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

thousands of legitimate telemarketers who subscribe to

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.

telephone numbers on the Do Not Call Registry and called consumers who previously asked

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

enforcement. In addition, defendants in four of

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

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,

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-

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 27

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

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 a-2(c)44(-2(c10(a)4(-6]c -0.00nk1(b)21or)3(t)-2(a)nvi)-2(i)-2

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

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]

disseminates these tips through articles,[69] blog posts,[70] social media,[71] infographics,[72] videos,[73] audio,[74]