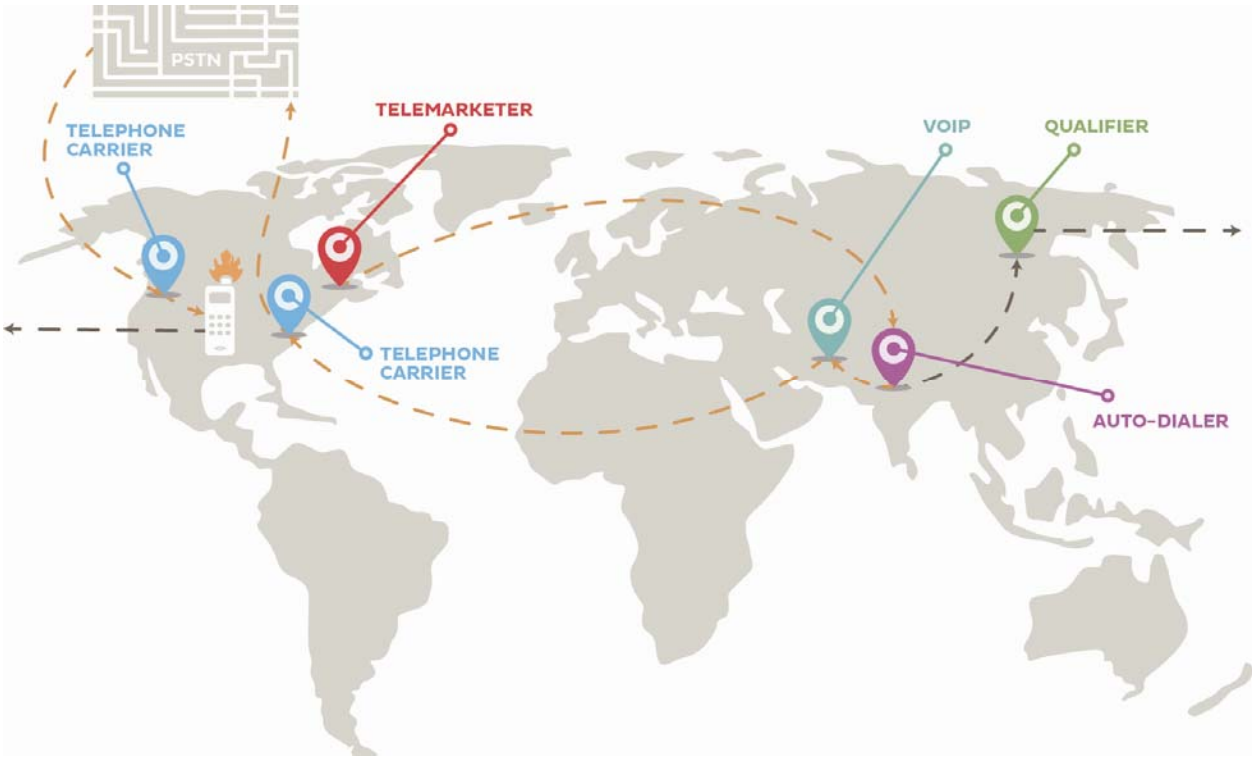
57 *See, e.g.*, Panagia, Tr. at 129.

58 Schulzrinne, Tr. at 21-22.

59 *Id.* at 24-26; Maxson, Tr. at 97; Bash, Tr. at 103.

60 *See* Truth in Caller ID Act, 47 U.S.C.§ 227(e); *cf.* 16 C.F.R. Part 310.4(a)(8) (the Telemarketing Sales Rule requires that sellers and telemarketers transmit or cause to be transmitted the telephone number and, when made available by the telemarketer's carrier, the name of the telemarketer, to any caller identification service in use by a recipient of a telemarketing call, or transmit the customer service number of the seller on whose behalf the call

Finally, new technologies help robocallers operate outside the jurisdiction where they are most likely to face prosecution.[61] Indeed, all of the many different entities involved in the path of a robocall can be located in different countries, making investigations even more challenging.



The path of a robocall can span the entire globe.

B. Need to Stimulate Technological Solutions

The Commission recognized the need to spur the marketplace into developing technical solutions that could help American consumers block illegal robocalls. Thus, at the conclusion of the Robocall Summit, the FTC announced its first public contest, a "Robocall Challenge" hosted on the challenge.gov platform, with a $50,000 prize for the individual or small team that could propose a technological solution to help consumers block robocalls on their landlines and mobile

---

is made and, when made available by the telemarketer's seller, the name of the seller. Under this provision, it is not necessary to prove intent to defraud.).

[61] Schulzrinne, Tr. at 21; Bellovin, Tr. at 16-17.

phones. The Commission also offered a separate award for the best solution by an organization with ten or more employees, which did not have a cash prize.[62]

The FTC received an astounding 798 eligible submissions, many of which were extremely well-considered technical proposals that moved the ball forward. As a result of the Robocall Challenge, a wide array of people with the necessary technical expertise spent countless hours thinking about these issues. All of the winning proposals were submitted by people who had never previously worked on the specific problem of illegal robocalls. In addition, the Robocall Challenge received an overwhelming amount of public attention and interest, helping the FTC spread the word about illegal robocalls and what consumers can do to fight them.

The primary goal of the Robocall Challenge was encouraging development of realistic ideas for decreasing the prevalence of telemarketing robocalls in a way that the FTC's traditional law enforcement efforts could not achieve alone. On April 2, 2013, the agency announced three winning solutions, which all contained promising ideas about how to address difficult realities such as the limitations of the telecommunications infrastructure and the prevalence of caller ID spoofing.[63] As the winning contestants and others further develop their ideas for introduction into the marketplace, we expect positive results for American consumers.

---

[62] The judges for the Challenge were FTC Chief Technologist Steve Bellovin, FCC Chief Technology Officer Henning Schulzrinne, and co-Executive Editor of *All Things Digital* Kara Swisher. The basic judging criteria were: Does it work? (50%); Is it easy to use? (25%); and Can it be rolled out? (25%). For details, see FTC Robocall Challenge Criteria Details, http://www.robocall.challenge.gov/details/criteria.

[63] *See* Press Release, FTC Announces Robocall Challenge Winners; Proposals Would Use Call Filter Software to Reduce Illegal Calls (Apr. 2, 2013), *available at* http://www.ftc.gov/opa/2013/04/robocall.shtm; Appendix B, Summary of Winning Robocall Challenge Submissions.

III. Consumer Education

Public education is an equally essential tool in the FTC's consumer protection and fraud prevention work. The Commission's education and outreach program reaches 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 information on dozens of issues. Indeed, the Commission uses law enforcement announcements as opportunities to remind consumers how to recognize a similar situation and report it to the FTC. In the case of robocalls, whether the offer involves fraudulent credit card services, so-called auto warranty protection plans, or bogus vacation travel packages, the FTC's message to consumers is simple: If you answer a call and hear a recorded sales message – and you haven't given your written permission to get calls from the company on the other end – hang up. Period. Other key self-help messages to consumers include how to place a phone number on the Do Not Call Registry, what to consider before asking a phone carrier to block calls, and how and where to report illegal robocalls. The FTC's education materials also explain how robocallers use technology to make thousands of calls at minimal cost, send fake caller ID information, and conceal their locations. The FTC disseminates these tips through articles,[64] blog posts,[65] social media,[66] infographics,[67] videos[68] and audio.[69]

---

[64] *See, e.g.*, FTC Robocall Microsite, http://www.consumer.ftc.gov/features/feature-0025-robocalls.

[65] *See, e.g.*, FTC Consumer Information Blog, http://www.consumer.ftc.gov/blog.

[66] *See, e.g.*, FTC Robocalls Facebook Q&A Transcript (July 17, 2012), http://www.ftc.gov/opa/socialmedia/facebookchats/1207ftcrobocallsfb.pdf.

The FTC updates its consumer education whenever it has new information to share. The Commission's library of articles on robocall scams in English and Spanish also includes pieces specifically describing credit card interest rate reduction scams, auto service contract and warranty fraud, and travel-related schemes.[70] When Robocall Challenge participants submitted to the Commission techniques they were using to successfully reduce illegal robocalls, the GSA and FTC used these tips in a video that relays some of the best consumer suggestions about what works today to fight robocalls.[71]

The Robocall Challenge expanded the reach of the Commission's consumer education messages about robocalls by spurring tremendous media interest. The announcement of the Challenge in October 2012 prompted a nationwide flurry of articles and television stories.[72]

---

[67] *See, e.g.*, FTC Robocalls Infographic, http://www.ftc.gov/bcp/edu/microsites/robocalls/infographic.shtm.

[68] *See, e.g.*, FTC Video and Media, http://www.consumer.ftc.gov/media.

[69] *See, e.g.*, FTC Consumer Information Audio, "Hang Up on Robocalls," http://www.consumer.ftc.gov/media/audio-0045-hang-robocalls.

[70] *See* FTC Consumer Information, "Travel Tips" (May 2013), http://www.consumer.ftc.gov/articles/0046-travel-tips; FTC Consumer Information, "Auto Service Contracts and Warranties" (Aug. 2012), http://www.consumer.ftc.gov/articles/0054-auto-service-contracts-and-warranties; FTC Consumer Information, "Credit Card Interest Rate Reduction Scams" (Feb. 2011), http://www.consumer.ftc.gov/articles/0131-credit-card-interest-rate-reduction-scams; *see generally* FTC Robocall Microsite, http://www.consumer.ftc.gov/features/feature-0025-robocalls; FTC Robocall Microsite in Spanish, "Llamadas automáticas pregrabadas o robocalls," http://www.consumidor.ftc.gov/destacado/destacado-s0025-llamadas-automaticas-pre-grabadas-o-robocalls.

[71] Robocall Challenge: Consumer Tips & Tricks (Apr. 2, 2013), http://www.consumer.ftc.gov/media/video-0086-robocall-challenge-consumer-tips-tricks.

[72] *See, e.g.*, Craig Timberg, *Find a way to block "robo-calls" and win $50K from the FTC*, WASH. POST, Oct. 18, 2012, *available at* http://www.washingtonpost.com/business/economy/find-a-way-to-block-robocalls-and-win-50k-from-the-ftc/2012/10/18/a2d648c6-1943-11e2-aa6f-3b636fecb829_story.html; Trevor Mogg,

When the agency announced the winners in April 2013, it again made headlines in national news outlets and technology publications, also reaching a television audience of an estimated 2.2 million viewers in the first 24 hours following the announcement.[73] Stories explained the problem of illegal robocalls and the FTC's determination to block them from landlines and mobile phones nationwide.

IV. Next Steps and Conclusion

The 10-year old Do Not Call Registry remains enormously successful in protecting consumers against unsolicited calls from legitimate telemarketers. But as technology changes and fraudsters exploit those changes, we must remain agile and creative. The Commission will continue its multifaceted efforts to fight illegal robocalls, including but not limited to the following actions:

- Continue Aggressive Law Enforcement
    - We will maintain our enforcement efforts, in coordination with state, federal, and international partners, to target high-volume offenders and pursue robocall gatekeepers in order to stop the largest number of illegal calls.
    - We will work with the telecommunications industry, encouraging carriers to be proactive in monitoring for illegal robocalls and securing the information necessary for prosecutions.

Wanna be a national hero? FTC contest offers $50,000 prize for solution to end annoying robocalls, DIGITAL TRENDS, Aug. 18, 2012, *available at* http://www.digitaltrends.com/cool-tech/ftc-contest-offers-50000-prize-for-solution-to-end-annoying-robocalls; NBC Bay Area, *FTC Holding Anti-Robo Call Contest*, Oct. 20, 2012, *available at* http://www.nbcbayarea.com/news/local/FTC-Holding-Anti-Robo-Call-Contest-175078991.html.

[73] *See, e.g.*, Edward Wyatt, *2 Deterrents to Robocalls Win Contest by FTC*, N.Y. TIMES, Apr. 2, 2013, *available at* http://www.nytimes.com/2013/04/03/technology/two-deterrents-to-robocalls-win-ftc-contest.html; Jon Brodkin, *No more robocalls: New tech automatically hangs up on robots*, ARS TECHNICA, Apr. 2, 2013, *available at* http://arstechnica.com/information-technology/2013/04/no-more-robocalls-new-tech-automatically-hangs-up-on-robots; Cristin Dorgelo, "Innovative Solutions to Fight Illegal Robocalls," Apr. 17, 2013, http://www.whitehouse.gov/blog/2013/04/17/innovative-solutions-fight-illegal-robocalls.

- Spur Innovation
    - We will work with industry leaders and other experts to further stimulate the development of technological solutions to block illegal robocalls.
    - We will continue to encourage industry-wide coordination to create and deploy VoIP standards that incorporate robust authentication capabilities.[74] Such coordination is the only way to ensure a future phone system with accurate and truthful calling information.
- Engage in Ongoing Consumer Education
    - We will continue our broad outreach to consumers regarding the Do Not Call Registry as well as illegal robocalls and how best to fight them.
- Work with Congress
    - We stand ready to assist in your efforts to protect consumers.

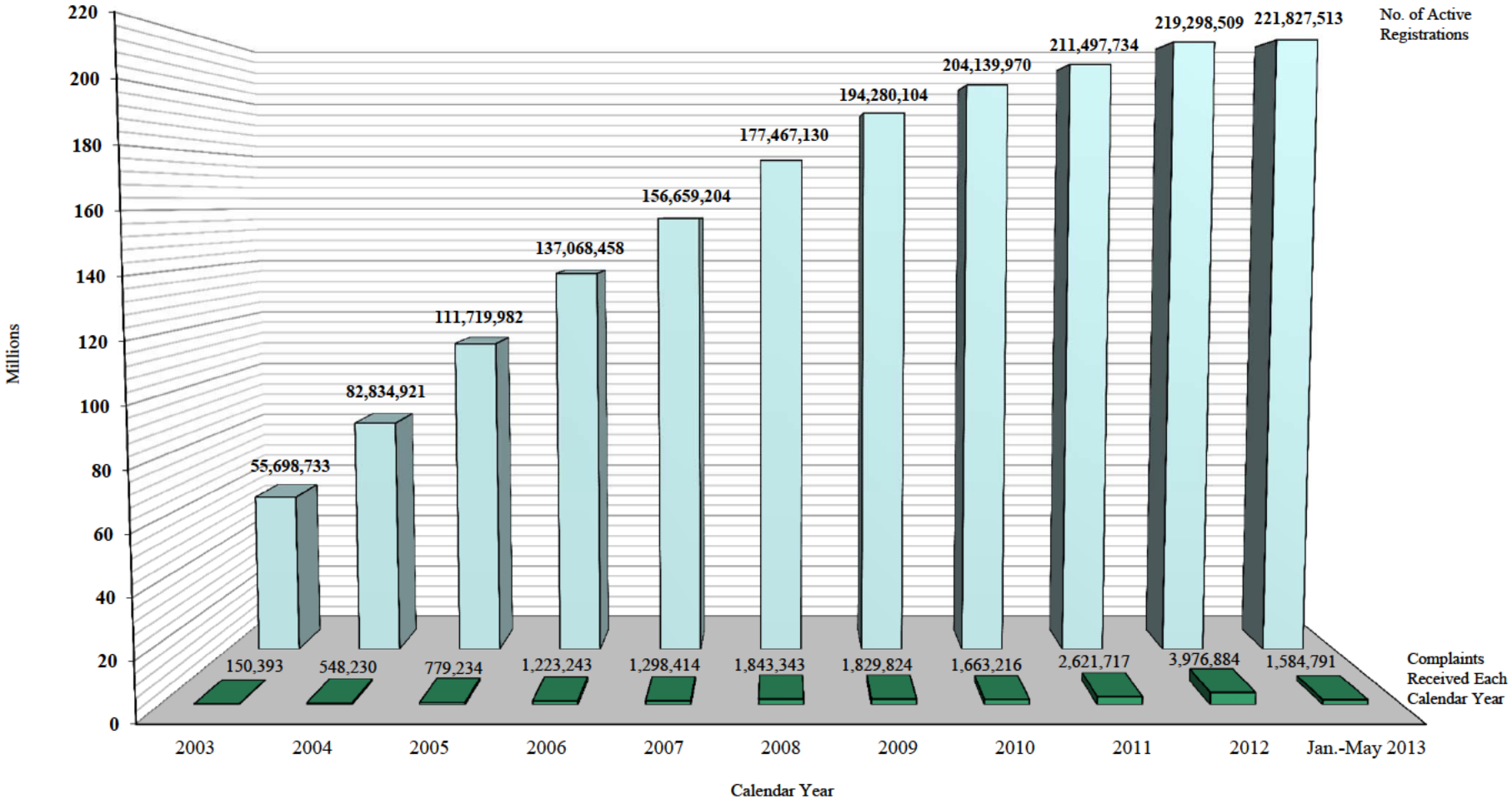
Thank you for the opportunity to share some of the highlights regarding the FTC's battle against illegal robocalls. We look forward to working with you on this important issue.

[74] This process will require active planning and cooperation in the coming months and years, as we move away from the legacy telecommunications infrastructure and toward a VoIP-based system. Experts around the world, including those involved in the Internet Engineering Task Force ("IETF"), have already begun to explore the technical changes necessary to permit authentication of VoIP calls. In fact, the IETF is in the process of creating a working group about this very topic called "STIR" – Secure Telephone Identity Revisited. Participants in the FTC Robocall Summit also mentioned the Alliance for Telecommunications Industry Solutions as the type of standard-setting group that might assist in organizing the necessary collaboration. Schulzrinne, Tr. at 167*; see also* Rupy, Tr. at 51, 67; Diggs, Tr. at 68-69; Whitt, Tr. at 208-09; *see generally* Paula Bailey-Stine, *Public Comment*, cmt #565017-00022, at 3-5.

Appendix A

National Do Not Call Registry Active Registrations and Complaint Figures

National Do Not Call Registry
Active Registration and Complaint Figures



Appendix B

Summary of Winning Robocall Challenge Submissions

FTC Robocall Challenge Winners
April 2, 2013

BEST OVERALL SOLUTION AWARD (Tie, winners receive $25,000 each):

Serdar Danis

Serdar Danis is a computer engineer who, in his free time, enjoys entering crowd-sourced technology contests such as patent research contests through Article One Partners and innovation contests through InnoCentive. This was his first time entering a contest through ChallengePost. Mr. Danis has several patent applications pending pertaining to this solution and also other inventions. You can direct inquiries about his solution to robocallchallengewinner@gmail.com.

For his solution, ***Robocall Filtering System and Device with Autonomous Blacklisting, Whitelisting, GrayListing and Caller ID Spoof Detection***

This solution involves a software application that can authenticate caller ID information as either authentic or spoofed, and display this information to the customer. It can be implemented through a customer-installed software application on smartphones and certain telephone systems, through updates to smartphone operating systems or carriers' software, or through a hardware device at the customer premises. In addition to authenticating caller ID information, the system depends on white and black lists that can be populated manually or autonomously and then aggregated into global white and black lists. Calls with authentic caller IDs on private or global white lists can be put through to the customer and calls from spoofed caller IDs or authentic callers IDs on the private or global black lists can be dropped. Any number not on a white or black list, or not authenticated, can be handled based on customer preferences, such as forwarded to voice mail or subjected to human verification without ringing the customer phone. Human verification would rely on continuously changing pre-recorded questions presented to the caller, which would be difficult for a computer to answer. The solution stops those who abuse the telephone system without inconveniencing regular callers.

Aaron Foss

Aaron Foss is a freelance software developer based in Long Island, New York. He went through the TechStars NYC program (Summer 2011) and is co-founder and lead developer of SmartChemo. You can direct inquiries about his solution to aaron@nomorobo.com or 631-406-9283.

For his solution, ***Nomorobo***

Nomorobo uses an existing feature of the current phone system along with the power of cloud computing to fight back against illegal robocallers. By using simultaneous ringing – which is widely available through most phone carriers - the call is split and routed to the Nomorobo server as well as the user's phone. Instantly, Nomorobo analyzes the call and determines the threat level by using machine learning to identify and adapt to new robocallers based on their calling patterns. Nomorobo inspects the CallerID header, analyzes the frequency of every call, and compares this data to its real-time black and white lists. Potential robocallers are presented with an audio CAPTCHA for final verification while legal robocallers have their phone numbers whitelisted to guarantee message delivery. If it's an unknown robocall, Nomorobo answers and immediately hangs up. If no threat is detected, Nomorobo does nothing and the call goes through like normal. All of this happens instantly, before the consumer's phone begins to ring. Nomorobo works with any kind of phone, no additional hardware is necessary, and no infrastructure changes are required by phone companies.

TECHNOLOGY ACHIEVEMENT AWARD (Non-monetary):

Daniel Klein and Dean Jackson, from Google

Mr. Klein and Mr. Jackson are engineers based out of the Google office in Pittsburgh, Pennsylvania. You can direct inquiries about their solution to Google's press office.

For their solution, ***Crowd-Sourced Call Identification and Suppression***

Google's robocall concept could give consumers the power to block robocalls -- and to allow that information to be used to shield all consumers from robocallers even before their phones ring. The concept could work across all phone platforms as deployed via a smartphone app, changes to VoIP telephone software, or hardware devices. In each case, consumers could easily indicate whether an unknown number should be blocked in the future, which could then be communicated to a centralized database. After a number of people marked a caller as needing to be blocked, that caller could be blocked for everyone else that chose to use the system. The system would include a specialized mechanism to combat CallerID spoofing. In addition, before adding a number to the centralized database, many factors could be considered such as call volume, frequency, and inbound/outbound ratio. These factors could be computed dynamically, adjusting the behavior of the system to match current calling patterns. Also, the system could use a whitelist to keep some numbers out of the database. By using aggregated data about the incoming phone numbers in this manner, this concept could quickly identify and block robocallers and the fraudsters that use these automated calls to swindle consumers.