Prepared Statement of
The Federal Trade Commission

Before the
United States Senate
Special Committee on Aging

on

Still Ringing off the Hook: An Update on Efforts to Combat Robocalls

Washington, DC
October 4, 2017

Chairman Collins, Ranking Member Casey, 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 discuss the Commission's initiatives to fight illegal robocalls, including those that target seniors.[2]

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.[3] The Registry, which includes more than 226 million active telephone numbers,[4] has been tremendously successful in protecting consumers' privacy from the unwanted calls of tens of

---

[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] *See, e.g., FTC v. Life Management Services of Orange County, LLC*, 6:16-CV-982-Orl (M.D. Fla. June 8, 2016) (FTC alleged defendants bombarded consumers with illegal prerecorded calls fraudulently pitching interest rate reduction and debt elimination schemes, in some instances targeting seniors), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3216/life-management; *FTC v. Lifewatch Inc.*, 1:15-cv-05781 (N.D. Ill. June 20, 2015) (FTC and Florida Attorney General alleged defendants used blatantly illegal and fraudulent prerecorded calls to trick older consumers into signing up for medical alert systems with monthly monitoring fees), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3123/lifewatch-inc; *FTC v. All Us Marketing LLC*, 6:15CV1016-0RL-28GJK (M.D. Fla. June 29, 2015) (FTC and Florida Attorney General alleged defendants engaged in massive prerecorded call campaigns designed to defraud consumers, often seniors, into paying significant up-front fees for worthless credit card interest rate reduction programs), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3256/all-us-marketing-llc-formerly-known-payless-solutions-llc.

[3] 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. *See generally* The Telemarketing Sales Rule, 16 C.F.R. Part 310.

[4] *See* National Do Not Call Registry Active Registrations and Complaint Figures. National Do Not Call Registry Data Book FY 2016 at 4 (Dec. 2016), *available at* https://www.ftc.gov/reports/national-do-not-call-registry-data-book-fiscal-year-2016.

thousands of legitimate telemarketers who subscribe to the Registry each year.[5] More recently, changes in technology led to a new source of immense frustration – the blasting of prerecorded messages that primarily rely on Voice over Internet Protocol ("VoIP") technology.[6] In 2008, the Commission responded by amending the TSR to prohibit the vast majority of prerecorded sales calls.[7]

Illegal robocalls remain a significant consumer protection problem because they repeatedly disturb consumers' privacy and frequently use fraud and deception to pitch goods and services, leading to significant economic harm. Illegal robocalls are also frequently used by criminal impostors posing as trusted officials or companies. Consumers are justifiably frustrated—in 2016 the FTC received more than 3.4 million robocall complaints and in 2017 the FTC received more than 3.5 million robocall complaints just between January and August.[8] The FTC is using every tool at its disposal to fight these illegal calls.[9] This testimony describes the Commission's efforts to stop telemarketer violations, including our aggressive law enforcement, initiatives to spur technological solutions, and robust consumer and business outreach.

---

[5] For example, in fiscal year 2016, more than 17,000 telemarketers accessed the Do Not Call Registry. National Do Not Call Registry Data Book FY 2016 at 8 (Dec. 2016), *available at* https://www.ftc.gov/reports/national-do-not-call-registry-data-book-fiscal-year-2016.

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

[7] 73 Fed. Reg. 51164 (Aug. 29, 2008); 16 C.F.R. § 310.4(b)(1)(v).

[8] Total unwanted-call complaints for the first eight months of 2017, including both robocall complaints and complaints from consumers whose phone numbers are registered on the Do Not Call Registry, exceed 5.5 million. On average, over 400,000 of these complaints each month are about robocalls.

[9] *See* FTC Robocall Initiatives, http://www.ftc.gov/robocalls.

I. Law Enforcement

Since establishing the Do Not Call Registry in 2003,[10] the Commission has fought vigorously to protect consumers' privacy from unwanted calls. Indeed, since the Commission began enforcing the Do Not Call provisions of the TSR in 2004, the Commission has brought 131 enforcement actions seeking civil penalties,[11] restitution for victims of telemarketing scams, and disgorgement of ill-gotten gains against 429 corporations and 345 individuals. From the 124 cases that have been resolved thus far, the Commission has collected over $120 million in equitable monetary relief and civil penalties.

A. Robocall Law Enforcement

On September 1, 2009, TSR provisions went into effect prohibiting the vast majority of robocalls selling a good or service.[12] The robocall provisions cover prerecorded calls to all

---

[10] 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* https://www.ftc.gov/news-events/press-releases/2003/09/ftc-files-motion-stay-pending-appeal-oklahoma-dnc-ruling; Press Release, Statement of FTC Chairman Timothy J. Muris (Sept. 26, 2003), *available at* https://www.ftc.gov/news-events/press-releases/2003/09/statement-ftc-chairman-timothy-j-muris. 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* https://www.ftc.gov/news-events/press-releases/2003/09/statement-ftc-chairman-timothy-j-muris-0. 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* https://www.ftc.gov/news-events/press-releases/2004/02/appeals-court-upholds-constitutionality-national-do-not-call.

[11] As is true of all TSR violations, telemarketers who violate the Do Not Call provisions are subject to civil penalties of up to $40,000 per violation. 15 U.S.C. § 45(m)(1)(A); 16 C.F.R. § 1.98(d).

[12] Like the other provisions of the TSR, the robocall provisions do not apply to non-sales calls, such as calls placed by charities to its members and prior donors or those calls that are purely political, informational, or survey calls. *See generally* "Complying with the Telemarketing Sales Rule" (June 2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/complying-telemarketing-sales-rule. 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. § 310.4(b)(1)(v)(D), and for certain calls placed by telemarketers who solicit charitable contributions, 16 C.F.R. § 310.4(b)(1)(v)(B).

consumers, including those who have not registered their phone number on the Do Not Call Registry. The Commission has been aggressive in enforcing prohibitions against robocalls, filing 45 cases against 163 companies and 121 individuals responsible for *billions of illegal robocalls*.[13] From the 41 cases that have concluded thus far, the Commission has collected more than $29 million in civil penalties, redress, or disgorgement. Set forth below are details regarding several of our enforcement actions in this area.

1. Historic Victory in Dish Network

The FTC and our law enforcement partners recently achieved an historic win in the fight against unwanted calls and robocalls. On June 5, 2017, a federal district court in Illinois issued an order imposing the largest penalty ever issued in a Do Not Call case: $280 million against Dish Network.[14] The *Dish* litigation began in 2009 when the Department of Justice brought an action on behalf of the FTC with the states of California, Illinois, North Carolina, and Ohio alleging millions of violations of the Telemarketing Sales Rule, the Telephone Consumer Protection Act ("TCPA") and various state Do Not Call laws.[15] The litigation centered on allegations that Dish and its telemarketers made tens of millions of calls—often robocalls[16]—to

---

[13] The FTC filed 12 of the 45 cases before the rule change went into effect on September 1, 2009.

[14] *See U.S. v. Dish Network, LLC*, No. 3:09-cv-03073 (C.D. Ill. June 6, 2017) *available at* https://www.ftc.gov/news-events/press-releases/2017/06/ftc-doj-case-results-historic-decision-awarding-280-million-civil.

[15] *U.S. v. Dish Network, LLC*, No. 3:09-cv-03073 (C.D. Ill. Mar. 25, 2009), *available at* https://www.ftc.gov/news-events/press-releases/2009/03/ftc-charges-dish-network-formerly-known-echostar-multiple-do-not.

[16] When the *Dish* case was filed in March of 2009, the robocall provision of the TSR was not yet in effect, thus the complaint reached Dish's unlawful use of robocalls through a count alleging violations of the TSR's abandoned call provisions. Since October 1, 2003, telemarketers have been prohibited from abandoning an outbound telephone call, and sellers are prohibited from causing a telemarketer to do so in violation of the TSR. 16 C.F.R. § 310.4(b)(1)(iv). An outbound telephone call is

telephone numbers on the Do Not Call Registry and called consumers who previously asked Dish and its telemarketers to stop calling.[17] In January 2015, the Court found that Dish and its telemarketers had engaged in more than 66 million violations of the TSR and that Dish was responsible for calls made by its retailers.[18] The $280 million penalty against Dish includes $168 million to the United States for violations of the TSR and $112 million to the states for violations of the TCPA and various state laws. The order also imposed strong injunctive relief that, among other provisions, requires Dish to hire a monitor to ensure that Dish and its retailers comply with telemarketing laws.[19] The tireless efforts of DOJ and our state co-plaintiffs were invaluable in securing an outcome that takes a strong stand against companies who invade a consumer's privacy through unwanted calls and robocalls.

2. Strategic Targeting of Robocall Violators

In response to growing consumer complaints about illegal robocalls, the FTC engages in strategic targeting to maximize impact, prioritizing targets that are causing the most harm to consumers. For example, in January 2017, the Commission filed two lawsuits, *FTC v. Justin Ramsey* and *FTC v. Aaron Michael Jones*, that shut down operations responsible for *billions* of

---

abandoned if a person answers it and the telemarketer does not connect the call to a sales representative within two (2) seconds of the person's completed greeting. 16 C.F.R. § 310.4(b)(1)(iv). The use of robocalls, where a sales pitch to a live consumer begins with or is made entirely by a pre-recorded message, violates the TSR's abandoned call prohibition because the telemarketer is not connecting the call to a sales representative within two (2) seconds of the person's completed greeting.

[17] *Id.*

[18] *U.S. v. Dish Network, LLC*, No. 3:09-cv-03073 (C.D. Ill. Jan. 21, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/01/court-grants-partial-summary-judgment-ftc-case-against-dish.

[19] *See U.S. v. Dish Network, LLC*, No. 3:09-cv-03073 (C.D. Ill. June 6, 2017) *available at* https://www.ftc.gov/news-events/press-releases/2017/06/ftc-doj-case-results-historic-decision-awarding-280-million-civil.

illegal robocalls. The *Ramsey* and *Jones* defendants bombarded consumers with pitches for home security systems and extended auto warranties and compounded their illegal robocalls by dialing more that 70 million phone numbers that were registered on the Do Not Call Registry.[20]

In June 2016, as part of the FTC's work targeting telemarketers that use robocalls to defraud consumers, the FTC and the Florida Attorney General brought an action to shut down a company that allegedly blasted consumers with illegal robocalls touting bogus credit-card interest rate reduction and debt relief services.[21] The FTC alleged that this scheme bilked consumers out of more than $23 million since 2013.[22] In some instances, the defendants allegedly tailored their debt elimination pitch to consumers over age 60.[23]

Over the past two years the FTC, often in conjunction with its law enforcement partners, initiated nine new actions targeting defendants we alleged are responsible for billions of illegal robocalls hawking home security systems, free vacations, medical alert devices, energy savings, and credit card interest rate reductions.[24] Many of the defendants in these cases are now banned

---

[20] *FTC v. Justin Ramsey*, 9:17-cv-80032-KAM (S.D. Fl. Jan. 13, 2017), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3254/justin-ramsey; *FTC v. Michael Aaron Jones*, 8:17-cv-00058 (M.D. Fla. Jan. 13, 2017), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3152/allorey-inc. Evidence reviewed by FTC staff in connection with the *Ramsey* case indicated that a portion of the unlawful telemarketing calls targeted "distressed seniors."

[21] *See FTC v. Life Management Services of Orange County, LLC*, 6:16-CV-982-Orl (M.D. Fla. June 8, 2016), https://www.ftc.gov/enforcement/cases-proceedings/152-3216/life-management. We alleged that the defendants used fake company names that deceived consumers into thinking that the defendants had a relationship or affiliation with the consumers' credit-card issuers.

[22] *See FTC v. Life Management Services of Orange County, LLC*, 6:16-CV-982-Orl (M.D. Fla. May 1, 2017), D.E. #163.

[23] For example, one consumer stated that the telemarketer claimed to be offering "a program to help senior citizens eliminate their debt." *FTC v. Life Management Services of Orange County, LLC*, 6:16-CV-982-Orl, Plaintiff's Exhibit 7 (M.D. Fla. June 8, 2016).

[24] *FTC v. Justin Ramsey*, 9:17-cv-80032-KAM (S.D. Fla. Jan. 13, 2017), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3254/justin-ramsey; *FTC v. Michael Aaron*

from robocalling or telemarketing.[25]

3. Reaching Violators Attempting to Avoid Detection

Increasingly, the perpetrators behind these abusive and often fraudulent calls take steps to avoid detection, either by operating through a web of related entities, "spoofing" their Caller ID information, or hiding overseas. The FTC uses every investigative and litigation tool at its disposal to cut through these deceptions. For example, the defendants in the *Jones* and *Ramsey* cases operated through a tangle of related individuals and entities to avoid detection by law

---

Jones, 8:17-cv-00058 (M.D. Fla. Jan. 13, 2017), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3152/allorey-inc; *U.S. v. Consumer Education.info, Inc.*, 1:16-cv-02692 (D. Col. Nov. 1, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3081/consumer-educationinfo-inc; *FTC v. Life Management Services of Orange County, LLC*, 6:16-CV-982-Orl (M.D. Fla. June 8, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3216/life-management; *U.S. v. Lilly Management and Marketing, LLC*, 6:16-cv-485-Orl (M.D. Fla. Mar. 17, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3115/usa-vacation-station; *U.S. v. KFJ Marketing Inc.*, 2:16-cv-01643 (C.D. Cal. Mar. 10, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3166/kfj-marketing-llc; *FTC v. Lifewatch Inc.*, 1:15-cv-05781 (N.D. Ill. June 20, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3123/lifewatch-inc; *FTC v. All Us Marketing LLC*, 6:15CV1016-0RL-28GJK (M.D. Fla. June 29, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3256/all-us-marketing-llc-formerly-known-payless-solutions-llc; *FTC v. Caribbean Cruise Line, Inc.*, 0:15-cv-60423 (S.D. Fla. Mar. 4, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3196-x150028/caribbean-cruise-line-inc.

[25] *See, e.g., FTC v. Michael Aaron Jones*, 8:17-cv-00058 (M.D. Fla. May 31, 2017), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3152/allorey-inc (final orders permanently banning Jones and related companies from all telemarketing activities, including initiating robocalls, calling numbers on the Do Not Call Registry, and selling data lists containing consumers' phone numbers and other information); *FTC v. All Us Marketing LLC*, 6:15CV1016-0RL-28GJK (M.D. Fla. May 22, 2017, June 8, 2016 and Nov. 1, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3256/all-us-marketing-llc-formerly-known-payless-solutions-llc (multiple final orders permanently banning most defendants from robocalling, telemarketing, and providing debt relief services); *FTC v. Justin Ramsey*, 9:17-cv-80032-KAM (S.D. Fla. Apr. 11, 2017), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3254/justin-ramsey (stipulated order banning Ramsey and his company from placing robocalls to individuals to sell goods or services, initiating sales calls to numbers listed on the Do Not Call Registry, and selling data lists containing phone numbers listed on the Registry); *FTC v. Caribbean Cruise Line, Inc.*, 0:15-cv-60423 (S.D. Fla. Feb. 17, 2017), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3196-x150028/caribbean-cruise-line-inc (final stipulated order banning the Pacific Telecom defendants from robocalling and illegal telemarketing, as well as helping anyone else make such calls).

enforcement. In addition, defendants in four of our recent robocall cases routinely hid their true name or phone number to deceive consumers and evade detection by law enforcement and the Commission included counts in its suits targeting this unlawful Caller ID spoofing.[26]

The perpetrators behind many unlawful calls also seek to evade law enforcement by operating overseas. When consumers are victimized by fraudulent calls from international call centers, the Commission finds ways to stymie the scammers by cracking down on their U.S. enablers. In one recent case, the Commission filed suit against individuals and entities in the U.S. who were collecting money on behalf of telemarketers at India-based call centers operating government impostor scams that conned consumers into paying hundreds or thousands of dollars for taxes they did not owe, or fees for services they did not receive.[27] In another recent case, the Commission brought suit against the U.S. operators of a scam that relied on Peruvian call centers and sophisticated Caller ID spoofing to pressure Spanish speaking U.S. consumers into purchasing English-language learning materials of little value—and then posing as government officials to threaten and harass uninterested consumers into "purchasing" their products.[28]

---

[26] *See U.S. v. KFJ Marketing Inc.*, 2:16-cv-01643 (C.D. Cal. Mar. 10, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3166/kfj-marketing-llc; *FTC v. Lifewatch Inc.*, 1:15-cv-05781 (N.D. Ill. June 20, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3123/lifewatch-inc; *FTC v. All Us Marketing LLC*, 6:15CV1016-0RL-28GJK (M.D. Fla. June 29, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3256/all-us-marketing-llc-formerly-known-payless-solutions-llc; *FTC v. Caribbean Cruise Line, Inc.*, 0:15-cv-60423 (S.D. Fla. Mar. 4, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3196-x150028/caribbean-cruise-line-inc. In each case, the FTC alleged that defendants failed to transmit complete and accurate Caller ID information in violation of 16 C.F.R. § 310.4(a)(8). In addition, the complaint in *FTC v. Jones*, alleged that the defendants assisted and facilitated others engaged in illegal spoofing. *FTC v. Michael Aaron Jones*, 8:17-cv-00058 (M.D. Fla. Jan. 13, 2017), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3152/allorey-inc.

[27] *FTC v. PHLG Enterprises LLC*, 8:17-cv-00220-RAL-AEP (M.D. Fla. Jan. 27, 2017), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3245-x170019/phlg-enterprises-llc.

[28] *FTC v. ABC Hispana Inc.*, 5:17-cv-00252-JGB-DTB (C.D. Cal. Apr. 19, 2017), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3108/abc-hispana-inc-et-al.

B. Coordination with Law Enforcement Partners

As the law enforcement challenges associated with illegal telemarketing have increased, the FTC's relationships with other agencies have become increasingly 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 Internal Revenue Service ("IRS"), the U.S. Treasury Inspector General for Tax Administration ("TIGTA"), 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 FTC's collaboration with its partners takes many forms, including sharing information and targets, assisting with investigations, and working collaboratively on long-term policy initiatives.

The Commission also coordinates with various partners to bring law enforcement actions. Seven of the nine most recent robocall enforcement actions the FTC has led involved collaboration with the Department of Justice or our state partners.[29] The FTC also leads robocall law enforcement "sweeps"—coordinated, simultaneous law enforcement actions—in conjunction with state and federal partners.[30] Most recently, the FTC led a multinational robocall sweep announced in June 2016 that took action against operations estimated to be

---

[29] *See supra* n. 24.

[30] *See, e.g.*, Press Release, FTC Leads Joint Law Enforcement Effort Against Companies that Allegedly Made Deceptive "Cardholder Services" Robocalls (Nov. 1, 2012), *available at* https://www.ftc.gov/news-events/press-releases/2012/11/ftc-leads-joint-law-enforcement-effort-against-companies.

responsible for billions of illegal robocalls.[31] The June 2016 sweep included thirty-nine actions taken by the FTC, the Canadian Radio-television and Telecommunications Commission (CRTC), the United Kingdom's Information Commissioner's Office (ICO), as well as DOJ, the FCC and the attorney generals' offices of Colorado, Florida, Indiana, Kansas, Mississippi, Missouri, North Carolina, Ohio, and Washington State, and the Tennessee Regulatory Authority.

II. Policy and Market Stimulation Initiatives

Despite the 2009 prohibition of unauthorized robocalls and the Commission's vigorous enforcement efforts, technological advances have permitted law-breakers to make more robocalls for less money with a greater ability to hide their identity. For example, at the end of 2009, the FTC received approximately 63,000 complaints about illegal robocalls each month.[32] That number has now more than quadrupled—so far in 2017 the FTC has received an average of 400,000 robocall complaints per month.[33]

A. Understanding the Landscape of the Robocall Problem

Recognizing that law enforcement, while critical, 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,

---

[31] *See* Press Release, FTC, Florida Attorney General Take Action Against Illegal Robocall Operation (June 14, 2016), *available at* https://www.ftc.gov/news-events/press-releases/2016/06/ftc-florida-attorney-general-take-action-against-illegal-robocall and https://www.ftc.gov/system/files/attachments/press-releases/ftc-florida-attorney-general-take-action-against-illegal-robocall-operation/160614robocallenforcementactions.pdf (listing actions comprising the coordinated enforcement crackdown).

[32] National Do Not Call Registry Data Book FY 2010 at 5 (Nov. 2010), *available at* https://www.ftc.gov/reports/national-do-not-call-registry-data-book-fiscal-year-2010. Since that time, the FTC began separately tracking Do Not Call complaints and robocall complaints based on information provided by the consumer.

[33] *See supra* n. 8.

consumers, and counterparts at federal, state, and foreign government agencies. The Commission ramped up these efforts in October 2012, when the Commission hosted a public summit on robocalls to explore these issues (the "Robocall Summit").[34] Since then, as discussed below, the Commission has spurred the creation of specific groups of experts and industry members to work together and with international law enforcers to tackle this vexing consumer protection issue.

Speakers at the Robocall Summit made clear that convergence between the legacy telephone system and the Internet has allowed robocallers to engage, at very little cost, in massive, unlawful robocall campaigns that cross international borders and hide behind spoofed Caller ID information. 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 relatively recently, telemarketing required significant capital investment in specialized hardware and labor.[35] Now, robocallers benefit from automated dialing technology, inexpensive international and long distance calling rates, and the ability to move internationally and employ cheap labor.[36] The only necessary equipment is a computer connected to the Internet.[37] The result: law-breaking telemarketers can place robocalls for a fraction of one cent

---

[34] *See generally* FTC Workshop, *Robocalls: All the Rage* (Oct. 18, 2012), *available at* https://www.ftc.gov/news-events/events-calendar/2012/10/robocalls-all-rage-ftc-summit. A transcript of the workshop (hereinafter "Tr.") is available at https://www.ftc.gov/sites/default/files/documents/public_events/robocalls-all-rage-ftc-summit/robocallsummittranscript.pdf.

[35] Herrmann, Tr. at 58-59; Schulzrinne, Tr. at 24.

[36] Schulzrinne, Tr. at 24.

[37] Herrmann, Tr. at 59-61.

per minute. In addition, the 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, or selling products.[38] Because of the dramatic decrease in upfront capital investment and marginal cost, robocallers—like email spammers—can make a profit even if their contact rate is very low.[39]

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 many calls. Thus, the typical call now takes a complex path, traversing the networks of multiple VoIP and legacy carriers before reaching the end user.[40] Such a path makes it cumbersome to trace back to a call's inception.[41] All too often, this process to trace the call fails completely because one of the carriers in the chain has not retained the records necessary for a law enforcement investigation.[42]

Second, new technologies allow callers to easily manipulate the Caller ID information that appears with an incoming phone call.[43] While "Caller ID spoofing" has some beneficial uses,[44] it also allows telemarketers to deceive consumers by pretending to be an entity with a

---

[38] Schulzrinne, Tr. at 20-21; Maxson, Tr. at 95-98.

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

[40] Panagia, Tr. at 130-32; Bellovin, Tr. at 17.

[41] Schulzrinne, Tr. at 24-25; Maxson, Tr. at 100; Bash, Tr. at 104.

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

[43] Schulzrinne, Tr. at 24-26.

[44] *See, e.g.*, Panagia, Tr. at 129 (AT&T allows the third party that performs AT&T's customer service to "spoof" AT&T's customer service line).

local phone number or a trusted institution such as a bank or government agency.[45] In addition, telemarketers can change their phone numbers frequently in an attempt to avoid detection.[46]

Finally, new technologies allow robocallers to operate outside of jurisdictions where they are most likely to face prosecution.[47] Indeed, the entities involved in the path of a robocall can be located in different countries, making investigations even more challenging.

B. Need to Stimulate Technological Solutions

1. Robocall Contests

Recognizing the need to spur the marketplace into developing technical solutions that protect American consumers from illegal robocalls, the FTC led four public challenges to help tackle the unlawful robocalls that plague consumers. In 2012-2013, the FTC conducted its first Robocall Challenge[48], and called upon the public to develop a consumer-facing solution that blocks illegal robocalls, applies to landlines and mobile phones, and operates on proprietary and non-proprietary platforms. In response, we received 798 submissions and partnered with experts in the field to judge the entries. One of the winners, "NomoRobo," was on the market and available to consumers by October 2013—just 6 months after being named one of the winners.

---

[45] Schulzrinne, Tr. at 21-22.

[46] *Id.* at 24-26; Maxson, Tr. at 97; Bash, Tr. at 103. Under the Truth in Caller ID Act, it is generally illegal to transmit misleading or inaccurate Caller ID information with intent to defraud. *See* Truth in Caller ID Act, 47 U.S.C.§ 227(e); *cf.* 16 C.F.R. § 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 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.).

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

[48] For more information on the first FTC Robocall Challenge, *see* https://www.ftc.gov/news-events/press-releases/2013/04/ftc-announces-robocall-challenge-winners.

To date, "NomoRobo," which reports blocking over 279 million calls, is being offered directly to consumers by a number of telecommunications providers and is now available as an app on iPhones.[49]

The following year the FTC launched its second challenge—Zapping Rachel[50]—which called upon information security experts to help create a robust robocall honeypot. Sixty teams and individuals signed up for one or more phase, and FTC staff obtained new insights that improved current robocall honeypot designs and connected new partners and stakeholders.

In June 2015, the FTC sponsored its third challenge, DectectaRobo[51], in which it called upon the public to analyze call data to create algorithms that could predict which calls were likely robocalls. Nineteen teams from all over the U.S. participated. Later in 2015, the FTC challenged information security experts to create tools people could use to block and forward robocalls automatically to a honeypot as part of the Robocalls: Humanity Strikes Back challenge.[52] Contestants built and submitted robocall solutions to the judges and finalists, then competed to "seed" their solutions and collect the highest number of robocalls.

Each of the four challenges provided the Commission with an opportunity to promote industry dialogue and innovation in combatting illegal robocalls, develop industry partnerships,

---

[49] *See* https://www.nomorobo.com/ (last visited Sept. 22, 2017) and Robocall Strike Force, Robocall Strike Force Report at 17-18 (April 28, 2017), https://www.fcc.gov/file/12311/download ("*Strike Force Report II*") at 17-18.

[50] A robocall honeypot is an information system designed to attract robocallers and help investigators and academics understand and combat illegal calls. For more information on the Zapping Rachel challenge *see* https://www.ftc.gov/news-events/contests/zapping-rachel.

[51] For more information on the Detectarobo challenge *see* https://www.ftc.gov/news-events/contests/detectarobo.

[52] For more information on the Robocalls: Humanity Strikes Back challenge, *see* https://www.ftc.gov/news-events/contests/robocalls-humanity-strikes-back.

and refine its understanding of the robocall problem and potential solutions. More importantly, the challenges contributed to a shift in the development and availability of technological solutions in this area, particularly call-blocking and call-filtering products. A number of voice service providers now offer call-blocking or call-filtering products to some or all of their customers.[53] In addition, there are a growing number of free or low-cost apps available for download on wireless devices that offer call-blocking and call-filtering solutions.[54]

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

The FTC provided input to support the industry-led Robocall Strike Force, which is also working to deliver comprehensive solutions to prevent, detect, and filter unwanted robocalls.[55] In tandem with this effort, the FTC worked with a major carrier and federal law enforcement partners to help block IRS scam calls that were spoofing well-known IRS telephone numbers.

---

[53] For example, in late 2016 AT&T launched "Call Protect", which is a product available to many AT&T wireless customers that blocks fraud calls and flags others as potential "spam." *See* http://about.att.com/story/att_call_protect.html. T-Mobile offers its wireless customers two free products, "Scam ID" and "Scam Block", that flag and block unwanted calls. *See* http://explore.t-mobile.com/callprotection (last visited Sept. 22, 2017). Verizon offers a product called "Caller Name ID" to its wireless customers that also attempts to flag and block unwanted calls. *See* https://www.verizonwireless.com/solutions-and-services/caller-name-id/. In addition, a number of carriers make Nomorobo available to their VoIP or cable line customers. *See, e.g.*, https://www.fcc.gov/consumers/guides/stop-unwanted-calls-texts-and-faxes (listing available call blocking resources from a number of wireline providers) (last visited Sept. 22, 2017).

[54] The Cellular Telecommunications Industry Association (CTIA) maintains a list of some of the available call blocking apps, both for iOS devices: https://www.ctia.org/consumer-tips/robocalls/ios-robocall-blocking and for Android devices: https://www.ctia.org/consumer-tips/robocalls/android-robocall-blocking (last visited Sept. 22, 2017).

[55] The Robocall Strike Force developed in response to a call from the FCC to make better call blocking solutions available to consumers, quickly, and free of charge. *See* Robocall Strike Force, Robocall Strike Force Report at 1 (2016), https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf. The FTC has long been a proponent of call blocking services as a critical tool to reduce unwanted calls and robocalls and strongly supports the Strike Force's efforts. *See e.g.*, FTC Staff, Comments Before the Federal Communications Commission on Public Notice DA 14-1700 Regarding Call Blocking, CG Docket No. 02-278; WC Docket No. 07-135 (Jan. 23, 2015), *available at* https://www.ftc.gov/policy/policy-actions/advocacy-filings/2015/01/ftc-staff-comment-federal-communications-commission.

The Strike Force expanded this effort and it contributed to a drop in IRS scam calls at the end of 2016.[56]

The Strike Force also found that, while several providers and third parties offered call-blocking products, there was no widespread call-blocking solution spanning the networks. In order to provide proactive call-blocking services to customers, the Strike Force sought clarification from the FCC that "blocking presumptively illegal calls is one of the tools carriers are permitted to use to provide consumers additional relief."[57] In response, this spring the FCC issued a Notice of Proposed Rule Making and Notice of Inquiry that seeks to expand the categories of calls that voice service providers are authorized to block and invites comment on what types of standards should govern providers engaged in call blocking.[58] The FTC filed a comment in response, supporting the NPRM's efforts to expand the categories of calls that voice service providers are authorized to block and encouraging the FCC to allow for some provider flexibility when considering standards to govern provider-based blocking of presumptively-illegal calls.[59]

---

[56] *See* Robocall Strike Force, Robocall Strike Force Report at 32-33 (2016), https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf.

[57] *See id*. at 40.

[58] Specifically, the FCC's NPRM sought input on rulemaking proposals that would authorize two categories of provider-based call blocking: 1) when the subscriber to a particular telephone number requests that telecommunications providers block calls originating from that number; and 2) when the originating number is invalid, unallocated, or unassigned. *See* Advanced Methods to Target and Eliminate Unlawful Robocalls, Notice of Proposed Rulemaking and Notice of Inquiry, CG Docket No. 17-59, FCC 17-23 (released Mar. 23, 2017), *published in* 82 Fed. Reg. 22625 (May 17, 2017).

[59] *See* Comment of the FTC to the Federal Communications Commission, Advanced Methods to Target and Eliminate Unlawful Robocalls, Notice of Proposed Rulemaking and Notice of Inquiry, CG Docket No. 17-59, FCC 17-23 (July 3, 2017), *available at* https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-federal-communications-commission-supporting-fccs-proposed-expansion-provider/ftc_comment_to_fcc_re_nprm_noi_call_blocking_07032017.pdf. As call-blocking technology

The FTC also has engaged with technical experts, academics, and others through industry groups, such as the Messaging, Malware and Mobile Anti-Abuse Working Group ("M[3]AAWG"). M[3]AAWG is a consortium of industry, regulators, and academics focused on developing solutions to mitigate various forms of messaging abuse such as email spam.[60] After discussions with the FTC and others, M[3]AAWG leadership formed the Voice and Telephony Abuse Special Interest Group ("VTA SIG") in 2014, a subgroup formed to apply M[3]AAWG's expertise on messaging abuse to voice spam, such as robocalls.[61]

Through the VTA SIG, the FTC coordinates with experts working on industry standards that will combat Caller ID spoofing by enabling the authentication of VoIP calls, such as the Internet Engineering Task Force's working group called "STIR"—Secure Telephone Identity Revisited.[62] The FTC further promotes technical advancements by collaborating with its counterparts in other countries, through its leadership in the Unsolicited Communications Enforcement Network ("UCENet") an international syndicate of government agencies and private sector representatives focused on international spam enforcement cooperation.[63]

---

gains momentum, the FTC is mindful about concerns that bad actors may place telemarketing calls while spoofing an innocent consumer's telephone number as the outbound caller ID number in an effort to evade detection or that the inadvertent blocking of legitimate calls may occur. These concerns were also raised by the FCC and addressed in the FTC's Comment.

[60] *See* M[3]AAWG, Activities, https://www.m3aawg.org/ (last visited Sept. 22, 2017).

[61] *See* M[3]AAWG, Voice and Telephony Abuse Special Interest Group, https://www.m3aawg.org/voice-and-telephony-abuse-sig (last visited Sept. 22, 2017).

[62] *See* Internet Eng'g Task Force, Secure Telephone Identity Revisited (STIR), https://datatracker.ietf.org/wg/stir/charter/ (last visited Sept. 22, 2017).

[63] *See* https://www.ucenet.org/ (last visited Sept. 22, 2017).

3. Data Initiatives

The Commission also engages in information sharing to help facilitate technological solutions such as call blocking and has taken steps to increase the quality and quantity of shared information. To that end, on September 28, 2016, the FTC updated its Do Not Call complaint intake process to provide a drop-down list of possible call categories for consumers to choose from to make it easier for consumers to report the subject of the call and to help the Commission identify trends. The top six categories selected to date by consumers are the same for Do Not Call complaints and robocall complaints:

Reducing your debt (credit cards, mortgage, student loans)

Dropped call or no message

Vacation & timeshares

Warranties & protection plans

Calls pretending to be government, businesses, or family and friends

Medical & prescriptions

In addition to refining our complaint intake process, the FTC recently began a new initiative to help facilitate industry call-blocking solutions by increasing the amount and frequency of consumer complaint data that we make publicly available.[64] Beginning in August of this year, when consumers report Do Not Call or robocall violations to the FTC, the phone numbers consumers report are released each business day. The FTC is also releasing the following consumer-reported data: the date and time the unwanted call was received, the general subject matter of the call (such as debt reduction, energy, warranties, home security, etc.), and

[64] *See* https://www.ftc.gov/news-events/press-releases/2017/08/ftc-escalates-fight-against-illegal-robocalls-using-consumer. The complaint data is available at: https://www.ftc.gov/site-information/open-government/data-sets/do-not-call-data.

whether the call was a robocall.[65] By making our available data more up-to-date and more robust, the FTC seeks to help telecommunications carriers and other industry partners that are implementing call-blocking solutions for consumers that choose to use a call-blocking service or feature.

The Commission is committed to continuing to work with industry and government partners to improve information sharing to combat illegal calls.

III. Consumer Education

Public education is also an 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 FTC's behalf.

The FTC delivers practical, plain language information on numerous issues in English and in Spanish. The Commission also 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, the FTC's message to consumers is simple: if you answer a call and hear an unwanted recorded sales message—hang up. Period. Other key messages to consumers include how to place a phone number on the Do Not Call Registry, how and where to report illegal robocalls,[66] available call blocking solutions,[67] and how to identify common scams.[68] The FTC

---

[65] In the past, the Commission released a bi-weekly report that published only the telephone numbers that consumers complained about in their Do Not Call and robocall complaints.

[66] *See, e.g.*, National Do Not Call Registry, http://www.consumer.ftc.gov/articles/0108-national-do-not-call-registry.

[67] *See, e.g.*, FTC Consumer Information Blocking Unwanted Calls https://www.consumer.ftc.gov/articles/0548-blocking-unwanted-calls.

disseminates these tips through articles,[69] blog posts,[70] social media,[71] infographics,[72] videos,[73] audio,[74] and campaigns such as "Pass It On"—an innovative means of arming older consumers with information about scams that they can "pass on" to their friends and family members.[75]

IV. Next Steps and Conclusion

The Do Not Call Registry continues to help protect consumers against unsolicited calls from legitimate telemarketers. But, as technology continues to develop and fraudsters exploit those developments, we must remain agile and creative. The Commission will continue its multifaceted efforts to fight illegal robocalls, including 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.

---

[68] *See, e.g.*, FTC Consumer Information Scam Alerts, https://www.consumer.ftc.gov/scam-alerts.

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

[70] *See, e.g.*, FTC Consumer Information Blog, Looking to Block Unwanted Calls? https://www.consumer.ftc.gov/blog/looking-block-unwanted-calls.

[71] *See, e.g.*, FTC Robocalls Facebook Q&A Transcript (Oct. 25, 2012), https://www.ftc.gov/sites/default/files/attachments/ftc-facebook-chats/1210robocallschallenge-fb.pdf.

[72] *See, e.g.*, FTC Robocalls Infographic, https://www.ftc.gov/sites/default/files/documents/public_events/robocalls-all-rage-ftc-summit/pdf-0113-robocalls-infographic.pdf.

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

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

[75] *See* Pass It On, http://www.consumer.ftc.gov/features/feature-0030-pass-it-on#identity-theft.

- We will work with the telecommunications industry, encouraging carriers to be proactive in monitoring for illegal robocalls, blocking illegal calls, and securing the information necessary for prosecutions.

- Spur Innovation

  - We will work with industry leaders and other experts to further stimulate the development of technological solutions to protect consumers from illegal robocalls.

  - We will continue to encourage industry-wide coordination to create and deploy VoIP standards that incorporate robust authentication capabilities. 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.

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.