

**STILL RINGING OFF THE HOOK: AN UPDATE
ON EFFORTS TO COMBAT ROBOCALLS**

HEARING
BEFORE THE
SPECIAL COMMITTEE ON AGING
UNITED STATES SENATE
ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

WASHINGTON, DC

OCTOBER 4, 2017

Serial No. 115-10

Printed for the use of the Special Committee on Aging



Available via the World Wide Web: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

31-486 PDF

WASHINGTON : 2019

SPECIAL COMMITTEE ON AGING

SUSAN M. COLLINS, Maine, *Chairman*

ORRIN G. HATCH, Utah
JEFF FLAKE, Arizona
TIM SCOTT, South Carolina
THOM TILLIS, North Carolina
BOB CORKER, Tennessee
RICHARD BURR, North Carolina
MARCO RUBIO, Florida
DEB FISCHER, Nebraska

ROBERT P. CASEY, JR., Pennsylvania
BILL NELSON, Florida
SHELDON WHITEHOUSE, Rhode Island
KIRSTEN E. GILLIBRAND, New York
RICHARD BLUMENTHAL, Connecticut
JOE DONNELLY, Indiana
ELIZABETH WARREN, Massachusetts
CATHERINE CORTEZ MASTO, Nevada

KEVIN KELLEY, *Majority Staff Director*
KATE MEVIS, *Minority Staff Director*

CONTENTS

Opening Statement of Chairman Susan M. Collins	Page 1
Statement of Ranking Member Robert P. Casey, Jr.	2

PANEL OF WITNESSES

Lois Greisman, Associate Director, Division of Marketing Practices, Federal Trade Commission, Washington, DC	4
Honorable Josh Shapiro, Attorney General, Pennsylvania Office of Attorney General, Harrisburg, PA	6
Kevin Rupy, Vice President, Law and Public Policy, USTelecom, Washington, DC	8
Genie Barton, President, BBB Institute for Marketplace Trust, Arlington, VA	9

PREPARED WITNESS STATEMENTS AND QUESTIONS FOR THE RECORD

Lois Greisman, Associate Director, Division of Marketing Practices, Federal Trade Commission, Washington, DC	26
Questions submitted for Ms. Greisman	48
Honorable Josh Shapiro, Attorney General, Pennsylvania Office of Attorney General, Harrisburg, PA	58
Questions submitted for Mr. Shapiro	64
Kevin Rupy, Vice President, Law and Public Policy, USTelecom, Washington, DC	66
Questions submitted for Mr. Rupy	67
Genie Barton, President, BBB Institute for Marketplace Trust, Arlington, VA	71
Questions submitted for Ms. Barton	83

ADDITIONAL STATEMENTS FOR THE RECORD

Chris Drake, Chief Technology Officer, iconectiv, letter to Senators Collins and Casey	88
--	----

STILL RINGING OFF THE HOOK: AN UPDATE ON EFFORTS TO COMBAT ROBOCALLS

WEDNESDAY, OCTOBER 4, 2017

U.S. SENATE,
SPECIAL COMMITTEE ON AGING,
Washington, DC.

The committee met, pursuant to notice, at 9 o'clock a.m., in room 562, Dirksen Senate Office Building, Hon. Susan M. Collins, Chairman of the Committee, presiding.

Present: Senators Collins, Fischer, Casey, Nelson, Gillibrand, and Donnelly.

OPENING STATEMENT OF SENATOR SUSAN M. COLLINS, CHAIRMAN

The CHAIRMAN. The Committee will come to order. Good morning.

A couple of years ago, one of my most valued staff members retired after more than 30 years of public service. She served as Staff Director right here on the Senate Aging Committee, where she organized many hearings examining robocalls and senior fraud. She tells me, however, that it was not until she retired, and is now home during the day, that she fully realized the problem of robocalls. From morning until night, she says her phone rings, often with threatening scam artists on the other end of the line.

When Congress created the national Do Not Call registry 14 years ago, we hoped that it would end this flood of unwelcomed phone calls. Despite some initial success, phones are still ringing off the hook. Last year, Americans received an estimated 2.4 billion unwanted calls each and every month. That is about 250 calls a year for every household in the country. My husband and I received so many on our landline in Bangor that we discontinued the landline.

This morning, we will look at why Americans who have signed up for the Do Not Call Registry are still getting annoying, unwanted phone calls on both their landlines and their cell phones, and we will explore what can be done about it. We will focus especially on the importance of education, enforcement, and call-blocking technologies.

In previous hearings on this topic, we learned that changes in technology have made it possible for scammers operating overseas to use automated dialing, or robocalls, to reach victims here in the United States. This was not feasible in 2003. At that time, phone calls were routed through telecommunications equipment that was complicated to operate. This made high-volume, automated calling

difficult and expensive, particularly for international calls. Also, older equipment could not be used easily to disguise or spoof a caller ID. But now phone calls can be routed from anywhere in the world, at practically no cost, using so-called Voice Over Internet Protocol technology, or VoIP.

Combined with simple computer apps, criminals can use VoIP to generate millions of robocalls to cast a wide net in their hunt for victims. They can even spoof the number displayed by caller ID to hide their true identity, making it more likely that their intended victim will pick up the phone.

But just as technology has enabled these frauds, it can also be used to fight back. Today we will learn about technologies consumers can use to block illegal robocalls. We will also hear about the Robocall Strike Force, a collaboration between telecommunications and technology companies that are working together on ways to identify robocall traffic at the network level, and block it before it even reaches the consumer. We will assess whether or not the telecoms are doing enough, quickly enough, to protect their customers.

Aggressive law enforcement is also key to stopping illegal robocalls. In a case brought by the Department of Justice last year, dozens of individuals, operating through call centers in India, were indicted for allegedly defrauding tens of thousands of Americans out of hundreds of millions of dollars, using the notorious IRS impersonation scam. That is the most commonly reported scam to our Committee's Fraud Hotline.

Our own data show that these arrests had a real impact. Prior to the arrest, nearly three out of every four calls to our hotline involved the IRS impersonation scam. But in the three months after the arrest, reports of the scam dropped an incredible 94 percent. Though the numbers have since rebounded somewhat, they are still far below the levels we have seen in the past. The point is that law enforcement works. It deters others from committing the crime.

If we are going to win this fight, we need to better our understanding of these con artists and their scams and how they operate. What we learn will help inform those who are most at risk, particularly our older Americans, so that they do not fall victim to these scams.

The witnesses who are testifying today have invaluable insights, and I look forward to hearing their testimony.

It is now a pleasure to turn to the Ranking Member Casey for his opening statement.

**OPENING STATEMENT OF SENATOR ROBERT P. CASEY, JR.,
RANKING MEMBER**

Senator CASEY. Chairman Collins, thank you very much for calling this hearing today. This issue of robocalls is personal to many people in this room. In fact, just recently, a con artist, likely using robocalling technology, contacted my wife, demanding money. She knew to hang up the phone. I am not sure if she said something in the course of hanging up—I did not get that information—but then she, of course, reported it to one of the Aging Committee's Fraud Hotline personnel. That would be me.

[Laughter.]

Senator CASEY. But that is not atypical across the country. All too often, unsuspecting individuals fall victim to these same con artists. Worse yet, we know that certain types of scams may target older adults, specifically, or may have a disproportionate impact on them.

At our February hearing on scams, we heard about an 80-year-old from Montgomery County. Her name is Arlene, and it happens to be the Montgomery County in Pennsylvania, not Maryland. Arlene was scammed out of more than \$800,000 through calls she received, claiming that she won an international lottery. We all have a sacred responsibility to do more to ensure that con artists do not scam our loved ones out of one more penny of their nest eggs.

This is going to take continued commitment at the federal, state, and local levels, and among others, including those in the telecommunications industry. For example, the Senate recently passed the Elder Abuse Prevention Act. This bill provides law enforcement officials with the tools to prosecute con artists and bring perpetrators to justice. The House should pass this bill without delay.

The FCC has proposed a rule that will help to deter con artists from disguising themselves as a government agency or a local business, in an effort to entice someone to answer the telephone. Thieves should not be able to spoof the phone numbers that all of us know and answer every day. It has been 8 months since the rule was proposed by the FCC. This rule should be finalized and implemented immediately, and education and awareness are also a key part of this.

I spent the month of August going across Pennsylvania, to 32 counties, and had the chance to visit with many older Pennsylvanians. We discussed issues that range from Medicare to Meals on Wheels. But when I spoke about the Committee's work on fraud and scams, I asked folks in the audience to raise their hand if they had ever been contacted by a con artist. Nearly every hand in the room went up.

Keeping people informed of these scams and the latest methods of con artists goes a long way to preventing seniors from ever falling victim. We have a lot of complicated issues to tackle here in Congress, but this is not one of those complicated issues. To the scammers out there, we say this: Your time is up. You will not steal one more penny from seniors without suffering the consequences.

I look forward to hearing from our witnesses today about what more we can be doing, collectively, to ensure that older Americans do not lose that one more penny to thieves falsely claiming to be the IRS or a grandchild in need of rescuing.

On a logistical note, I do want to thank Chairman Collins for starting the hearing 30 minutes early. This morning, as she knows, I have a Finance Committee hearing that is marking up a bill to extend the Children's Health Insurance Program, which expired over the weekend, and must be reauthorized in order to ensure that millions of young children are not without coverage. In order to express my support for that program I will be leaving the hearing briefly to go to that, but I will be back.

So, Chairman Collins, thank you for doing this so early. It is a record early start for a hearing here in the Senate. Thank you.

The CHAIRMAN. Senator Casey, I was very glad to accommodate you. I know how important it is to get the CHIP program reauthorized. I was a very early supporter and co-sponsor of it many years ago, and I hope it will slide through the Committee, with your help.

We now turn to our panel of witnesses. First we will hear from Lois Greisman, Associate Director of the Division of Marketing Practices of the Bureau of Consumer Protection at the Federal Trade Commission. She has testified many times before our Committee on various issues involving consumer fraud and we welcome her back today.

I would now like to call on Senator Casey to introduce the next witness, who is from his home state.

Senator CASEY. Thank you, Chairman Collins. I am pleased to be introducing Josh Shapiro, the Attorney General for the Commonwealth of Pennsylvania, someone I have known for a long time, someone who has a deep commitment to public service, someone of great integrity. His work as attorney general has focused on educating and protecting seniors from unfair health care practices, financial exploitation, fraud and scams, and that is just the beginning of the work that he does.

Under Attorney General Shapiro's leadership, the office's Senior Protection Unit has committed increased resources and energy to addressing complaints from seniors and conducting grassroots education for seniors in every community.

I would like to thank the Attorney General for making the trip to DC today from Pennsylvania, and I look forward to his testimony. Thanks, Josh.

The CHAIRMAN. Thank you, and I welcome you as well.

Next we will hear from Kevin Rupy, who is Vice President for Law and Policy at USTelecom, located right here in Washington. USTelecom is the industry trade association representing most of the major telecommunication carriers as well as some of the smaller, rural carriers.

And finally we will hear from Genie Barton, President of the Better Business Bureau Institute for Marketplace Trust, in Arlington, Virginia.

We welcome you all and we will start with Ms. Greisman.

STATEMENT OF LOIS GREISMAN, ASSOCIATE DIRECTOR, DIVISION OF MARKETING PRACTICES, FEDERAL TRADE COMMISSION, WASHINGTON, DC

Ms. GREISMAN. Thank you and good morning, Chairman Collins, Ranking Member Casey, members of the Committee. I am Lois Greisman with the Division of Marketing Practices at the Federal Trade Commission. I am honored to have the opportunity to return before this Committee to discuss the FTC's work to fight illegal robocalls, including those that harm seniors.

As you have stated, all of us, the entire country, is keenly aware of the robocall problem, namely unwanted, abusive telephone calls, disturbing consumers' privacy, and frequently using fraud and deception to pitch goods and services which cause significant harm. None of us has been immune from these illegal calls, and the steady and sharp rise in our complaint numbers reflects consumer frustration and resentment.

Since the start of 2017, on average, every single month, the FTC receives 400,000 complaints about robocalls. That is a daunting number. But the complaints are truly valuable to law enforcement. We mine the data. We use it to identify bad actors and to build out our enforcement cases. Further, the complaints are also valuable to carriers and to third parties who use them to assist in their call-blocking efforts. As noted in the testimony, the Commission now is releasing its data to the public on a daily basis, some 25,000 telephone numbers each business day, with additional information on the date and time of the call.

In response to illegal robocalls, the Commission continues to deploy its full range of resources, law enforcement advocating technological solutions, and, of course, robust consumer and business education. Our law enforcement efforts to combat all Do Not Call violations, which include robocalls, are unabated.

Since 2004, when we started enforcing Do Not Call, no less than 131 enforcement actions have been filed against 163 companies and 121 individuals. So far, 124 of those cases have been resolved. And I want to emphasize that many of the recent cases we have brought have stopped individuals and companies that have been placing literally billions of illegal robocalls.

Now while telemarketers are happy to abuse and take money from consumers of all ages, we have seen some that appear to target or disproportionately impact older consumers. For example, one telemarketing fraud we recently shut down specifically promoted debt elimination programs to help seniors eliminate their debt.

These cases can be challenging, as defendants seek to evade detection by using caller ID spoofing, and we have sued call centers operating abroad, running, for example, government imposter scams to con consumers into paying hundreds of dollars for taxes or debt they do not owe.

And, of course, not all illegal telemarketing is conducted by scammers. The recent and historic \$280 million civil penalty order against DISH network shows that even some legitimate companies fail to abide by the law. That litigation dates back to 2009, when the Department of Justice filed the case on behalf of the FTC and four state co-plaintiffs.

We know that sustained law enforcement alone will not stem the tide. Through no less than four robocall contests, the FTC has spearheaded efforts to develop technological solutions to the robocall problem. Real progress is being made. For the past several years, the FTC encouraged carriers and others simply to develop call-blocking technologies. We met with a good deal of resistance and we worked hard to address many valid concerns.

Today, however, we now have a good number of call-blocking tools in the marketplace and the discussion has shifted somewhat to best practices for call-blocking and related issues, many of which are teed up in the recent FCC Notice of Proposed Rulemaking and Notice of Inquiry. This is an important shift in the debate, and it reflects meaningful progress. But we remain miles behind providing the level of protection against unwanted calls that consumers deserve.

Our work is ongoing. This very week we are meeting again with industry members, technologists, and others from the international

community to address robocalls and promote technological advancements.

Finally, and often with assistance from your offices, the FTC continues to push out a large quantity of high-quality educational messages to all. Just this past Monday, we issued an FTC blog providing important information on call-blocking.

So to sum up, while I am very proud of the work the FTC has done to curb illegal robocalls, we know we still have a significant consumer protection problem, and I commit to you that we will not let up our efforts to curb these abusive calls.

Thank you. I look forward to your questions.

The CHAIRMAN. Thank you. Attorney General Shapiro.

STATEMENT OF THE HONORABLE JOSH SHAPIRO, ATTORNEY GENERAL, PENNSYLVANIA OFFICE OF ATTORNEY GENERAL, HARRISBURG, PENNSYLVANIA

Mr. SHAPIRO. Thank you, Chairman Collins, Ranking Member Casey, Senator Gillibrand, members of the Committee. It is an honor to be with you and I am grateful for your attention to this important matter. Forty-seven million seniors in this country, representing roughly 17 percent of the population in Pennsylvania, makes this, combined with the threats against seniors, a top priority for mine, as Pennsylvania's Attorney General.

Senior citizens are specifically targeted for fraud and scams more than any other age group, and the data shows that, and seniors today are more easy to reach than ever before, with 67 percent of seniors online, and this generation of seniors actually representing the wealthiest generation of seniors as compared to the war babies generation and others, making them a prime target for access and availability of resources that can be scammed.

The combination of scammers' greed and seniors' vulnerability has resulted in significant financial losses for Pennsylvania's elderly and America's elderly. Over a third of seniors have experienced some form of fraud and financial abuse, including scams, and the average senior loses \$36,000 per scam.

The Pennsylvania Office of Attorney General dedicates significant resources to combating these types of scams and for consumer protection. We receive 20,000 complaints each year from Pennsylvanians, and the most common complaint, Madam Chair, that we receive, is from seniors about violating the Do Not Call list, or telephonic scams.

IRS impersonation scams are at the top of that list, where they call people and falsely claim to represent the Internal Revenue Service. The callers will claim that, say, back-taxes are owed by the recipient. They threaten to have them arrested and demand payment, typically via wire transfer. Last year, my office received 881 complaints about IRS impersonation scams, 62 percent of which were targeting seniors.

Fortunately, Pennsylvanians are typically able to recognize those calls as fraudulent. In the past, it really helped to know that the IRS did not call people about their taxes and they only sent letters. However, in April, Congress authorized the IRS to begin contracting out some of its debt collection work to private debt collec-

tors who do, in fact, make phone calls, and take away this defensive knowledge.

I want to share with you one story of a case that we are currently working on, and because we are currently working on it, Madam Chair, I will not share the person's name. We will call him John.

In May of this year, agents in my office received a complaint from a man in the Pittsburgh area, in western Pennsylvania. Again, I will call him John to protect his identity, as this investigation is ongoing. John received a call from a 1-866 number, who claimed to be an IRS employee. The caller said that an arrest warrant had been issued for John because he sends money to his wife and child in a foreign country. The purported IRS employee then said that John would soon receive a call from the local police department and instructed him on how to merge the calls together.

Shortly thereafter, John received a call from a number, and the caller ID showed that it was actually someone calling from the Pennsylvania State Police. The callers then, together, threatened John and said his only way out of this situation as to send money to help pay for an investigation to clear his name. John then, through a series of wire transfers, ultimately sent \$13,500 of his hard-earned money to these scammers.

Unfortunately, these kinds of cases are very, very difficult to prosecute. Criminals hide behind these spoofed phone numbers, using shady financial transactions, leaving little for law enforcement, here in the state or federally, to work with. That is why one of the best approaches we find is preventative education, and the preventative education aspects of what we do, I am happy to discuss later on in question-and-answers.

But recognizing, Madam Chair, the limited time we have, I would like to close by suggesting two reforms that this Congress, again, respectfully, might consider that would help us do our job better.

First, prevent IRS debt collectors from calling in the first place. As I mentioned earlier, we used to be able to tell seniors that if anyone was calling you claiming to be from the IRS, hang up immediately because it is a scam. I would respectfully request to this Committee that you carefully look at the effects of permitting debt collectors, working on behalf of the IRS, to make telephonic calls to people whom they are collecting debts.

And second, Madam Chair, I would ask that we give telephone companies the tools to block scammers. Seventy-five percent of consumers who file fraud-related complaints, and reported how the fraud was perpetrated, indicated that they were contacted by the telephone. That is why the Federal Government needs to give telephone service providers the ability to block the kind of spoofed calls that targeted John in the story I shared with you before.

Look, we have Do Not Call lists, and often times seniors will say to me and Senator Casey, when we are back in Pennsylvania, "But they still called." Well, that is because scammers do not pay attention to the law, and when they can use these spoof technologies to get around it, it is very troublesome.

I know Senator Casey shares my views on this issue. He and I, later today, will be sending a joint letter to the FCC to ask them

to implement their proposed rule without further delay. It is also something that 29 attorneys general joined together in a bipartisan basis to appeal to the FCC to allow these telephone companies to block these spoofed calls.

Madam Chair, there is much to cover and a lot more in my prepared testimony, but mindful of the time I will yield at this moment and look forward to your questions. Thank you again for having this hearing.

The CHAIRMAN. Thank you very much, and the case that you described, it is very similar to one that we had in Portland, Maine, and highlighted at a previous hearing, where the spoofed number was from the Portland Police Department, right after the IRS impersonation call had come through. That second call is what convinced the individual to part with his money. So I appreciate your mentioning that.

Mr. Rupy.

**STATEMENT OF KEVIN RUPY, VICE PRESIDENT, LAW AND
PUBLIC POLICY, USTELECOM, WASHINGTON, DC**

Mr. RUPY. Chairman Collins, Ranking Member Casey, members of the Committee, thank you for giving me the opportunity to appear before you today.

My name is Kevin Rupy and I serve as Vice President of Law and Policy at USTelecom. Over the last several years, USTelecom and our member companies have been tremendously focused on the robocall issue, and we share the Committee's concern about the problems associated with phone-based imposter scams targeted at seniors.

Calls using VoIP technology, when combined with caller ID spoofing, can be used by scammers to mask their identity and location, giving their target a false sense of confidence about who is calling.

In this ongoing battle against criminal robocallers, there have been three important developments over the last year that are particularly significant.

First, the industry-led, ecosystem-wide Robocall Strike Force issued its report to the FCC on October 26, 2016. Follow-up reports by the industry groups, continuing the work started by the Strike Force, were delivered to the FCC on April 28, 2017. The reports note that the SHAKEN/STIR standards development for the next generation of robocall mitigation tools have been accelerated by six months. These standards, which incorporate caller ID authentication capabilities into the network and consumer devices, have entered the industry testing phase. Some of the initial testing of the SHAKEN standard is expected to complete later this year, with additional potential deployments anticipated as early as 2018. The reports also highlight the increasing number of tools that are being developed and actively deployed to consumers by a growing number of national voice and device providers.

Finally, the reports detail the efforts of USTelecom's Industry Traceback Group, which is comprised of a broad range of network providers from several industries, who are working collaboratively to identify the origin of these calls at their source.

Industry's strong commitment to this effort can be seen in its significant growth over the last year, from three carriers in July 2016, to 22 carriers as of today. The goal of this group is to identify the source of the worst of these illegal calls and further enable enforcement actions by federal agencies. In this regard, we applaud the FCC's three enforcement actions since June of this year that have resulted in more than \$200 million in proposed fines targeting perpetrators of illegal robocalling, as well as the complementary enforcement actions by the FTC.

Second, the reports show that USTelecom member companies, independent application developers, and a growing number of diverse companies offer services today that can help older Americans reduce unknown and potentially fraudulent calls. For example, AT&T has launched its Call Protect service that allows customers with iPhones and HD Voice-enabled Android handsets to automatically block suspected fraudulent calls. Verizon has been trialing a service that warns its wireline customers about calls identified as suspicious, and on the wireless side has deployed robocall mitigation features as part of its Caller Name ID service. And various carriers have worked with NoMorobo to facilitate their customers' ability to use that third-party blocking service.

Third, the FCC recently published a rulemaking in which it proposes to clarify rules for when voice providers may block certain types of calls. USTelecom supports the proposed rules and has participated fully in the proceeding. One issue the FCC raises is what protection legitimate callers should have if their calls are blocked due to the inappropriate scoring of that call. It is an issue USTelecom and other parts of the robocall scoring ecosystem have been wrestling with for years, and this fall we are hosting a workshop aimed at helping develop best practices for the scoring and labeling of calls.

All these recent developments further demonstrate the essential commitment from a broad range of stakeholders that will be necessary to effectively mitigate and defeat these scammers. Industry stakeholders from a wide range of companies have advanced a concerted, broad-based effort focused on developing practices, technologies, and methods for mitigating phone-based attacks and scams. This coalition has also expanded its cooperation with equally important stakeholders within the Federal Government and with consumer groups. While our partners in government play a crucial enforcement role, our partners in consumer organizations are vital to raising awareness about the tools available to consumers to help mitigate illegal robocalls.

In closing, let me again thank the Committee for holding this timely hearing. We share the Committee's concerns and we look forward to our continued work together to address this constantly evolving challenge.

The CHAIRMAN. Thank you. Ms. Barton.

**STATEMENT OF GENIE BARTON, PRESIDENT, BBB INSTITUTE
FOR MARKETPLACE TRUST, ARLINGTON, VIRGINIA**

Ms. BARTON. Chairman Collins, Ranking Member Casey, members of the Committee, thank you for giving me the opportunity to appear before you today.

I am Genie Barton and I serve as President of the BBB Institute for Marketplace Trust. We are the 501(c)(3) educational arm of the Council of Better Business Bureaus, the umbrella organization of the more than 100 BBBs serving communities across North America.

Our mission is to advance trust in the marketplace, by protecting consumers and promoting ethical business practices. Scams not only cost the American economy around \$50 billion each year, they erode trust, humiliate their victims, and litter our daily lives.

In this testimony, I will summarize BBBI's insights about scams that prey on seniors, especially those initiated by robocalls. The data that I will share are derived from Scam Tracker, our crowd-sourced, interactive, online tool that collects consumers' own reports of actual scams and presents them in a searchable, online heat map. Scam Tracker shows consumers the number and types of scams in their communities, and provides a view into the changing scam landscape to all. The data are shared with the FTC for inclusion in the Consumer Sentinel data base, the National Cyber Forensics and Training Alliance, and law enforcement agencies for investigative purposes, on request.

Our two recent white papers have shattered stereotypes about scams. In cracking the invulnerability illusion, we found that millennials, who think only old and gullible people are at risk, are, in fact, the most scammed, while seniors, who know that they are at risk, are less likely to be scammed. The cost to seniors, however, is much higher. When scammed, seniors suffer nearly 56 percent higher financial losses from scams than any other demographic. Because many retirees live on a fixed income, older people can be harder hit than others by scams.

In our other white paper, the Scam Tracker Risk Report, we introduced the BBB Risk Index, which replaces a risk assessment by frequency alone of exposure with a new three-dimensional model—exposure, susceptibility, and monetary loss. This provides a more meaningful measure of the relative risk of a scam and can help inform policy choices and resource allocation.

Based on the Risk Index, the 10 riskiest scams for seniors are fake family friend emergencies, tech support, sweepstakes lottery prizes, travel vacations, investment, foreign money exchange, home improvements, online purchases, tax collection, and fake check money orders. For seven out of these 10 scams, the method of initial contact was a telephone call, often initiated by a robocall.

Of all the scams reported by seniors aged 65, 71 percent began with a call. Fortunately, just 33 percent of those calls involved monetary loss, according to our data. The highest percentage of robocall scams for seniors were “can you hear me now?” scams, at 34 percent, but losses were extremely low.

The tax collection, or IRS scam, represents 20 percent of all robocall, robo-initiated scams. In 2016, approximately 27 percent of all scams reported to us by seniors, and 16 percent of scams across all age groups, were tax collection scams. While only one in 278 of these reports involved a dollar loss, the median loss of \$3,000 for seniors is higher than for any other demographic.

As I close, let me say that Scam Tracker, along with our other programs focusing on consumer protection and financial and digital

literacy, help us to take the pulse of the marketplace and empower consumers to recognize the red flags that scams and deceptive practices perpetrate.

Thank you very much for inviting me to be here today to share our data, our messaging, and our outreach, to help fight back against the scourge of scams. I would be pleased to answer any questions you may have.

The CHAIRMAN. Thank you very much.

Senator Casey, I know that you have to leave. Would you like to ask a question before you do so?

Senator CASEY. I appreciate that, Madam Chair. I will maybe just get one question in I wanted to ask Attorney General Shapiro, with regard to the FCC. As you know, the FCC has proposed a rule—we mentioned that earlier—that will help curb spoofing and make it a bit harder for con artists to disguise themselves. Earlier this year, the two of us wrote separate letters to the FCC requesting the proposed rule be finalized, and later today we will be sending a joint letter asking for the same.

Why do you believe this rule is so important at this time, to have it implemented, and how will it help you in your work as attorney general, attacking these schemes?

Mr. SHAPIRO. Well, Senator, thank you for your question, and also, again, thank you for your leadership in this area.

Look, scammers are only successful if they can pretend to be someone else, right? We know that these scams have a 0.5 percent success rate, so we know that the combination of education and outreach, the good work that this Committee and others are doing to make seniors aware of these kinds of scams, it is working. But still, this 0.5 percent, because of just the sheer magnitude, the sheer volume of the number of calls, is something that ultimately is still hitting a lot of seniors in Pennsylvania and across the United States.

I spoke about the example of the John case in the Pittsburgh area here in Pennsylvania. We need, in law enforcement, to have all of the tools necessary to stop this.

Senator, I will share with you that we issued 2,141 subpoenas last year, in cases involving these kinds of calls. It only resulted in four legal actions. Part of that is because the spoofing technology is so difficult to penetrate, it is so difficult for us to get to the bottom of, that it becomes very hard to trace it back to the scammers, and ultimately prosecute them. And we are working incredibly hard at this, as I know my colleagues are around the country as well, and it has still only resulted in four actions.

If the FCC gives the telecom companies the power to stop these kind of spoof calls, it makes our job in law enforcement easier to protect seniors from these kinds of scams.

I would note, Senator, that your letter to the FCC, others, represents a bipartisan commitment at the highest levels of government. I am hopeful that the FCC will do this.

To be frank with you, I cannot imagine a reason why the FCC would not approve this. The telecom companies have the technology available to them to stop these spoof calls. We should allow them to flip that switch on and do that work. And so having the strength of this Committee, having the strength, Senator, of you,

29 attorneys general coming together behind this, it is going to make us be able to deal with the task of protecting seniors from telephonic scams easier and more successful.

Senator CASEY. Thanks very much. Madam Chair, thank you.

Senator NELSON. Madam Chairman, I have got to go to the same mark-up—

The CHAIRMAN. Why don't you go ahead.

Senator NELSON [continuing]. As Senator Casey, but I just want to say thank you. We started this five years ago. That is hard to believe that much time has passed. Thank you.

I have the privilege of being the Ranking on Commerce that has telecom jurisdiction, that has FCC jurisdiction. That is an excellent suggestion, Attorney General Shapiro.

Mr. SHAPIRO. Thank you, Senator.

The CHAIRMAN. Thank you very much, Senator Nelson.

I have to say, in following up on Senator Nelson's comments, that it is very frustrating to hear all that is being done and yet realize that these robocalls are still continuing at an unprecedented rate. I would like to ask each of you—I think Attorney General Shapiro has answered in part but may want to add something—what more should we be doing? What specific action is needed?

It sounds like we no longer have the technology problem that we once had, the technology is there, we are making efforts to educate consumers, but the calls are still coming, even if the success rate has dropped. And it is so frustrating that the American people are being harassed by 2.4 billion unwanted calls each and every month. So what do we need to do to bring this to an end?

Ms. Greisman, we will start with you.

Ms. GREISMAN. Thank you, and, of course, we all share the same frustration with these unwanted calls. I do not think the technology is there yet. I think we have made tremendous progress, but as Mr. Rupy indicated, they are still beta testing a lot of the call authentication methods and also other factors that are sometimes referred to as data inputs that go into call-blocking technologies to make it more intelligent, more accurate.

So I think that we are still looking for a better technological fix than is currently available, and, of course, we will continue to sustain law enforcement and our educational outreach efforts.

The CHAIRMAN. Mr. Shapiro?

Mr. SHAPIRO. Madam Chair, I spoke before about two recommendations. Just to reiterate very briefly, preventing the IRS debt collectors from contacting individuals directly, and I absolutely respect the Congress's efforts to collect outstanding debts. I just think that more focus needs to be on how those calls are made and doing so in a way that is more transparent.

Second is we have talked about here today is allowing the FCC to block these scammers. And then, finally, I would suggest that there would be greater emphasis placed on education and outreach. I am a huge believer that if you empower the population that you are there to serve and protect, and they can stop a scam in their tracks, ultimately there is less work for attorneys general, district attorneys, and others to do, and that is a good thing.

We have an initiative in our office, in Pennsylvania, called SCAM, and we try and alert seniors to understand what SCAM

stands for. Any kind of sudden—S—contact—C—acting now, urging a senior to do something right away—and the M, for money, you know, to send money over. That is a scam, and we want to alert seniors to that. And more and more, as they wise up to it, they are not only able to stop a scam but they are actually in a position to help educate other seniors to prevent scams there. And hopefully that 0.5 percent success rate, which, again, sounds small but represents a lot of seniors, can come down.

So we are hopeful that as the Congress considers funding bills and other initiatives, that there be resources put in specifically to driving home that message and focusing on education.

The CHAIRMAN. You know, your suggestion about preventing IRS debt collectors from calling, or at least setting up some guidelines, rings very true with us because we, too, advise seniors that one way they could tell that it was a scam was that the IRS would never call you—

Mr. SHAPIRO. Correct.

Chairman COLLINS [continuing]. Especially without sending a certified letter first. We are going to have to rewrite all of our fraud book materials and our little postcards to update that because of the contracting out of those functions. So I think that is a good point.

Mr. Rupy, you mentioned that it was about a year ago that your Strike Force presented its report to the FCC. Comment for me on whether the technology is there or whether the FCC is just too slow in this area.

Mr. RUPY. Thank you for that question, Senator, and with regard to that technology, that is a very good question and it is an important question. And one of the things I would note is that in the Strike Force report there is obviously a lot of discussion about SHAKEN/STIR standard, which has been in development.

One of the things I would note in that was that even before the launch of the Strike Force, industry was working toward that standard, because we realize that at the core of this issue, that you have heard several witnesses talking about today, is that problem of caller ID spoofing and the lack of trust in that caller ID information.

SHAKEN/STIR goes to that, and our industry members, a broad range of industry members were working on that prior to the launch of the Strike Force, and because of the Strike Force those standards were accelerated by six months, which is good news for consumers. Because what you are seeing now are multiple providers conducting testing through the standards organization, ATIS, for this standard, to make sure it is functional and operates on their networks. And industry is committed to getting that standard deployed and into the network.

But one of the other things I would note, that Ms. Greisman mentioned, that I think is an important shift, that is also included in the Strike Force Report, is that you are seeing a growing diversity of consumer tools that are available today. You are seeing major national providers that are deploying these tools, and that is an important shift. So you are seeing companies like AT&T are partnering with companies like Hiya; Verizon, Sprint are partnering with companies like TNS Cequent; First Orion

PrivacyStar partnering with T-Mobile to put these types of important consumer tools into the hands of consumers.

The only other thing I would mention, that I would just echo, I wholeheartedly agree with Attorney General Shapiro that education is crucial on this. I think education is a very important component on this, and I would of course agree that enforcement, as well, is a tremendously powerful tool on this front. As folks have indicated, when those arrests happened in Mumbai, India, for the IRS scam, the complaints to the FTC, to the IRS, to the Senate Aging Committee's own hotline plummeted, and that just shows that you are pulling this problem out at the root with good enforcement. And we certainly want to partner with our partners in government on that.

The CHAIRMAN. Thank you. Ms. Barton.

Ms. BARTON. I really would like to echo what you, Senator Collins, have said about education and what Attorney General Shapiro has said. We are all about consumer education and simple messaging that people can hold onto, and we are also about reporting. Scam Tracker is our tool, both for awareness and for reporting, and what we find is that 49 percent of all people who report a scam do it in order to stop scammers from doing it to someone else. So the thought that having people fight back, be empowered, and pass it on is very important.

We also keep up with trending scams, and on the side of Scam Tracker there is a place to click for the latest trending scam, so people can learn more about it. There are also, if you look up a scam, you will get resources to learn more about that scam.

I will also say that our messaging about the IRS scam used to be much simpler. We used to simply say, "The IRS will not call you." Now we have had to change that messaging to say, "The IRS will not threaten you. It will not empower law enforcement to threaten or arrest you." And, very importantly, the scammers often use gift cards, redeemable at stores like iTunes, and they force victims to purchase numerous cards and read the numbers off to avoid being arrested.

We need to tell people, "You only pay either through the IRS portal or by check made out"—it has to say U.S. Treasury. The IRS will never ask you to go get a prepaid card.

But those messages just took me longer to say. And we also find that it is hard for people—the idea that you will never be contacted without a letter first is really not as helpful as we wish it would be, because you can get a letter and a scammer can still call you. It is very easy for scammers to actually look up credit reports and see that you have a debt, and then say, "We are calling to collect this."

So it is very, very hard to work that way. The simpler the messaging, and the more, if we are not going to stop calls, then we need, really, to monitor the aggressiveness of the private companies that are calling, particularly seniors.

So those are just a few thoughts. I also think that, as Mr. Rupy said, we all need to work together, and that includes, obviously you have the power to legislate. Regulatory agencies such as the FTC and the FCC have the power to enforce and pass rules. We have the power to educate and to work with both consumer groups and

businesses, and to urge consumers to report. There is no stigma in reporting, and unfortunately they think there is.

The CHAIRMAN. Thank you. Senator Donnelly, you have been very patient. Please feel free to take some extra time in your question.

Senator DONNELLY. Thank you, Madam Chair, and to the attorney general, I just want to follow up on what Ms. Barton was asking about, or was telling us about, I should say, and that is in regards to the IRS. What would you tell the people of Pennsylvania and the people of this country as to how to prevent them becoming part of an IRS scam, that you see out there?

Mr. SHAPIRO. Thank you, Senator Donnelly, and again, I would just echo, I think, the sentiment of the panel here that our job was easier. My job in law enforcement was a lot easier before Congress gave the authority to these, you know, third parties to go out and make these calls for collection. I would respectfully urge this body to revisit that and ideally do away with it, but at the very least have very, very specific transparency methods, and have those methods be communicated to seniors across Pennsylvania, and—

Senator DONNELLY. Let me ask you this, just on that point that you just made, that there be very specific methods. Probably likely that groups like the group in Indiana, and all of them, would not care less about the very strict rules we put in place regarding this, if that was what we were to do going forward, would they?

Mr. SHAPIRO. Are you referring to a scammer or to a legitimate call center?

Senator DONNELLY. To a scammer, yeah.

Mr. SHAPIRO. Well, absolutely. The scammers do not pay any attention—

Senator DONNELLY. Right.

Mr. SHAPIRO [continuing]. To what the rules are, certainly. So on that point, then, I think it comes back, Senator, to the education piece, and alerting seniors as to what is ultimately, you know, a legitimate call.

Senator, I think one of the biggest challenges we face on the education front, and from hearing from seniors, is that they are very embarrassed and ashamed when it happens, and I do not think we can underestimate the effect of that. Furthermore, I do not think we can underestimate the fact that when it occurs, and they are embarrassed and ashamed, and really unwilling to call and—

Senator DONNELLY. And scared, probably, too.

Mr. SHAPIRO [continuing]. Tell someone—right, and scared, Senator—is they do not know who to call, right?

Senator DONNELLY. Right.

Mr. SHAPIRO. I am the attorney general representing 13 million Pennsylvanians. They do not always know to call me. They probably know that calling 911 is not the right answer, right? This is not like a burglar breaking into their home where they would call 911.

I think that there—I would respectfully suggest to this body that there be more of an emphasis focused on where federal dollars go to aging organizations in all of the states, so a AAA, an area aging agency—I always forget the acronym there. When federal dollars go there, that there be some requirement that they be repositories of

these kinds of complaints and also have educational materials from the Federal Government that can be disseminated to seniors.

Other points of contact, whether it is Meals on Wheels or other things that the Federal Government funds, if seniors know that they can go there and get information, and the Federal Government knows that they can share information and it can be a two-way street, that would also help us, so that there is a point of contact.

We are working our tails off in Pennsylvania to let seniors know they can call us. I am sure the same is the case with Attorney General Hill in Indiana. But the reality is, seniors are ashamed, they are embarrassed, they do not know where to call, and they do not have access to the information, and the more education we provide, the fewer scams are going to be successful.

Senator DONNELLY. Well, in that leads to my next question. Ms. Greisman, what have you found to be the most effective ways to educate our seniors in regards to these phone scams, and to make it so that they are comfortable to try to find out more information, to be willing to make the call and say, "Hey, I think I might be getting scammed"? What are the best sources to contact them, to let them know to kind of enter their world, to provide them with the information to be on your toes on this stuff?

Ms. GREISMAN. Well, Senator, we do have a signature education piece that is targeted at active seniors, and, in fact, Ms. Barton referred to it. It is called Pass It On, and it is constantly being updated with new information. The way it is structured, it talks about various types of scams. So, for example, charitable scams which are often initiated through telemarketing, imposter scams, which is where the IRS scam falls in. And the goal of Pass It On, the way it is structured and it was based upon research in the field, is to empower seniors to share the information that they gain from Pass It On with others, to become visible in their communities as a go-to person, if somebody receives a call and they are questioning, does it sound right, is it good enough?

And that is a piece that, through your offices, we have successfully disseminated throughout the country, and will continue to do so.

Senator DONNELLY. Thank you, Ms. Greisman. Thank you, Madam Chair.

The CHAIRMAN. Thank you. Senator Casey.

Senator CASEY. Thanks very much. I wanted to go back to an issue we raised earlier, the Elder Abuse Protection and Prosecution Act, which, in fact, passed the House last night by voice vote. I wanted to ask Attorney General Shapiro about that as well.

The legislation will, among other provisions, provide law enforcement officials with prosecution tools to reduce crimes against seniors and bring perpetrators to justice. I know how important this is to you and to your work.

Just from a purely law enforcement perspective, how do you think this will help you in your fight to curb both frauds and scams in ways that would help this bill with your efforts at the state level?

Mr. SHAPIRO. Thank you, Senator. I think this bill would be very helpful to us in law enforcement. Look, I think we all agree, we

need to punish the criminals who scam our seniors, and so this bill would give some added tools to us. It would provide us with more resources and personal power, which, of course, is always good in this effort.

In my experience, I think you see this dealing with the heroin and opioid epidemic, which I know, Senator, you and Chairman Collins and others have worked so diligently on. Having greater collaboration in law enforcement between federal, state, and local partners is really key, so this bill would increase the possibility for that and increase the information-sharing that is available.

I like, in the bill, that it increases training for federal investigators and prosecutors, and it equips each judicial district with someone specifically knowledgeable about the kind of elder abuse cases that are out there. I would love to see some of those dollars come to state prosecutors as well, so that we can be part of that training.

I would also say that having the elder abuse coordinator, I think it is called, within the FTC—I do not want to speak for the FTC—but to me it seems like a very good idea.

So, overall, I think this is a really important piece of legislation and I would urge its passage.

Senator CASEY. Thanks very much. I wanted to move to Ms. Barton with regard to the IRS impersonation scam problem. It is the top scam reported to the Aging Committee fraud hotline in the calendar year 2016. In an effort to prevent our loved ones from being a victim, we have been saying that the IRS will never call you about your taxes. Unfortunately, the IRS recently contracted with private debt collectors—and this has been mentioned already today but it bears repeating—to call and collect from taxpayers, and scammers are onto this. The IRS is warning consumers about a scam based on this program.

Has the new program changed the way that you message about these IRS scams, and what do you think Congress can do to help address any confusion that the new private debt collection may cause?

Ms. BARTON. Senator Casey, thank you for that question. We share everyone's concern and we, too, have had to change our messaging. We are getting it out. We have over 100 BBBs that are in their local communities. They spend a lot of time with seniors, in various parts of the community, and Meals on Wheels, in senior centers. And we are all getting the message out, they will never arrest you, they will never threaten you, and here is where you send money. Do not ever use any method or any payment except to the U.S. Treasury. Pay through the portal.

What can you do to help? I really think that education, with all due respect to the IRS, needs to be more robust. A press release is not the same as a public service announcement, as paid advertising, and the kind of outreach that we, the FTC, and others, are doing. It is hard to message. We have gotten a lot of media attention with our reports, both locally and nationally. These are the kinds of things, they do not reach everyone but they reach a lot more people.

Senator CASEY. Thanks very much. In the interest of time I will submit some more questions for the record.

Thank you, Madam Chair.

The CHAIRMAN. Thank you very much, Senator Casey.

Mr. Rupy, in June, a federal court issued an order imposing a \$280 million fine against DISH network, and that was the largest penalty ever issued in a do-not-call case. According to the court records, DISH network says its telemarketers made tens of millions of calls, often robocalls.

So I mention this case because I think we expect robocalls to come from the call center in India, or an international criminal cartel. We do not expect it to come from a well-known telecommunications company. What is your organization doing to identify the source of illegal robocalls, and what if it involves a member of your organization?

Mr. RUPY. Senator, thank you for that question. So in terms of identifying the source of these illegal robocalls, that is a principal focus of USTelecom's Industry Traceback Group. And as I mentioned in my opening statement, that is a broad-based coalition of companies that include traditional wire-line phone companies, cable companies, wireless providers, wholesale providers, working collaborative to trace back the origin of these illegal phone calls. That is an effort that we have been working through and conducting. We have active tracebacks underway to identify the source of these calls.

One of the ways I explain it is that what we want to do, in industry, if you think about it as a football field, the traceback process as it currently stands is a very manual process, and any given call can transit multiple networks. It can transit anywhere from four to 10, if not more, networks as it goes from its point of origin to its point of termination.

What we want to do in our industry group is basically move that traceback, like a football, down the field, so that we can get 80, 85 yards down the field until we hit a point where we are dealing with what I call an intransigent carrier, a carrier that will not provide the source of that call, where they got that call from. And at that point we want to turn that information over to federal enforcement officials so that they can identify the source of those illegal calls.

And at the end of the day, that is our focus with the Traceback Group, is to identify the source of these illegal calls, whether they are originating from domestic or international sources. I would note that the two of FCC's recent enforcement actions, one dealing with fraudulent travel schemes and the other dealing with health insurance, both of those individuals named in the case—individual cases, were domestic. One was in Florida. I believe the other was in North Carolina. So at the end of the day, we want to root these out and find the source of these illegal calls.

The CHAIRMAN. Ms. Greisman, we have noticed, on our Committee Hotline, a change in some of the kinds of complaints that we are getting. One is that there appears to be a new scam where the person says, "Are you there? Can you hear me?" Could you tell us whether you are familiar with that scam? Clearly the caller is after the word "yes," and what are they doing? I think this is one where we need more education.

Ms. GREISMAN. Yes, certainly. We are very much familiar with it, and it is a bit of a conundrum to figure out what is going on there. What we think is happening is that they are not so much

looking for the “yes,” which they might then later use as authorization for some other good or service, because we are just not seeing that. We are not seeing any unauthorized billing. What we think is going on is that this is sort of a filler. Instead of music it is—and rather than dead air, it is a filler waiting for a live telemarketer to free up and actually get on the call.

So that is our best take on it. It also, of course, is an effort to figure out, is this a number that a true person will pick up the phone, and they might be able to monetize that type of call with that kind of information.

The CHAIRMAN. Mr. Rupy, another development that our Committee’s Fraud Hotline has noticed is an increasing trend in complaints of unwanted robocalls that appear to originate from the same area code and often sometimes the same prefix, the three numbers following the area code. So it looks like a neighbor is calling you. Are you familiar with this new approach to robocalls, and could you give us your insights?

Mr. RUPY. Senator, thank you for that question, and as you noted in your statement, it looks like a neighbor is calling, and we have a name for it and it is called “neighbor spoofing.” And what is happening there is the scammers are essentially spoofing what is called the MPA NSX, which is the first three numbers, the area code, the next three numbers, the exchange. I have heard instances where they will spoof, you know, the first two numbers of the final four numbers, and, you know, change the last two digits, so it does look like a neighbor is calling down the street.

My insight on that is that, as I think everyone here would agree, the robocallers behind these calls are adaptive and they are manipulative, and I think the primary reason that they are doing neighbor spoofing is because it works. Because when individuals see a phone number that looks like it might be from somebody down the street, they are going to be more inclined to pick up that call.

The CHAIRMAN. Exactly. Ms. Barton, you obviously have done so much to help educate people about the dangers of these scams, and you make a really important point about the sophistication and the ever-changing nature of these con artists’ approach. If you are comfortable, would you share with the Committee how you almost became a victim yourself, because I think it is illustrative of the fact that even those of us who pay a lot of attention to this issue can become a victim.

Ms. BARTON. Thank you, Senator Collins. I am perfectly happy to share it. One of the things we try to do is tell people not to be embarrassed. So I will try to hide how embarrassed I am.

[Laughter.]

Ms. BARTON. And that is, I think I know a lot about phishing, but my daughter had lost her credit card, and that was the only one she had, and she was in St. Petersburg, where she was at university, and she was evacuating to Atlanta. So we urgently called and said, “Can you overnight this?” and they were very good. They said, yes, they would. But I was worried that she was not going to get it, so I texted her. Well, of course, she is 22 so she did not answer.

I then got an e-mail saying, "Did you receive your credit card?" and I thought, oh, my goodness, maybe she did not. And then I got another one, saying, "To confirm that you got your credit card, please give us the numbers." And, of course, I did not have them because it was hers. So I texted her again and said, "Urgently, I need these numbers." And as I did it, I said, "What am I thinking?" And so I almost got caught, and it was because, situationally—and I am a mother—I want my daughter to have the card. I will do anything. And, of course, that is how the grandparent scam works, that your grandson, your granddaughter, they are in jail in Mexico, and that is the biggest scam that seniors fall for. And when we care the most, sometimes we think the least.

The CHAIRMAN. That is a very good way to put it, and how extraordinary that you got that at the exact time that you were seeking to get a new credit card for your daughter. I hope it will make you feel better that I almost became a victim of essentially the grandparent—but I am an aunt—the scam, several years ago when I received an e-mail message that appeared to be from my nephew, saying that he was traveling overseas, that he had been robbed, that he needed money to get back. Being hard-hearted, however, I referred him to the American Embassy.

[Laughter.]

The CHAIRMAN. And then later I started thinking about it and thought, I do not think Mark is overseas. I called his father and, of course, he was not. But I do not know what my response actually says about me, that I did not fall for it because I thought he should go to the American Embassy for help, rather than reaching out to his aunt. But it does happen to everybody, and as you said, when you care about the well-being of the person you try to help. And it was so sophisticatedly done. It sounded just like my nephew. So I think that is a real problem.

I appreciate very much the work that all of you are doing on this issue. I just want to make a plea that we have got to move forward, and I hope, when this technology is developed fully and approved by the FCC, that it will be made available at no cost to consumers. That is another thing that I am worried about. If it is very expensive then consumers are not going to be able to participate in it. So that is an issue that I hope we can explore at some point.

Before I turn to Senator Casey to see if he has any closing questions or statements he wants to make, I do want to recognize that Senator Cortez Masto, who is a very active member of this Committee—in fact, I do not think she has ever missed a single hearing—is home in Nevada because of the horrible acts of violence in Las Vegas. Otherwise, I am confident that she would be here today, because I know, given her background, that she has worked very hard to protect seniors from scams as well.

Senator Casey, do you have any further questions or comments you would like to make?

Senator CASEY. Just briefly. Thank you for the hearing and I want to thank the panel for your testimony. We have a long way to go to get this right, but we heard a good bit today about new tools and technologies on the horizon that will help, and we have got to continue to work together, at all levels of government, to stamp this out. But we are grateful for your testimony, and I am

especially grateful for Attorney General Shapiro making the trip down from my home state. We are grateful that everyone had an opportunity today to provide this testimony. Thanks very much.

The CHAIRMAN. I too want to thank all of our witnesses today, as well as our staff for working hard and continuing to focus on this issue. One reason we have had so many hearings on this is to try to elevate public awareness, and the attorney general just gave me a thumbs-up on that, because I know that has been a focus of his as well.

It is frustrating that despite the creation of the National Do Not Call Registry 14 years ago, when we thought we solved this problem—which we did for a very, very brief period of time—that Americans, especially seniors, continue to be inundated with these annoying and unwanted calls that can produce very harmful results. I mean, it is not just the fact that these calls are coming and interrupting the serenity and privacy of our seniors. It is that they are scams and they seeking to part seniors and others—and I was interested in your comments, Ms. Barton, about the millennials—from their money. Moreover, advancements in robo-technology has made it so much easier and cheaper for con artists to target more potential victims and to bilk them out of their hard-earned savings.

So I am hopeful that continued education, more aggressive law enforcement—we saw what happened with the IRS scam after the call center in India was closed down, that there was a real drop for a while—and advances in technology—and I am really looking at the industry and the FCC to lead the way here—will ultimately put an end to these unwanted and harassing calls.

Committee members will have until Friday, October 13th, to submit questions for the record. Again, I want to thank each of you for your personal commitment to ending this series of scams that evolves by the day, and thank you for being here. Thank you, Senator Casey, for your work.

This hearing is now adjourned.

[Whereupon, at 10:19 a.m., the committee was adjourned.]

APPENDIX

**Prepared Witness Statements and Questions
for the Record**

**Prepared Statement of
Lois Greisman, Associate Director, Division of Marketing Practices,
Federal Trade Commission, Washington, DC**

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

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

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-ORL-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 robocalls¹⁶—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 than 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/allore-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/alloreys-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-ORL-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/alloreys-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-ORL-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-ORL-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/alloreyc-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/160614robocall-enforcement-actions.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 Challenge⁴⁸, 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 Rachel⁵⁰—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, DetectaRobo⁵¹, 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 (“M³AAWG”). M³AAWG 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, M³AAWG leadership formed the Voice and Telephony Abuse Special Interest Group (“VTA SIG”) in 2014, a subgroup formed to apply M³AAWG’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 M³AAWG, Activities, <https://www.m3aawg.org/> (last visited Sept. 22, 2017).

⁶¹ See M³AAWG, 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.

**Questions for the Record
To Lois Greisman**

From Ranking Member Bob Casey

Introduction: There are a number of initiatives going on to help reduce robocalls. There is the Strike Force, FCC rules, FTC actions, education campaigns and other things. However, the number of robocalls seems to still be at an all-time high.

Question: What action do you believe would be most helpful to reducing the number of unwanted robocalls?

Answer:

In my view, the most effective way to reduce the number of illegal calls reaching consumers is a multi-faceted approach that focuses on rigorous law enforcement, technological innovation, consumer education and involves multiple stakeholders, including our government partners, industry, academics, and consumer groups.

The FTC is actively working to stop those responsible for making illegal calls. First, we engage in a vigorous law enforcement campaign against violators. When the FTC is able to locate and identify companies responsible for placing illegal telemarketing calls, the FTC takes aggressive action to hold those companies accountable. To date, the FTC has filed law enforcement actions against more than 770 companies and individuals alleged to have been responsible for placing billions of unwanted telemarketing calls to consumers. The FTC has obtained more than \$1.5 billion in judgments against these violators and has collected over \$121 million dollars.¹ In cases where perpetrators were running telemarketing scams, the FTC obtained court orders shutting these businesses down and freezing their assets so that those funds could ultimately be returned to consumer victims. The FTC will continue its ongoing efforts to identify and take strong law enforcement action against those who place illegal telemarketing calls.

Technological solutions, particularly call-blocking and call-filtering solutions for consumers, are also a critical part of the effort to stop unwanted robocalls. Such efforts have been underway for some time and continue to gain momentum. To spur the development of effective call-

¹ One example of a recent successful enforcement action is the historic win the FTC and its law enforcement partners achieved in a long-running litigation against Dish Network. 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. 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>. The litigation centered on allegations that Dish and its telemarketers made tens of millions of calls—often robocalls—to telephone numbers on the Do Not Call Registry and called consumers who previously asked Dish and its telemarketers to stop calling. Additional information is available on the FTC’s [Do Not Call Enforcement page](#) about our recent enforcement efforts targeting defendants who violate the [Do Not Call](#) rules and the [robocall](#) prohibitions.

blocking and call-filtering solutions to help consumers ward off illegal and unwanted calls, in 2012, the FTC announced a robocall challenge in which it called upon innovators to develop a consumer-facing solution that blocks illegal robocalls, applies to landlines and mobile phones, and operates on proprietary and non-proprietary platforms.² One of the winners, “NomoRobo,” was on the market six months later and today reports blocking over 300 million calls.³ The FTC hosted three additional, successful challenges to spur industry initiatives to develop solutions to help both consumers and law enforcement combat illegal and unwanted robocalls.⁴

In addition, last year, the industry-led Robocall Strikeforce continued the push to develop call-blocking and call-filtering solutions.⁵ Now, a number of major voice service providers offer these products to some or all of their customers.⁶ In addition, a growing number of free or low-cost apps that offer call-blocking and call-filtering solutions are available for download on wireless devices.⁷

² 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>.

³ See <http://www.nomorobo.com/> (last visited Nov. 15, 2017).

⁴ For more information on the FTC’s subsequent challenges see <https://www.ftc.gov/news-events/contests/zapping-rachel> (Zapping Rachel challenge); <https://www.ftc.gov/news-events/contests/detectarobo> (Detectarobo challenge); and <https://www.ftc.gov/news-events/contests/robocalls-humanity-strikes-back> (Robocalls: Humanity Strikes Back challenge).

⁵ The Robocall Strike Force organized in response to a request from the FCC to carriers 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>.

⁶ For example, in late 2016 AT&T launched “Call Protect”, 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 Nov. 15, 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 Nov. 15, 2017).

⁷ 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 Nov. 15, 2017).

Most recently, the FTC 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.⁸ Beginning in August of this year, the FTC began releasing the phone numbers reported by consumers in their Do Not Call and robocall complaints each business day. The FTC also began 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 whether the call was a robocall.⁹ By making our available data more up-to-date and 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.

To maximize their effectiveness, call-blocking and call-filtering solutions will need to be supported by long-term technological solutions such as the STIR/SHAKEN framework for Caller ID authentication.¹⁰ And, of course, call-blocking and call-filtering solutions should be made available to all consumers and consumers should be made aware of the available options. While technological solutions are no substitute for vigorous law enforcement, which the FTC continues to pursue, such solutions are a necessary complement.

In addition to law enforcement and technological innovation, consumer 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

⁸ 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>.

⁹ 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.

¹⁰ The STIR/SHAKEN standards will serve as the basis for verifying calls, classifying calls, and facilitating the restoration of trusted caller ID information. More information about STIR (Secure Telephony Identity Revisited) is available at <https://datatracker.ietf.org/wg/stir/about/> (last visited Nov. 16, 2017). More information about SHAKEN (Signature-based Handling of Asserted information using toKENs) is available at <https://www.sipforum.org/activities/technical-wg-overview-and-charter/atissip-forum-nni-task-force-charter/> (last visited Nov. 16, 2017).

phone number on the Do Not Call Registry, how and where to report illegal robocalls,¹¹ available call blocking solutions,¹² and how to identify common scams.¹³

I believe that this combination of law enforcement, technological innovation, and consumer education, in collaboration with our public and private partners, is the best approach to reduce the number of illegal calls reaching consumers.

From Senator Elizabeth Warren

In December of 2015, Congress directed the IRS to contract with private debt collectors to collect certain categories of uncollected tax receivables.¹⁴ The IRS hired four debt collection companies – CBE, ConServe, Performant, and Pioneer¹⁵ – and they have now begun to contact Americans to collect unpaid taxes. The companies are compensated based on the amount they recover.

This arrangement raises two primary concerns as it relates to seniors. First, these debt collectors are authorized to attempt to collect tax debts on the phone.¹⁶ For years, phone scammers have been trying to steal money from seniors by impersonating IRS agents. In fact, the Treasury Inspector General for Tax Administration (TIGTA) has received nearly 2.1 million complaints of calls impersonating the IRS¹⁷ and IRS impersonation is the scam

¹¹ See, e.g., National Do Not Call Registry, <http://www.consumer.ftc.gov/articles/0108-national-do-not-call-registry>.

¹² See, e.g., FTC Consumer Information Blocking Unwanted Calls <https://www.consumer.ftc.gov/articles/0548-blocking-unwanted-calls>.

¹³ See, e.g., FTC Consumer Information Scam Alerts, <https://www.consumer.ftc.gov/scam-alerts>.

¹⁴ Fixing America's Surface Transportation (FAST) Act, Pub. L. No. 114-94 §32102.

¹⁵ "Private Debt Collection," IRS, last reviewed October 4, 2017. Available at: <https://www.irs.gov/businesses/smallbusinesses-self-employed/private-debt-collection>.

¹⁶ Tax Scam / Consumer Alerts, IRS, last reviewed October 3, 2017. Available at: <https://www.irs.gov/newsroom/tax-scams-consumer-alerts>.

¹⁷ "Testimony of the Honorable J. Russell George," Subcommittee on Financial Services and General Government, Committee on Appropriation, United States House of Representatives, last reviewed October 4, 2017. Available at: <http://docs.house.gov/meetings/AP/AP23/20170523/105897/HHRG-115-AP23-Wstate-GeorgeJ-20170523.pdf>.

most-often reported to the Senate Committee on Aging's hotline.¹⁸ In 2015 alone, IRS scams cost Americans over \$15 million. In the past, educational efforts to protect seniors from this scam have focused on one simple message: the IRS would never attempt to collect a debt by phone.¹⁹

Question: Now that debt collectors working on behalf of the IRS will contact taxpayers by phone, what guidance is the FTC giving seniors to help them differentiate between scams and legitimate attempts to collect taxes?

Answer:

In April of 2017, the FTC changed the guidance²⁰ it gives to consumers regarding how to recognize an IRS scam call and informed consumers that debt collectors working on behalf of the IRS may contact them by phone. The FTC advises consumers that if their tax debt is assigned to a private debt collection company, they will receive two letters. The first letter will come from the IRS and will identify the private debt collection company to which the account has been assigned, and the second letter will come from the debt collection company assigned to the account. The FTC guidance emphasizes that both letters will include the tax amount owed, the name of the private debt collection company assigned, and a unique taxpayer authentication number.

The FTC's updated guidance also gives tips to consumers regarding how they can tell if they are dealing with a legitimate debt collector or a scammer.²¹ The most important difference that we emphasize is that the private debt collectors working with the IRS will never ask consumers to pay them directly, but will instead direct consumers to pay electronically at [IRS.gov/payments](https://irs.gov/payments), or to send a check, made out to the US Treasury, directly to the IRS. We highlight that anyone who claims to be collecting for the IRS and asks you to make a payment over the phone is a scammer and we instruct consumers never to pay by credit or debit card, electronic check, wire, or a prepaid or gift card. We also let consumers know that the debt collectors will never use robocalls or pre-recorded messages and they will always use the authentication number identified in the hard copy letters sent to the consumer.

¹⁸ "Fighting Fraud: Senate Aging Committee Identifies Top 10 Scams Targeting Our Nation's Seniors," United States Senate Special Committee on Aging, last reviewed on October 4, 2017. Available at: <https://www.collins.senate.gov/sites/default/files/Fraud%20Book%202017.pdf>.

¹⁹ "The IRS is Now using Private Debt Collectors; Here's What You Need to Know," Consumerist, last reviewed on October 4, 2017. Available at: <https://consumerist.com/2017/04/03/the-irs-is-now-using-private-debt-collectors-heres-what-you-need-to-know/>.

²⁰ See "The IRS is Now Using Private Debt Collectors" available at <https://www.consumer.ftc.gov/blog/2017/04/irs-now-using-private-debt-collectors>.

²¹ See *id.* In addition, the FTC has published comprehensive guidance to help consumers recognize government impostor scams: <https://www.consumer.ftc.gov/articles/0048-government-imposter-scams>.

Question: What measures is the FTC taking to correct seniors' now-mistaken impression that IRS will not attempt to collect tax debt over the phone?

Answer:

The FTC published a consumer advisory in April of 2017²² to communicate the information summarized above. Over 240,000 consumers and groups automatically receive copies of our consumer blog posts, including the IRS private debt collector guidance, and they are available in English and Spanish. The FTC also updated its imposter scam materials to reflect this change in IRS practice.

In addition to changing our online and printed guidance, the FTC has highlighted the change in IRS practice throughout our many outreach initiatives. For example, we talk about these changes during presentations on identity theft and imposter scams, including at the National Aging and the Law Conference, National Area Agencies on Aging (n4a) Conference, Home and Community Based Services (HSCBS) Conference, and webinars with the Identity Theft Resource Center (ITRC). The FTC also highlighted these changes during the FTC's Tax Identity Theft Awareness Week 2017 and we plan to do the same during Tax Identity Theft Awareness Week 2018. The FTC also hosts monthly consumer education calls with our federal, state, and private partners who engage in consumer outreach, and specifically highlighted the IRS changes and our revised guidance to consumers in our March 2017 call. Finally, the FTC has begun offering state-specific webinars on fighting fraud and identity theft, and includes information about the IRS changes in each webinar.

Question: Has the FTC seen any increase in the number of IRS impersonation scams? Has the FTC taken any additional steps to more closely monitor IRS scams given the IRS's new policy?

Answer:

I understand that the IRS began contacting consumers using four private debt collection companies in or around April of this year. The FTC's Division of Consumer Response and Operations reviewed government-imposter fraud complaints in our Consumer Sentinel database in which the primary or associated subject name entered was "IRS" from November 2016 through October 2017. While there was a short spike in this type of complaint from May to June, the complaint numbers have decreased every month since June, so it does not appear that the use of private debt collectors is causing a sustained increase in IRS imposter scams at this time.

In addition to monitoring consumer complaints, we are in regular contact with staff from IRS and TIGTA to discuss trends and monitor developments relating to IRS scams.

²² See "The IRS is Now Using Private Debt Collectors" at <https://www.consumer.ftc.gov/blog/2017/04/irs-now-using-private-debt-collectors>

Question: If there has been an increase in these scams, does the FTC have adequate funding to address this increase? If not, will you bring your additional funding needs to the attention of the committee?

Answer:

We appreciate the Committee's willingness to hear about any additional funding needs the Commission may have in this area, and will reach out should the need arise and appreciate your support for our mission.

Senator Warren: I am also concerned that the use of debt collection companies that are compensated based on the amount they recover increases the risk of abusive collection practices. According to a report released in December 2016, the Consumer Financial Protection Bureau has received more total complaints about debt collection practices than about any other subject.²³ In fact, the IRS has hired a debt collection company with a troubling history of misleading debtors that it contacted on behalf of the government. Pioneer, a subsidiary of Navient, was one of the several debt collectors fired by the Department of Education in 2015 for providing borrowers with "inaccurate information at unacceptably high rates."²⁴

Question: Was the FTC consulted in IRS's procurement process which resulted in hiring these debt collection companies? Does the FTC ever consult with the other agencies to ensure that they procure services from the good actors?

Answer:

The Federal Trade Commission does not perform procurement consultation for other government agencies or offices that engage in debt collection activities, and was not consulted in the IRS's private debt collector procurement process. The FTC is primarily a law enforcement agency. Our expertise is in monitoring marketplaces for significant law violations and then taking appropriate enforcement action to halt unlawful conduct. More generally, the FTC does not "pre-approve" any particular company's practices; the Commission only comments on an individual company's business operations if it has reason to believe, after an investigation has been completed, that the law has been violated and law enforcement action is warranted. Information about the Commission's public law enforcement actions is available on the FTC's website, ftc.gov. The website also includes a list of companies and people who are banned by federal court order from participating in the debt collection business. See <https://www.ftc.gov/enforcement/cases-proceedings/banned-debt-collectors>.

²³ "Monthly Complaint Report," Consumer Financial Protection Bureau, last reviewed on October 4, 2017. Available at: http://files.consumerfinance.gov/f/documents/201612_cfpb_MonthlyComplaintReport.pdf.

²⁴ "Feds Fire 5 Debt Collectors," Inside Higher Ed, last reviewed on October 4, 2017. Available at <https://www.insidehighered.com/news/2015/03/02/us-ends-contract-5-debt-collectors-citing-misrepresentations-borrowers>.

In support of our law enforcement mission, the Commission regularly educates businesses on how to comply with the laws the FTC enforces, and consumers on how to exercise their rights and identify and report illegal conduct. As the IRS was preparing to initiate its private debt collection program, the FTC recognized the need to update its consumer education in this area to provide consumers with the tools they would need to avoid IRS impersonation scams. As such, we coordinated with the IRS and TIGTA on a new consumer education piece explaining to consumers how to determine whether collection attempts were from actual IRS debt collectors and not scammers.²⁵

Any consumer complaints the Commission receives are available through the FTC-maintained Consumer Sentinel Network to numerous federal and state law enforcement partners, including a number of offices within Treasury and the IRS.

Question: Has the FTC received complaints that any of the IRS debt collectors – CBE Group, ConServe, Performant Recovery or Pioneer – have acted inappropriately or unlawfully in collecting IRS or any other debts?

Answer:

The FTC gathers complaints across the debt collection industry through the Consumer Sentinel Network—a secure online database maintained by the FTC containing millions of consumer complaints. The contents of Consumer Sentinel are non-public, and the complaints are unverified. As a baseline matter, large, consumer-facing companies tend to be the subject of a number of consumer complaints, and the FTC has received some complaints about the collectors identified above. This fact by itself does not establish that a law violation has occurred. On the other hand, where law violations are occurring, complaints may represent only a fraction of the total number of consumers affected, as many consumers do not complain even when they are harmed.

Question: What process does the FTC use to investigate consumer complaints that it received via the Consumer Sentinel database? Under what circumstances would it make these complaints public?

Answer:

The FTC routinely receives complaints from consumers regarding potentially unlawful conduct, including from consumers with debt collection-related issues. Consumer complaints help the FTC detect patterns of fraud and abuse, and may be among the reasons the FTC decides to open an investigation into potentially unlawful conduct. In determining whether a particular practice warrants FTC enforcement or other action, the Commission may consider a number of factors, including the type of violation alleged, the nature and amount of consumer injury at issue, the number of consumers affected, and the likelihood of preventing future unlawful conduct.

²⁵ See “The IRS is Now Using Private Debt Collectors” available at <https://www.consumer.ftc.gov/blog/2017/04/irs-now-using-private-debt-collectors>.

Each year, the FTC releases aggregate data about consumer complaints.²⁶ Individual complaints often contain significant amounts of personal information about the consumers who submit them, including identifying information and sensitive financial information, and the agency treats individual complaints as non-public information. Such complaints generally are available only to members of law enforcement organizations that have entered into a confidentiality and data security agreement with the FTC, but may otherwise be released—typically in redacted form to protect consumers’ personal information—in other limited circumstances, including in response to court orders, subpoenas, discovery requests, or Freedom of Information Act requests.

Question: When considering whether to bring an enforcement action for a violation of the Fair Debt Collection Practices Act, does the FTC give special consideration to companies that collect debts on behalf of the government?

Answer:

The FTC considers a number of factors when determining whether to open an investigation, and when deciding what, if any, action to take. Generally, no one or two factors are conclusive; we look at the whole picture, including the type of violation, the scope of consumer injury, the number of affected consumers, and the likelihood of deterring future unlawful conduct. One of the FTC’s key priorities of its debt collection program is halting collection-related scams that involve egregious practices like false threats of legal action, “phantom” debts that consumers do not actually owe to the collectors, or both. This is a particularly high-priority area for the FTC because of the pernicious threats, which sometimes involve government impersonation, these scammers make to consumers, including violent threats, and elaborate false threats of arrest or lawsuits. The Commission has also taken action where it has had sufficient evidence of other significant violations, including in circumstances where the violator is collecting debts on behalf of a federal agency. For example, when the FTC had reason to believe that a federal student loan debt collector had a practice of leaving voicemail messages that revealed consumer debts to third parties, the agency filed suit to stop this unlawful conduct.²⁷

Question: Given that the total number of taxpayer accounts turned over to private debt collectors will continue to grow as the IRS fully implements this program, what plans does the FTC have for continuing to monitor possible abuses by these companies as they contact a growing number of taxpayers?

Answer:

FTC attorneys and investigators regularly review complaints to look for law enforcement targets, evaluate the need for consumer education, and make policy recommendations. We will continue to monitor the marketplace for illegal conduct, including any such conduct associated with the collection of IRS tax debts by private companies, and we will continue to prioritize our debt collection enforcement work.

²⁶ The FTC’s Consumer Sentinel Network Data Book for January - December 2016 is available at <https://www.ftc.gov/reports/consumer-sentinel-network-data-book-january-december-2016>.

²⁷ See *FTC v. GC Services*, <https://www.ftc.gov/news-events/press-releases/2017/02/student-loan-debt-collector-will-pay-700000-unlawful-collection>.

The FTC has long been committed to halting unlawful debt collection practices that generate significant consumer concern and put compliant businesses at a competitive disadvantage. For example, since the beginning of 2010, the FTC has brought 48 debt collection cases and obtained more than \$425 million in judgments against a variety of debt collectors. In the past year alone, we filed or resolved 12 debt collection cases against 61 defendants, obtaining nearly \$70 million in judgments and banning 44 companies and individuals that engaged in serious and repeated violations of law from ever working in debt collection again. We remain committed to protecting consumers from deceptive, unfair, and abusive debt collection practices.

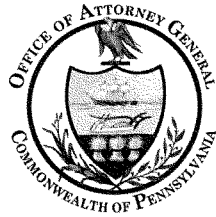
From Senator Sheldon Whitehouse

Question: Last election cycle, there were several reports of robocalls being made to voters falsely telling them their ballot would not counted unless they updated their voter registration status. How can robocalling technology be used to suppress votes? What actions can Congress take to address that threat?

Answer:

The FTC's enforcement authority over illegal robocalls is limited to telemarketing robocalls, as that term is defined in the Telemarketing Sales Rule,²⁸ and does not cover voter suppression calls. Voter suppression calls, however, may rely on similar deceptive tactics used in telemarketing scams that seek to deprive consumers of their money, rather than their vote. Congress could support extensive consumer outreach and education to assist consumers in identifying and knowing to hang up on scam calls.

²⁸ In relevant part, the Telemarketing Sales Rule defines telemarketing as "a plan, program, or campaign which is conducted to induce the purchase of goods or services or a charitable contribution, by use of one or more telephones and which involves more than one interstate telephone call." 16 C.F.R. § 310.2 (gg).



Pennsylvania Attorney General Josh Shapiro

Introduction

Chairman Collins, Ranking Member Casey, and members of the Committee, I am Josh Shapiro, Attorney General for the Commonwealth of Pennsylvania. Thank you for inviting me to speak with you today about what my office is doing to keep senior citizens safe from scam artists and financial predators and what steps the Federal government can take to further protect the elderly from financial exploitation.

The well-being of our nation's 47 million seniors is an important issue. As an elected official from Pennsylvania, it is particularly important to me. Pennsylvania has one of the highest populations of seniors over the age of 65 in the country: there are 2.2 million seniors in Pennsylvania—the fifth highest number in the U.S.—accounting for over 17 percent of our total population. And our population of seniors is only expected to grow, increasing by 25 percent by 2020.

As the chief law enforcement officer of the Commonwealth of Pennsylvania, I am responsible for protecting all Pennsylvanians in their roles as consumers. My responsibilities range from antitrust to home improvement contractors, from civil rights to managing our state's Do Not Call list. Protecting vulnerable seniors from unscrupulous scammers is one of my most important duties.

In my testimony today, I would like to cover three main topics: (1) seniors' vulnerability to scams and the impact scams have on them; (2) IRS impersonation scams; and (3) Pennsylvania's Do Not Call registry, which complements the federal system, and its effect on robocalls.

Seniors' vulnerability to scams

Senior citizens are specifically targeted for fraud and scams more than any other age group. Many of the most common scams are tailor-made for their specific life circumstances, including those involving Medicare, prescription drugs, funerals, anti-aging products, and grandparent scams. Understanding why seniors are vulnerable, and why they're being targeted, is necessary to developing solutions to better protect them.

Why seniors are more vulnerable

Seniors are now easier to reach than ever: according to a recent study from Pew Research Center, 67 percent of seniors have some form of internet access; 74 percent live in homes with computers; 51 percent access the internet through high-speed connections; and 34 percent of seniors who use the internet use social media (such as Facebook), making them even easier for scammers to locate and contact. Compounding this is seniors' comfort with conducting financial transactions online. Whereas 15 years ago, online financial transactions were relatively rare and viewed by the general public with skepticism, a recent study indicates that today 41 percent of seniors bank online, 26 percent pay their bills online, and 21 percent file their taxes online.

This is also the wealthiest generation of seniors perhaps ever. According to Nielsen, they have a median net worth of \$241,333. That's 34 percent more than the "War Babies" generation (born 1936 -1945) and 39 percent more than "Depression Babies" (born 1926-1935). In the words of the AARP, a scammer would "have to be an idiot to turn [their] back on this humongous market."

Impact

The combination of scammers' greed and seniors' vulnerability has resulted in significant financial losses for America's elderly. Over a third of seniors have experienced some form of financial abuse, including scams. Victims lose an average of \$36,000. While it is difficult to calculate, our best estimates indicate that American seniors lose over \$3 billion each year to scams and abuse. Two-thirds of seniors report having been victimized online: 38 percent have been targeted for online scams, and 28 percent have mistakenly downloaded a virus.

Discussing the impact of these scams in terms of billions of dollars or percentages of victims obscures the real impact on individuals. The loss of even a few thousand dollars can be devastating to a senior citizen. Nearly a million seniors in the United States have been forced to skip meals because they lost money to a scammer.

NAAG focus

Protecting seniors from scams and fraud is an important issue in every state, and attorneys general are making it a top priority. In August, the new president of the National Association of Attorneys General (NAAG), Kansas Attorney General Derek Schmidt, announced that NAAG will spend the next year focusing on "strengthening efforts nationwide to combat elder abuse." To quote Attorney General Schmidt, "There is no partisan divide on the commitment of state attorneys general to protecting seniors and combating elder abuse in all its forms."

OAG's efforts

The Pennsylvania Office of Attorney General (OAG) dedicates significant resources to consumer protection. Of our nearly 20,000 complaints from consumers each year, one third come from seniors in our Commonwealth. OAG receives and investigates complaints from seniors regarding:

- Purchase of goods and services (*e.g.* automobiles, pets, and insurance)
- Deceptive trade practices (*e.g.* false advertising or odometer tampering)
- Health care (*e.g.* health insurance service denials)
- Home improvement contractor scams
- Identity theft

In addition to this reactive work, OAG conducts proactive educational outreach to prevent seniors from becoming victimized in the first place. We have a dedicated Office of Public Engagement that manages this programming. Examples of some of our presentations most of interest to seniors are:

- Scams, fraud and identity theft education
- Senior Crime Prevention University, a specialized series of educational sessions for seniors to identify and avoid scams
- Cyber security for seniors

Finally, OAG manages Pennsylvania's Do Not Call list, which guards against unwanted marketing calls.

Throughout these various efforts, the most common complaints we receive from seniors are about violations of the Do Not Call list, including robocalls. The next most frequent complaints are about telecommunications and broadcast issues (including television and internet service providers), home improvement contractor issues, and scams like IRS impersonation.

IRS impersonation scams

IRS impersonation scammers call people and falsely claim to represent the Internal Revenue Service. The callers will claim that back taxes are owed by the recipient, threaten to have them arrested, and demand payment (usually via wire transfer). Last year, my office received 881 complaints about IRS impersonation scams, 62 percent of which were from seniors.

Fortunately, most Pennsylvanians are able to recognize these calls as fraudulent. In the past, it helped to know that the IRS did not call people about their taxes, and that they only sent letters; however, as of April, Congress authorized the IRS to begin contracting out some of its debt collection work to private debt collectors who do make phone calls, which takes this defensive knowledge away. While there are some safety measures in place, like a passcode sent by mail that the caller must provide to a senior, I fear that ending the simple rule that the IRS will not call opens the door to more successful scams by sophisticated con artists.

John's story

In May of this year, agents in my office received a complaint from a man from the Pittsburgh area. I will call him "John" to protect his identity, as this investigation is ongoing. John received a call from a 1-866 number who claimed to be an IRS employee. The caller said that an arrest warrant had been issued for John because he sends money to his wife and child in a foreign country. The purported IRS employee said that John would soon receive a call from the local

police department and instructed him on how to merge the calls. Shortly thereafter, John received a call from a number that his caller ID showed as coming from Pennsylvania State Police Headquarters.

The callers threatened John and said that his only way out of the situation was to send money to help pay for the investigation to clear his name. The money, they said, would be refunded to John after the investigation was complete.

John believed them, since they appeared to be calling from legitimate phone numbers. He was instructed to send six different payments from four different locations—Walmart, CVS, Western Union, and Rite Aid—over two days. In total, he lost \$13,500 because he truly believed he was speaking with tax authorities and wanted to clear his name. John’s story demonstrates just how manipulative and devastating IRS impersonation scams can be.

OAG's efforts – grassroots education

Unfortunately, cases like John’s can be difficult to prosecute. Anonymous criminals hiding behind spoofed phone numbers using shady financial transactions leave little for law enforcement to work with. That’s why one of the best approaches to battling scams like this is preventative education.

My office takes a grassroots approach to educating seniors on how to identify and avoid scams like the IRS impersonation scam. Each year, we hold around 250 events all across Pennsylvania, reaching 14,000 seniors. Additionally, we hold 50 events on identify theft for people of all ages that reach approximately 5,000 additional seniors. These presentations teach seniors about a wide variety of scams and how to recognize and avoid them. We have also begun to incorporate materials on how to be safe while using the internet, as more and more seniors go online each year.

Many seniors are aware of the most well-known scams. As a result, these scams have very low success rates. This Committee estimated that last year one million Americans were targeted with the IRS impersonation scam, yet only 5,000 were victimized—a 0.5 percent success rate. However, many scams are not well-known, and new scams are popping up on a regular basis. So during our info sessions, we focus on communicating two crucial strategies for avoiding scams.

The first is an easy way to remember how to recognize a scam. Our agents have developed a mnemonic around the word “scam” itself: Sudden Contact, Act now, Money or information required. We tell seniors that if they are suddenly contacted by someone that they weren’t expecting, and that person is demanding that they act immediately by sending money or information, then it is likely a scam.

The second is a simple, yet effective technique. If you don’t recognize a phone number that’s calling you, let it go to voicemail or your answering machine. Especially for seniors with diminished mental faculties, taking the time to listen to a message a couple of times, think about it, and even ask someone else for their advice can be the difference between avoiding a scam and losing thousands of dollars to a criminal.

Pennsylvania's Do Not Call list and robocalls

Under Pennsylvania's Telemarketer Registration Act, my office administers a free Do Not Call list service for both landlines and mobile phones. Pennsylvanians can sign up by completing a simple form on our website. We collect those numbers into a list that businesses must reference before placing solicitation calls.

There are currently 3.5 million Pennsylvanians registered on the Do Not Call list out of a population of 12.5 million, nearly 30 percent. The list contains 2.8 million phone numbers. The number of registered numbers is lower than registered individuals because multiple people from the same household can register the same phone number.

Despite the wide use of Pennsylvania's Do Not Call list, we receive thousands of complaints each year alleging unlawful telemarketing, robocalls, and scam calls. Last year, we received over 7,000 complaints, nearly 4,000 of which were from seniors. Many seniors that we talk to feel that the Do Not Call list is ineffective because they still receive unwanted marketing calls.

The Do Not Call list is not a panacea. While nearly every business complies with its restrictions, there continue to be a handful of bad actors who ignore it. There are also some major exceptions to the restrictions: political campaigns and nonprofits are not subject to the Do Not Call list, and any business that has had a business relationship with an individual in the last 12 months may disregard their placement on the Do Not Call list. Scammers also ignore the Do Not Call list; after all, it's often the least of the many crimes they're committing.

Still, the fact is that the Do Not Call list drastically reduces the number of unwanted calls that seniors receive and makes it easier for them to ignore calls from unknown numbers.

Again, our office recommends that seniors let any unknown number go to voicemail. This strategy lets them assess the validity of the call. Answering a call also lets the company calling know that the number is still active, and they'll keep it on their list to call again. Devices that screen calls automatically are also helpful in reducing seniors' vulnerability to scams.

OAG's efforts

In 2016, my office received 4,473 consumer complaints specifically relating to the Do Not Call list. Since then, my office has issued 2,141 subpoenas to phone carriers to try to locate calling parties. However, this resulted in only four legal actions, highlighting how difficult it is to pursue these cases. When we are able to build a complaint, though, we can build strong cases and obtain meaningful relief for those affected.

For example, last year my office took action against a man from Oregon named Richard Paul, alleging violations of Pennsylvania's Unfair Trade Practices and Consumer Protection Law and Pennsylvania's Telemarketer Registration Act. Our office alleged that Mr. Paul obtained telephone numbers for the purposes of conducting marketing calls. Many of the people he called were on Pennsylvania's Do Not Call list; our office received several complaints about his conduct as a result, including from seniors. This case is still pending; we are currently seeking

remittances of \$100 per affected consumer and civil penalties of \$1,000 per violation or \$3,000 per violation against a senior.

Steps the Federal Government can take to protect seniors

Prevent IRS private debt collectors from calling

As mentioned earlier, we used to be able to tell seniors that if someone was calling claiming to be from the IRS, then it was a scam—period—because the IRS does not call anyone. However, with the IRS’s new private debt collection practices that began in April, it is possible for people to receive legitimate calls seeking to collect on debts to the IRS. This is causing confusion in our communities, and has removed a crucial method of self-defense.

Congress should look closely at the effects of permitting debt collectors working on behalf of the IRS to make telephone calls to people from whom they are collecting debt. The IRS has used other means for decades and never felt the need to turn to phone calls. I believe their debt collectors should adhere to the same practices.

Give telephone companies the tools to block scammers

According to the *Consumer Sentinel Network Data Book for January-December 2015*, 75 percent of consumers who filed fraud-related complaints and reported how the fraud was perpetrated indicated they were contacted by telephone. This is more than nine times the number reporting fraud initiated by e-mail (eight percent) and more than 12 times the number of those reporting fraud triggered by the internet (six percent). This statistic reveals that the telephone remains a potent instrument for criminals who are intent upon defrauding consumers.

I appreciate and applaud the efforts of the telecom industry to try to stop scammers in their tracks. I recognize the difficult balance that they must achieve between maintaining free and open lines of communication for all Americans and closing off avenues for harassment and scams. As is the nature of nearly every criminal activity, it is a constant battle to keep up with new methods and new technologies used by bad actors to circumvent the systems in place to protect us.

That’s why the federal government needs to give telephone service providers the ability to block several kinds of “spoofed” calls (in which scammers mimic the phone numbers of legitimate businesses on the receiving party’s caller ID). In July, I joined a bipartisan coalition of 29 attorneys general from across the country to submit a formal comment to the Federal Communications Commission asking them to allow telephone companies to block certain robocalls and spoofed calls.

As we said in our FCC comment, telephone companies should be able to block calls originating from “spoofed” or invalid numbers, unallocated numbers, and numbers whose owners have requested be blocked. For example, phone providers would be able to block a scammer that is using a telephone number that clearly can’t exist because it hasn’t been assigned. Legitimate

businesses do not need to use any of these spoofing methods to contact consumers. Allowing providers to block these calls would stymie scammers without burdening businesses.

I know Senator Casey shares my views on this issue. He and I are sending a joint letter to the FCC today to implement their proposed rule without further delay. It has been nearly eight months since the FCC first proposed the rule. During that time, it is likely that 19 billion calls have been placed using robocalling technology. We need the FCC to help us put a stop to these harassing and predatory calls.

Conclusion

Thank you Chairman Collins, Ranking Member Casey and all the members of this committee for holding this hearing and highlighting the issue of scams and fraud against our seniors. This is a top priority for my office and I appreciate your focus on it here in Washington. I look forward to answering any questions you may have.

Questions for the Record to Josh Shapiro From Ranking Member Bob Casey

Introduction: There are a number of initiatives going on to help reduce robocalls. There is the Strike Force, FCC rules, FTC actions, education campaigns and other things. However, the number of robocalls seems to still be at an all-time high.

- **Question:** What action do you believe would be most helpful to reducing the number of unwanted robocalls?
- **Response:** I applaud the FCC's recent decision to finalize new rules to protect Americans from illegal robocalls, for which Senator Casey and I advocated shortly after this hearing. These new rules, which allow telecommunications carriers to block certain phone numbers that do not or cannot make outgoing calls, will help prevent scammers and con artists from reaching our loved ones in an effort to steal their hard-earned money.

Finalizing this rule was my main recommendation at the October hearing. With this rule now in place, Congress and the FCC should closely monitor its effects in the coming months to determine what impact it has on the number of robocalls received and the number of scams perpetrated using illegal robocalls.

From Senator Sheldon Whitehouse

- **Question 1:** During the hearing, you said, "The spoofing technology is so difficult to penetrate, it's so difficult for us to get to the bottom of that it becomes difficult to trace it back to the scammers and ultimately prosecute them." What actions can Congress take to make it easier for telephone service providers and law enforcement to penetrate and trace spoofing calls?
- **Response 1:** Much in the way prescription drug distributors are responsible for monitoring suspicious distribution patterns, telecommunications carriers should be more responsible for monitoring aggregations of inbound traffic from international destinations to help identify possible illegal activity, which can then be referred to law enforcement.

If Congress creates meaningful incentives for carriers to conduct this monitoring, then carriers will in turn develop market-based strategies to encourage legitimate foreign call centers to route their calls through trusted telecommunications partners. This will make it easier to identify and track illegitimate call center operations.

- **Question 2:** Last election cycle, there were several reports of robocalls being made to voters falsely telling them their ballot would not counted unless they updated their voter registration status. How can robocalling technology be used to suppress votes? What actions can Congress take to address that threat?
- **Response 2:** Any type of misinformation that can be spread in print, online, or in person can also be spread over the telephone. For example, the Senate's Judiciary Committee, in reviewing Russian attempts to influence the 2016 presidential election, brought to light a Facebook ad depicting actor and comedian Aziz Ansari holding a sign encouraging people to vote from home via Twitter – which of course is and was impossible.¹ Similar deceptive messages can be spread quickly and cheaply via robocalls, particularly to senior citizens. Deceptive messages in the past have included (but certainly have not been limited to) false notifications about: polling place location changes,² election dates,³ ballot contents,⁴ endorsements,⁵ and requirements to vote.⁶

One massive challenge for Facebook, Twitter, and other online platforms to address the spread of false information is the virtually infinite number of accounts that can be created to spread misinformation. Telecommunication carriers, on the other hand, know the full universe of telephone numbers from which calls can originate, and have more direct means to verify the authenticity of calls from those numbers. This is why the FCC's recent decision to grant telecommunications carriers greater ability to block spoofed calls is so important. I believe this will greatly reduce the ability of scammers to compromise the integrity of our elections, and will make it easier for law enforcement to locate those who attempt to do so.

Again, I recommend that Congress and the FCC closely monitor the effects of this new rule with respect to election fraud. While it is certainly possible that further action may be required, I cannot say what that action might be until the new rule's effects have been studied.

¹ David S. Cloud, *Facebook tells Congress that 126 million Americans may have seen Russia-linked ads*, L.A. TIMES, Oct. 31, 2017 (available at <http://www.latimes.com/nation/la-na-russia-tech-20171031-story.html>).

² Nahal Amouzadeh, *Calls, texts give false information to some Virginia voters*, WTOP, Nov. 7, 2017 (available at <https://wtop.com/virginia/2017/11/naacp-robo-calls-give-prince-william-co-voters-false-polling-locations/>).

³ Julian Walker, *Phony flier says Virginians vote on different days*, THE VIRGINIAN-PILOT, Oct. 28, 2008 (available at https://pilotonline.com/news/phony-flier-says-virginians-vote-on-different-days/article_a2520c8e-3ccf-5f4b-9816-c34a85adfl4d.html).

⁴ Michael Wooten, *False election info in message that's gone viral*, WGRZ, Nov. 1, 2017 (available at <http://www.wgrz.com/news/local/verify/false-election-info-in-message-thats-gone-viral/464631788>).

⁵ Katie Rogers and Jonah Engel Bromwich, *The Hoaxes, Fake News and Misinformation We Saw on Election Day*, N.Y. TIMES, Nov. 8, 2016 (available at <https://www.nytimes.com/2016/11/09/us/politics/debunk-fake-news-election-day.html>).

⁶ Steve Collins, *Bates College president: Fliers left on campus aimed to suppress student voting*, BANGOR DAILY NEWS, Nov. 7, 2016 (available at <https://bangordailynews.com/2016/11/07/politics/fake-fliers-passed-out-at-bates-college-in-apparent-voter-suppression-effort-2/>).

**Prepared Statement of Kevin Rupy, Vice President,
Law and Policy, USTelecom, Washington, DC**

Chairman Collins, Ranking Member Casey, Members of the Committee, thank you for giving me the opportunity to appear before you today.

My name is Kevin Rupy, and I serve as Vice President of Law and Policy at USTelecom. Over the last several years, USTelecom and our member companies have been tremendously focused on the robocall issue, and we share the Committee's concern about the problems associated with phone-based impostor scams targeted at seniors. Calls using Voice-over-Internet-Protocol (VoIP) technology when combined with Caller ID spoofing can be used by scammers to mask their identity and location, giving their target a false sense of confidence about who is calling.

In this ongoing battle against criminal robocallers, there have been three important developments over the last year that are particularly significant.

First, the industry-led, ecosystem-wide Robocall Strike Force issued its report to the Federal Communications Commission on October 26, 2016. Comprehensive follow-up reports by the industry groups continuing the work started by the Strike Force were delivered to the FCC on April 28, 2017. These reports, taken together, catalogue industry's substantial 8 month effort to advance the battle against illegal robocalls. These reports hold a significant amount of good news for consumers, including seniors. For example, the reports note that the SHAKEN/STIR standards development for the next generation of robocall mitigation tools that the industry had initiated prior to the Robocall Strike Force, have been accelerated by 6 months. These standards, which incorporate caller-ID authentication capabilities into the network and consumer devices, have entered the industry testing phase. Some of the initial testing of the SHAKEN standard is expected to complete later this year, with additional potential deployments anticipated as early as 2018. The reports also highlight the increasing number of tools that are being developed and actively deployed to consumers, by a growing number of national voice and device providers. Finally, the reports detail the efforts of USTelecom's Industry Traceback Group, which is comprised of a broad range of network providers from the cable, wireline, wireless and wholesale industries, who are working collaboratively in order to identify the origin of these calls at their source. Industry's strong commitment to this effort can be seen its significant growth over the last year, from just 3 carriers in July, 2016, to 22 providers as of today. The ultimate goal of this group is to identify the source of the worst of these illegal calls, and further enable enforcement actions by Federal agencies. In this regard, we applaud the FCC's three recent enforcement actions since June of this year that have resulted in more than \$200 million in proposed fines targeting perpetrators of illegal robocalling, as well as complementary enforcement actions by the FTC.

Second, the reports shows that USTelecom member companies, independent application developers and a growing number of diverse companies offer services today that can help older Americans reduce unknown and potentially fraudulent calls. For example, AT&T has launched its 'Call Protect' service that allows customers with iPhones and HD Voice enabled Android handsets to automatically block suspected fraudulent calls. Verizon has been trialing a service that warns its wireline customers about calls identified as suspicious, and on the wireless side has deployed robocall mitigation features as part of its Caller Name ID service. And various carriers have worked with NoMorobo to facilitate their customers' ability to use that third-party blocking service, such as Verizon's "one click" solution that simplifies customers' ability to sign up for the service.

Third, the FCC recently published a Notice of Proposed Rulemaking in which it proposes to clarify rules for when voice providers may block certain types of calls. USTelecom supports the proposed rules and has participated fully in the proceeding. One issue the FCC raises is what protections legitimate callers should have if their calls are blocked due to the inappropriate scoring of their call. That is an important topic both for situations where voice providers block numbers directly, and for blocking services that consumers may opt into in order to block or filter potentially unwanted calls. It is an issue USTelecom and its members, and other parts of the robocall labeling/scoring ecosystem, have been wrestling with for years, and this fall we are hosting a workshop aimed at helping develop "best practices" for the scoring and labelling of calls.

All these recent developments further demonstrate the essential commitment from a broad range of stakeholders that will be necessary to effectively mitigate and defeat these scammers. Indispensable industry stakeholders from a wide range of companies—including cable, wireline, wireless, and wholesale providers, as well as standards organizations, equipment manufacturers and apps developers—have advanced a concerted, broad-based, effort focused on developing practices, technologies

and methods for mitigating phone-based attacks and scams. This coalition has also expanded its cooperation with equally important stakeholders within the Federal Government and with consumer groups. While our partners in government play a crucial enforcement role, our partners in consumer organizations are vital to raising awareness about the tools available to consumer to help mitigate illegal robocalls.

Industry efforts to address the illegal robocall issue remain ongoing and extremely energized. Importantly, these efforts are being undertaken by the necessary broad range of industry stakeholders, including representatives from the wireline, wireless, wholesale, cable and app developer community, as well as critically important standards organizations. The results of these comprehensive industry efforts are detailed in the industry-led Strike Force report submitted to the Federal Communications Commission in April of this year. The collaborative efforts outlined in the report are highly detailed, extremely comprehensive and warrant more than a brief summary. In order for the Committee to gain a better and complete understanding of these efforts, USTelecom is submitting the April Strike Force Report as an addendum to this written testimony.

In closing, let me again thank the Committee for holding this timely hearing. We share the Committee's concerns, and we look forward to our continued work together to address this constantly evolving challenge.

Questions for the Record To Kevin Rupy

From Ranking Member Bob Casey

Call Authentication

Telecommunications providers have created a plan that will allow for calls to be authenticated before it reaches the recipient.

Question:

Are companies using this technology now and how will this help in the fight against robocalls and spoofing? And, when should we expect this technology to be activated on all of our phone lines?

USTelecom Response:

A broad range of industry stakeholders continue to move forward with a framework for managing the deployment of secure telephone identity technologies with the purpose of providing end-to-end cryptographic authentication and verification of the telephone identity and other information in an IP-based service provider voice network. This framework is comprised of two separate standards and best-practice implementations: (1) Signature-based Handling of Asserted Information Using toKENs (SHAKEN); and (2) Secure Telephone Identity Revisited (STIR). Adoption and deployment of these standards and best practices can provide a much stronger assurance of identity than the legacy telephone network provides today. This framework will become most effective upon a full transition to IP-based communications networks, a process that is well underway.

USTelecom and its member companies support industry-led efforts to collaboratively develop and voluntarily deploy the SHAKEN and STIR standards and best-practice implementations. USTelecom has long maintained that the ability of scammers to easily spoof caller-ID information is a key component of the illegal robocall scourge. For that reason, the association's member companies continue their work with both the Alliance for Telecommunications Industry Solutions (ATIS) in partnership with the SIP Forum and the Internet Engineering Task Force (IETF) to develop the SHAKEN and STIR standards and best-practice implementations for secure call authentication.

As a result of the industry-led robocall Strike Force, the SHAKEN/STIR standards development for the next generation of robocall mitigation tools were accelerated by 6 months. These standards have entered the industry testing phase. Some of the initial testing of the SHAKEN standard is expected to complete later this year, with additional potential deployments anticipated as early as 2018. In addition to helping to improve the reliability of the nation's communications system by better identifying legitimate traffic, SHAKEN and STIR may also facilitate the ability of a variety of stakeholders to identify illegal robocalls and the sources of untrustworthy communications.

However, it should be noted that while advances have been made in the development of the SHAKEN and STIR standards and best practices, efforts are ongoing on a variety of key issues. For example, the Federal Communications Commission

(Commission) remains in the early stages of an ongoing proceeding addressing efforts by ATIS and SIP Forum to implement the “Governance Model and Certificate Management for the Trust Anchor” (the “Governance Framework”). The Governance Framework describes the way in which entities will be granted the trust necessary to vouch for call authenticity, and the organizational structures needed to manage this process. In addition, ATIS and the SIP Forum are also in the process of advancing the “Call Validation Display Framework” that will develop standards for how to display SHAKEN/STIR information to consumers. Both of these important initiatives remain ongoing, with significant industry involvement.

In addition to helping to improve the reliability of the nation’s communications system by better identifying legitimate traffic, SHAKEN and STIR may also facilitate the ability of a variety of stakeholders to identify illegal robocalls and the sources of untrustworthy communications. USTelecom believes that SHAKEN/STIR adoption will likely be an evolutionary process, similar to the deployment of other industry standards. These initiatives included ATIS’s International Mobile Subscriber Identity Oversight Council that led to international roaming capabilities, as well as the Mobile Device Theft Prevention working group, which ultimately evolved into an industry-led and widely adopted voluntary commitment to improve handset security and deter smartphone theft.

USTelecom has also long maintained that a broad-based, multifaceted holistic approach will be necessary to effectively address the robocall scourge. In addition to the development of the SHAKEN and STIR standards and best-practice implementations, a broad range of stakeholders are also moving across a variety of other fronts to fight the robocall problem, including the deployment of various consumer tools, effectuating robust traceback efforts and consumer education, to name just a few. The rapid and ever-changing nature of the robocall problem, however, makes the potential for a single “silver bullet” solution highly problematic and strongly inadvisable.

An open communications network is inherently vulnerable to abuse, and the interdependent, interconnected and global nature of the internet means that areas of vulnerability exist throughout the network, and therefore cannot be realistically addressed by any single stakeholder or mitigation technique. Given the rapid and ever-changing nature of the robocall problem, multifaceted holistic approaches are necessary—and indeed, beneficial—in order to mitigate the harms resulting from such illegal calls.

Ranking Member Bob Casey

FTC Fight Against Robocalls

The FTC recently announced that it is now sharing consumer complaints about robocalls with industry on a daily basis so that telecommunications providers can quickly adapt to new techniques and scams.

Question:

What are some examples of how industry is using this information? Now that you are getting better and more up to date information, what can we expect from you in the fight in these unwanted robocalls in the next year? Earlier I mentioned the call my wife received, what can I tell my wife that you’re doing about this?

USTelecom Response:

The decision by the Federal Trade Commission (FTC) to release its complaint data on a timelier daily basis is another example of how a variety of stakeholders engaged in the fight against robocalls are working collaboratively. As a key stakeholder in the battle against robocalls, the FTC’s decision to release such data reflects its commitment and support of industry stakeholders who are also working to mitigate robocalls. There are a broad range of stakeholders currently engaged in mitigating the impact of robocalls, to include voice providers, equipment manufacturers, government entities, scoring/analytics companies and consumer groups. Many of these stakeholders utilize their own data sets to better inform their robocall mitigation activities.

For example, many scoring and analytics companies utilize so-called ‘honeypots’, which are servers that are configured to receive phone calls. By analyzing calls made to the honeypot, companies can identify robocall traffic in real-time to better inform their robocall identification analytics. Similarly, other companies will often utilize real-time call network analytics in order to identify and analyze suspicious calling patterns. Finally, many companies often utilize customer-generated complaints in order to identify illegal or unwanted robocalls to better inform their call analytics. The FTC’s data—comprised of consumer complaint information submitted

to the agency—provides an additional data set that can further inform their analytics.

Because robocallers often rapidly transition the spoofed numbers they use to make calls, the FTC's quicker release of its data provides a variety of industry stakeholders with more timely information with which to inform its analytics. Moreover, the combination of a variety of data sets (e.g., customer complaints, network analytics, etc.) provides additional information to these stakeholders so that they can better inform their respective analytics and mitigation efforts.

Finally, as highlighted in the industry-led Robocall Strike Force reports of October 26, 2016, and April 28, 2017, there are multiple fronts on which stakeholders are advancing the battle against illegal robocalls. In the coming year, it is anticipated that these efforts will continue along multiple fronts.

Ranking Member Bob Casey

Stopping Robocalls

There are a number of initiatives going on to help reduce robocalls. There is the Strike Force, FCC rules, FTC actions, education campaigns and other things. However, the number of robocalls seems to still be at an all-time high.

Question:

What action do you believe would be most helpful to reducing the number of unwanted robocalls?

USTelecom Response:

USTelecom shares the view of a broad range of industry, government and consumer stakeholders that the rapid and ever-changing nature of the robocall problem makes the potential for a single “silver bullet” both unlikely and inadvisable. An open communications network is inherently vulnerable to abuse, and the interdependent, interconnected and global nature of the internet means that areas of vulnerability exist throughout the network, and therefore cannot be realistically addressed by any single stakeholder or mitigation technique.

Given the rapid and ever-changing nature of the robocall problem, multifaceted holistic approaches are necessary—and indeed, beneficial—in order to mitigate the harms resulting from such illegal calls. Much in the same way that remediation efforts in areas such as spam or cybersecurity must continually evolve through a variety of approaches, the same can be expected with respect to robocalls.

USTelecom supports the development of a variety of solutions to the robocall problem by stakeholders throughout the internet ecosystem, including through technological measures, increased industry cooperation, heightened consumer education, and increased enforcement. In the report issued earlier this year by the Industry-led robocall strike force, the group noted that “to mitigate the problem of illegal robocalls, the industry is implementing a diverse multitude of evolving mitigation tools and efforts so that it becomes too costly for illegal robocalling campaigns to overcome the industry’s dynamic mitigation techniques.” The Strike Force focused on the following areas: (1) Authentication; (2) Empowering Consumer Choice; (3) Detection, Assessment, Traceback and Mitigation; and (4) Regulatory Support.

As noted in USTelecom’s written testimony, there have been a number of important developments in each of these areas over the last several months. For example, in the area of authentication, the SHAKEN/STIR standards development for the next generation of robocall mitigation tools that the industry had initiated prior to the Robocall Strike Force, have been accelerated by 6 months. These standards, which incorporate caller-ID authentication capabilities into the network and consumer devices, have entered the industry testing phase. Some of the initial testing of the SHAKEN standard is expected to complete later this year, with additional potential deployments anticipated as early as 2018.

In the area of Empowering Consumer Choice, there are an increasing number of tools that are being developed and actively deployed to consumers, by a growing number of national voice and device providers. USTelecom member companies, independent application developers and a growing number of diverse companies offer services today that can help older Americans reduce unknown and potentially fraudulent calls.

For example, AT&T has launched its ‘Call Protect’ service that allows customers with iPhones and HD Voice enabled Android handsets to automatically block suspected fraudulent calls. Verizon has been trialing a service that warns its wireline customers about calls identified as suspicious, and on the wireless side has deployed robocall mitigation features as part of its Caller Name ID service. And various carriers have worked with NoMorobo to facilitate their customers’ ability to use that third-party blocking service, such as Verizon’s “one click” solution that simplifies

customers' ability to sign up for the service. The website of the Federal Communications Commission (FCC) was recently updated to provide information to consumers on the growing number of tools available to them across a variety of voice platforms to protect them from illegal or unwanted calls. Equally empowering to consumers are the various education efforts underway that play an important role in mitigating illegal robocalls.

Regarding issues related to traceback and mitigation of robocalls, USTelecom has been leading an effort to mitigate the impact of certain robocalls, and identify their point of origin. Working with a broad range of 23 voice providers (including cable, wireline, wireless and wholesale providers), the Industry Traceback Group (ITB Group) shares call detail information of certain calls, thereby enabling them to quickly, efficiently and cooperatively identify the true source of fraudulent, abusive or unlawful calls, including robocalls. In instances where calls are traced to their point of origin, this often enables investigating providers to work with the originating carrier to cease such calls initiated by its customer.

Such efforts are also extremely valuable to law enforcement, since the ITB Group's ability to trace calls through several networks can substantially assist law enforcement personnel in subsequent investigations. Robust enforcement actions are often the most effective means for mitigating illegal robocalls, since they shut down the flow of such calls at the source. For example, in June of this year, the FCC initiated an enforcement action against one company that allegedly made 96 million spoofed robocalls during a 3-month period.

Finally, in the area of regulatory support, the FCC has moved forward on important initiatives—some of which were recommended by the industry-led Robocall Strike Force—that will further empower stakeholders to engage in robocall mitigation efforts. For example, the FCC recently adopted rules that permit voice service providers to combat illegal robocalls by blocking them before they reach consumers' phones. Specifically, the FCC adopted rules allowing providers to block calls from phone numbers on a Do-Not-Originate list and those that purport to be from invalid, unallocated, or unassigned numbers. The FCC has also initiated an effort regarding the governance framework for the SHAKEN and STIR standards and best practices. Finally—and perhaps most importantly—the FCC recently initiated several enforcement actions against illegal robocallers.

From Senator Sheldon Whitehouse

Question:

Last election cycle, there were several reports of robocalls being made to voters falsely telling them their ballot would not be counted unless they updated their voter registration status. How can robocalling technology be used to suppress votes? What actions can Congress take to address that threat

USTelecom Response:

Abuses of the telephony network by robocallers can take many forms. These include telephony denial of service (TDOS) attacks that can disable legitimate call centers, consumer fraud targeted toward taking money (e.g., the IRS Scam), and consumer fraud targeted at obtaining personal information. There are also reports that illegal actors can use robocalling platforms to suppress votes.

USTelecom agrees with the broad range of stakeholders from government, industry and consumer groups which maintain that a broad, multifaceted, holistic approach is best suited to addressing harms resulting from illegal robocalls, regardless of their intended focus. For example, providing consumers with the necessary tools to choose which calls to block (including political robocalls) can empower consumers in such an environment, and protect them against associated harms. Short of banning all political robocalls, it will be imperative for stakeholders to move forward with this holistic approach in order to effectively address the impact of all harmful robocalls, including those related to voter suppression.

PREPARED STATEMENT

of

Genie Barton
President
BBB Institute for Marketplace Trust
Arlington, Virginia

Hearing on
Robocall Scams

Before the
United States Senate Special Committee on Aging

Wednesday, October 4, 2017

Chairman Collins, Ranking Member Casey, Members of the Committee, thank you for giving me the opportunity to appear before you today.

My name is Genie Barton, and I serve as President of the BBB Institute for Marketplace Trust (BBBI).

I appreciate the opportunity to describe for the Committee BBBI's ongoing work to fight scams. In the United States, 50 billion dollars are lost to scams every year.¹ Data collected through our new, crowd-sourced BBB Scam Tracker tool has greatly enhanced our understanding of the nature of this intractable problem and how to combat it. In this testimony, I will summarize our recent work, including relevant insights from our research and reports, and provide data focused on scams that prey on seniors, including scams initiated by robocalls.

BBBI is the 501(c)3 educational arm of the Council of Better Business Bureaus, the national umbrella organization of the more than 100 local Better Business Bureaus serving communities across North America. BBBI partners with and leverages the reach of the BBB network. Every BBB in North America participates in Scam Tracker, reviewing and screening each consumer report before it is entered in the central data base, which is powered by BBBI.² BBBI then publishes the reports.

BBBI equips BBB staff with resources and training programs that help them to better serve their communities, particularly seniors. Grassroots senior educational programs have long been an important focus of BBB educational outreach, with scams being a major part of this outreach. Local BBB offices often have relationships with state agencies working to address the interests of seniors and relationships with senior centers in their communities. For example, the BBB located in Pittsburgh, Pennsylvania works through the Pennsylvania Department of Aging, and many of its over 90 presentations last year took place at senior community centers in its service area. BBBs power BBB Scam Tracker by reviewing each scam report, and they routinely field inquiries and share data with state and local law enforcement, especially Offices of State Attorneys General.

For more than 100 years, BBB has been working to build a trustworthy marketplace where consumers and responsible businesses can prosper. In the United States, 50 billion dollars are lost to scams every year.³ There is, we believe, no greater threat to consumers and legitimate businesses than the fraud perpetrated by con artists.

¹ Martha Deevy and Michaela Beals, *The Scope of the Problem: An Overview of Fraud Prevalence Measurement*, Financial Fraud Research Center, 2013. http://longevity.stanford.edu/wp-content/uploads/2016/07/Scope-of-the-Problem-FINAL_corrected2.pdf at 28.

² The over 100 BBBs in North America vet the scam reports that originate in their service area, using both software and staff review to determine whether the consumer is reporting an event that a reasonable person would consider to be a scam or fraud. Only those reports are passed on to BBBI for publication in BBB Scam Tracker. Please note that we are not able to investigate and independently verify that an actual fraud has occurred, only that the *allegations* of fraud appear well-founded.

³ Martha Deevy and Michaela Beals, *The Scope of the Problem: An Overview of Fraud Prevalence Measurement*, Financial Fraud Research Center, 2013. http://longevity.stanford.edu/wp-content/uploads/2016/07/Scope-of-the-Problem-FINAL_corrected2.pdf at 28.

It not only robs both consumers and legitimate businesses, but it does far more harm. It humiliates the individual scam victim. It damages the reputation of ethical businesses whose identities scammers assume. Finally, scams erode consumer trust and engagement in the marketplace.

BBB Scam Tracker

BBB Scam Tracker (www.bbb.org/scamtracker) gave BBB a crowd-sourced, digitally powered, 21st-century tactical weapon to fight the age old battle against fraud and deception. Launched throughout the U.S. and Canada in September 2015, BBB Scam Tracker is an interactive tool for consumers to report scams and fraud and warn others of malicious activity. Consumer reports capturing the scam in the consumer's own words are collected online and presented in a searchable online "heat map," showing consumers the number and types of scams reported in their communities. The tool provides a window on the scam landscape, enabling data-driven consumer alerts and tips based on current information. Reports are shared with the Federal Trade Commission for inclusion in its Consumer Sentinel database, with the National Cyber Forensics and Training Alliance, and with law enforcement agencies on request for investigative purposes.

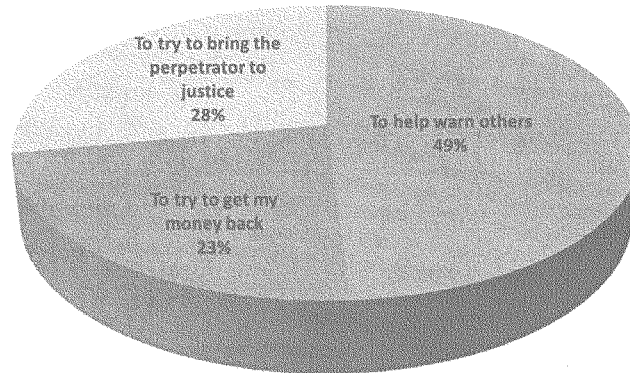
Scam Tracker is well-positioned to operate as the pre-eminent consumer reporting tool about scams. Respondents to our 2016 survey of more than 2,000 individuals said they were more likely to turn to BBB to report scams than to anywhere else (including the police). A subsequent study by FINRA Foundation and Stanford Center for Longevity also found that BBB is the first organization the public thinks of to report a scam, providing independent verification.⁴ To date, approximately 83,000⁵ scam reports have been published, and the rate of reporting per day has increased by 54% from 2016 to the end of September this year.

BBB Scam Tracker's crowd-sourced approach taps the altruistic impulse that frequently motivates consumer reporting activity of scams and fraud. When consumers are asked what would drive them to report a scam, nearly 50% indicate that they would do so to help make sure it did not happen to someone else.⁶ When the report is published, the consumer who has reported the scam often feels empowered by having taken action and less like a mere "victim". The consumer narratives drive home an important lesson—ordinary people like me get scammed. All of us are vulnerable. The impact of this reporting in warning others is amplified by our ability to connect reporters with individuals who are willing to be interviewed about their experiences.

⁴ *Findings From a Pilot Study to Measure Financial Fraud in the United States*, at 22, http://162.144.124.243/~longev0/wp-content/uploads/2017/02/SCL-Fraud-Report-Feb-2017_Draft2.pdf.

⁵ See generally, Better Business Bureau, *BBB Scam Tracker*, <https://www.bbb.org/scamtracker/us> (last visited Sep. 27, 2017).

⁶ *Cracking the Invulnerability Illusion: Stereotypes, Optimism Bias, and the Way Forward for Marketplace Scam Education* at 5, <https://www.bbb.org/globalassets/shared/media/truth-about-scams/bbb-scamprogram-whitepaper-08-digital-0630.pdf>

Figure 1: Motives for Reporting a Scam

The data and stories we gather and share through BBB Scam Tracker also have given us the power to fight scams through new evidence-based research. This research gives us insight to better target and message our outreach to the general public and engages national and local media, boosting our effectiveness in raising public awareness. The reach and searchability of the Scam Tracker database also provides valuable assistance to law enforcement and regulators, and spurs academic researchers to add to our body of knowledge about scams.

Our 2016 study, *Cracking the Invulnerability Illusion: Stereotypes, Optimism Bias, and the Way Forward for Marketplace Scam Education*, shattered previous stereotypes about vulnerability to scams. In the study we demonstrated that negative stereotypes around scam victimization predominate. When asked to describe a scam victim, consumers' responses were dominated by pejorative adjectives such as "naïve," "stupid," "gullible," "uninformed," and "old." We found that 83% percent of respondents believed that they were less at risk of being scammed than others.

Unfortunately, the belief that scams only happen to other people poses one of the biggest personal risks of all. Those who believe that it can't happen to them are less likely to heed warnings about scam activity and are not alert to the possibility that a seemingly legitimate phone call or email was actually from a scammer. One proof point is that the age group most likely to fall for a scam is actually millennials, a fact not widely recognized before this study. However, while on the whole seniors recognize their vulnerability and are therefore more cautious, when they are scammed they are most likely to suffer the largest financial loss.

While a number of studies have sought to understand the scope of the problem and the behavioral or psychological markers that distinguish scam victims, less has

been done to identify the knowledge and information that might be effective in preventing scam targets from becoming scam victims. With this in mind, our research was crafted to explore the contours of what a successful education and awareness campaign might look like. Nearly 80% respondents cited general knowledge of scam tactics and scam types as being most important in avoiding scams.⁷ The insights about scam victimization that Scam Tracker provides are helping us to better focus educational efforts to more effectively alert consumers.

In speaking to millennials and seniors alike, we strive to counter negative stereotypes with stories of real people that collectively convey the message that this can happen to anyone. We are *all* at risk and, by talking about our experiences, we help protect others with essential information about scam tactics and types. We empower ourselves, and we begin to chip away at some of the shame and stigma surrounding this issue.

The statistical insights we have derived from Scam Tracker data are important, but the value of individual stories is immeasurable, as they make the problem real and convey the critical message that this can happen to anyone. These reports also help us to understand what messaging will be most likely to best alert consumers to common traps.

BBB Risk Index

In March of last year, BBBI release its first annual report of data gathered through BBB Scam Tracker, the *2016 BBB Scam Tracker Annual Risk Report*.⁸ With this report we introduced the BBB Risk Index, a new, more nuanced conceptualization of risk. Prior to the introduction of the Index, attempts to compare scam types by relative risk, including by BBB, have generally consisted of simple rankings by frequency of exposure. This volume-based approach failed to acknowledge the multifaceted nature of scam risk. In fact, the risk posed to a given population by a particular scam type can best be understood by considering three dimensions: exposure, susceptibility, and monetary loss. By combining all three, as we have done with the BBB Risk Index, we are able to gain a far more meaningful measure of the relative risk of a given scam type. In our *Risk Report*, we applied the Index formula to various subgroups, including seniors, to identify the scams that present the greatest risk to each group.

To better understand the rationale for the Index, consider the broad spectrum of techniques employed across the scam landscape. On one end of the spectrum, a fraudster may employ a “wide net” approach. Robocalls, the subject of the hearing today, are an example of this technique. A scammer can inexpensively utilize robocalling technology to reach perhaps hundreds of thousands of individuals to find those few who would succumb to the ploy. While these scams reach a wide swath of the population, the susceptibility of those exposed is typically quite low.

⁷ *Id* at 12.

⁸ *2016 BBB Scam Tracker Annual Risk Report: A New Paradigm for Understanding Scam Risk*
www.bbb.org/riskreport.

At the other end of the spectrum is the far more intensive “high-touch” approach, as is commonly seen with romance and investment scams. These scams reach fewer individuals, but those exposed are often more likely to be successfully conned. Monetary loss is a final critical element. A con that separates mere pennies from its victims may do tremendous overall harm if it impacts a large portion of the population, while a scheme with relatively few victims may be of even greater concern if median losses are extremely high. The Index captures these real-world elements by representing the intersection of exposure, susceptibility, and monetary loss.

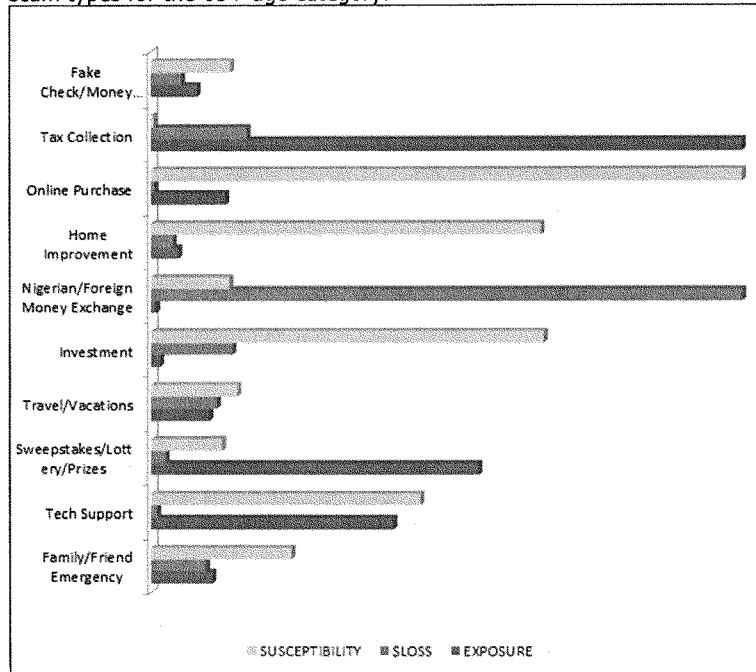
No law enforcement or regulatory agency has the resources to fight every scam. The Risk Index can help establish policy priorities and suggest resource allocation. The Risk Index can determine what are the greatest risks to a particular cohort of interest. In this testimony, we use the Risk Index to define the top 10 riskiest scams for seniors.

Approximately 16% of reports to BBB Scam Tracker are from individuals over the age of 65.⁹ By applying the BBB Risk Index discussed earlier, we are able to identify the following scam types as being the top 10 most risky for this cohort.

1. Family/Friend emergency
2. Tech Support
3. Sweepstakes/Lottery/Prizes
4. Travel/Vacations
5. Investment
6. Nigerian/Foreign Money Exchange
7. Home Improvement
8. Online Purchase
9. Tax Collection
10. Fake Check/Money Order

⁹ Data reported in this testimony is based on U.S. reports submitted to BBB Scam Tracker and published from the inception of Scam Tracker on February 13, 2015 through September 27, 2017, a period of approximately 20 months, except where otherwise indicated. These data updates result in statistics that differ from data reported in the *2016 BBB Scam Tracker Annual Risk Report*.

Figure 2 –Chart representing susceptibility, loss and exposure for top 10 risky scam types for the 65+ age category.



For seven out of these top ten scam types, the method of initial contact was a telephone call. In fact, 71% of *all* scams reported by seniors age 65+ began with a call. However, when we only look at reports that involved a monetary loss (i.e., where the target avoided the con), just 33% were initiated by telephone. This variance reflects the relatively low susceptibility levels common with telephone scams, particularly telephone scams that tend to be high-volume. For example, only 1 in 278 reports by seniors of the tax collection scam involved a dollar loss. Nonetheless, these scams are among the most risky to seniors due to high exposure levels and serious monetary losses.

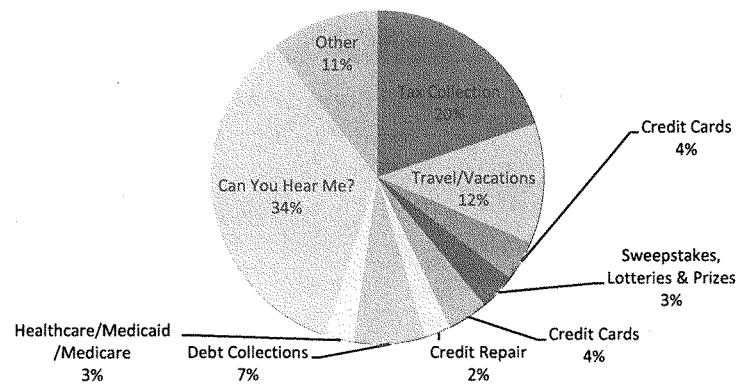
Our data show that when a senior loses money to a scam, the dollar loss is typically nearly 56% greater than losses incurred by younger individuals. The median reported loss by seniors is \$390, while the median loss reported by those under the age of 65 is \$250. The harm to retirees is further exacerbated because they are likely living on a fixed income.

Robocall Data

While we ask individuals reporting a scam to indicate if the scam was initiated by telephone, we do not currently ask if a robocall was involved. We are therefore unable to provide precise information on the percentage of all scams reported to us that were initiated by robocalls. We will consider revising this question to shed greater light on the impact of scams initiated by robocalls.

Fortunately, we do have the ability to search by keyword and have done so with respect to robocalls. The more than 400 mentions of the keyword "robocall" in consumer narratives about their experiences serve as a marker to help us understand which scams are most common among those perpetrated using this technology. The distribution of keyword "robocall" across scam types is represented in Figure 3.

Figure 3 – Scam type distribution of reports with keyword "robocall" during the period of January 1st 2016 to June 20th 2017.



There were no reports of the "family and friend emergency" scam that included the word "robocall," and tech support scams were grouped in the "other" category as just five of these reports included this keyword. These two common and high-risk telephone scams thus appear to be infrequently perpetrated using robocall technology.

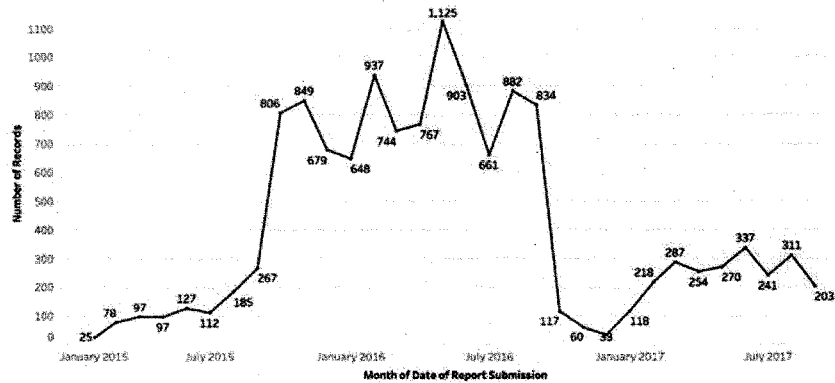
However, we caveat this conclusion based on the fact that a high number of scams are initiated by telephone and not all consumers will highlight the fact that some form of autodialer may have been used to initiate contact.

IRS Tax Collection Scam

Given that seniors are more vulnerable to the tax scam as compared to other demographics and tend to suffer greater financial losses, I would like to expand here on the information available to us on this scam type as gathered through BBB Scam Tracker reports.

In 2016, approximately 27% of all scams reported to us by seniors and 16% of scams across all age groups were classified as tax collection scams. The police raid on a call center in Mumbai, India in October 2016 resulted in an immediate 95% drop in reports of tax collection scams to BBB Scam Tracker, a decrease that continued through December of 2016, as shown in Figure 4. By January of 2017, reports of the tax scam were on the rise again, but much more slowly than in 2016. The steep drop in reports in fall 2016 is suggestive of a correlation. Today, our volume of tax scam reports has risen but is approximately 30% of the volume seen at the peak in 2016. While our data cannot explain why reports have not risen to 2016 highs, our ability to immediately detect these shifts shows the power and sensitivity of BBB Scam Tracker to take the pulse of the scam marketplace.

Figure 4: Evolution of Reports of Tax Collection Scams from January 2015 to September 2017.



As was set forth in Figure 3 above, we estimate that the IRS scam represents 20% of all robocall scams. While susceptibility levels are low, median losses are very high relative to other scam types. The median loss reported by seniors is more than \$3,000. Payment is typically collected by directing victims to read the numbers from prepaid cards, often iTunes cards, or to wire funds. Scammers often provide specific instructions about retail locations to complete these transactions, and are known to direct consumers to move from one location to another to reduce the risk of intervention by agents of the wire transfer services.

The statistical data we are able to derive from BBB Scam Tracker yield valuable insights. In addition, consumer narratives are highly instructive and help us to

understand the way scammers are working, how consumers are “falling for” the scam, and what educational approaches might be helpful. The following is an account reported to BBB Scam Tracker by a senior in Indiana who lost \$10,000:

“I received a phone call from a man claiming to be with IRS stating that I owed money. If I didn't pay they would send me to prison. He stated I would need to go to Walmart (4 different locations) to send money to them. I did wire money to them as requested. I figure that I sent approx. \$10,000 total via wire transfer. I sent the money . . . I did this because I didn't want to go to prison. I thought they were honest people. I now know this was a scam.”

BBB has found simple, unambiguous consumer fraud prevention messages to be the most effective. For years BBB had a simple message for consumers: the IRS will never call to demand immediate payment. However, in light of the fact that now that the IRS is using four private collection agencies (PCAs) to call consumers about outstanding debt, BBB has retooled our consumer fraud messaging to focus instead on pressure techniques and payment methods. We now emphasize that the IRS or its representatives will never ask you to pay over the telephone and that payments can be made in only one of two ways: Online at IRS.gov or by check or money order made out to the U.S. Treasury. We also make sure that consumers know that the IRS will never threaten them with arrest.¹⁰

Fraud prevention messages emphasizing that the IRS or its PCA representatives will never call you without first sending at least two letters are less helpful and may be problematic because individuals who receive these letters may also receive tax scam calls. Consumers who did not receive letters may assume that the letters simply got lost in the mail. We also know that scammers have learned to reference letters, even using the identifying codes for legitimate IRS notices, as we see in this recent report from a woman in New York who lost nearly \$11,000:

“‘Agent Teresa Moss’ and ‘Agent Richard Watson’ called me and told me I had a warrant for my arrest for tax evasion . . . they were the IRS and had sent me letters (which I never received). They asked me if I lived at my address (I confirmed that they had the correct address), but I told them I was certain I never received these notices (they called them the ‘CP 200 notice,’ and the ‘CP 11A notice’) . . . throughout the day they instructed which stores around my home I could visit to purchase \$50 and \$100 iTunes gift cards. I was then to immediately scratch off the sticker on the back and recite the serial code to them. I was to buy only a few at a time and not attract suspicion within the various stores . . . For eight hours I walked around and purchased these gift cards.”

The threat of arrest is a common intimidation tactic and is characteristic of many of the IRS scam reports where consumers suffered a monetary loss. Therefore anti-fraud messaging that states that the IRS or PCAs acting on behalf of the IRS will never threaten you with arrest may also be useful and may help prevent consumers from getting rattled and panicking.

¹⁰ BBB runs scam alerts on the Scam Tracker website and also provides consumer tips on scams, including the IRS scam. See, e.g. BBB tips explaining the tax scam in the U.S. and Canada at <https://www.bbb.org/taxscam/>.

"Can you hear me?" Scam

Beginning in early 2017, BBB began to receive large numbers of reports involving interactive robocalls where consumers are asked "Can you hear me?" or some variant apparently intended to solicit a "yes" response. A staggering one third of all published reports to BBB Scam Tracker this year to June 30th, 2017 can be classified as "Can you hear me?" calls.¹¹ As shown in Figure 3, 34% of all reports with keyword "robocall" are "Can you hear me?" calls. Often, these calls terminate immediately following a response. In other instances, the calls continue with additional recorded content and questions. Some are transferred to a live operator. The purported intent of these calls varies, and includes free vacations, sweepstakes, and government grants. Interestingly, only a tiny fraction of these reports (fewer than 1 in 1,000 reports) relate to tax collection. We believe the volume of reports is, at least in part, attributable to significant media coverage around this problem, but it also suggests a concerning trend toward more sophisticated uses of interactive robocall technology by con artists.

The example of a report below shows an individual who reported a \$199 dollar loss due to a Robocall scam scenario.

"[T]hey call you saying that you have been approved for a loan. they are going to ask if you are able to hear them, say no...do not say yes. they more then [sic] likely have all your information already. they [sic] will go through all that with you. and then they tell you that they are not able to use your accounts due to fees, and say that they can western union the money to you as long as you pay the fees first. if [sic] you decided to cancel your decision, they will say that you now owe them \$199 cancellation fees. and they will take it directly from your account"

The example of a report below shows an individual who encountered a robocall scam scenario but did not incur a financial loss.

"I received a call asking if I wanted to follow up on an inquiry for employment. Seeing as I've been applying for jobs, and honestly a bit desperate for one being a college student, I immediately fell into "interview mode" and said "yes" only for them to hang up. Nothing has actually happened yet, however with the sheer amount of scammers going around I felt like others should know about this method in case something does happen. I already had anxiety about answering the phone for numbers I'm not familiar with, and this is only making it much worse."

Of the nearly 10,000 published "Can you hear me?" reports, fewer than 20 involve a reported dollar loss, and those losses cannot be definitively connected to a "yes" response. We remain uncertain as to precisely what is the endgame of these scams. Cramming may be one possible outcome, but it is also possible that the "Can you hear me?" question is intended simply to confirm a live person has answered. The information we have on the volume and substance of these calls suggests an intent

¹¹ "Can you hear me?" is not one of the 30 scam types used in BBB Scam Tracker. The vast majority of these reports are classified as "phishing" or "travel/vacations." For purposes of Figure 3, we have reclassified reports as needed to create a "Can you hear me?" category.

to perpetrate a scam, but there are a large number where the caller simply disconnects, perhaps suggestive of a nasty, annoying prank.

Conclusion

In conclusion, we stand ready to assist this Special Committee, other congressional committees, the FTC, the IRS, the FBI, and any federal, state, or local agency with efforts to protect consumers from scams. As we have learned through our data collection and through our research, everyone is at risk. Everyone is vulnerable. We believe that government, media, consumer stakeholder groups, industry associations, and individual businesses both large and small, all have a role to play to fight back effectively against scams. BBB offers tools to help empower consumers to identify the common tactics and to learn to recognize the "red flags" that indicate a scam. We welcome the opportunity to share our data, our messaging, and our outreach capabilities to help put a halt to this immense problem.

Thank you very much for inviting me to be here today, and I would welcome the opportunity to answer any questions you may have.

**Questions for the Record
To Genie Barton**

From Ranking Member Bob Casey

Stopping Robocalls

There are a number of initiatives going on to help reduce robocalls. There is the Strike Force, FCC rules, FTC actions, education campaigns and other things. However, the number of robocalls seems to still be at an all-time high.

Question:

What action do you believe would be most helpful to reducing the number of unwanted robocalls?

Answer:

Ranking Member Casey, thank you for your question. BBBI believes that in order to turn the tide on fraudulent and abusive robocalls, we must all continue the efforts you described. While we have no “silver bullet” to recommend, we suggest that a task force comprised of the organizations represented at the hearing and other like-minded organizations could be an effective next step. BBB is proud that we are working closely with the FTC, the IRS, other national and local law enforcement entities, State attorneys general, and industry in the fight to protect consumers from fraudsters and that we are a recognized leader among the not-for-profit sector in combatting robocalls through consumer education and scam prevention. Our efforts include the BBB Scam Tracker reporting and research tool, consumer tips, alerts on trending telephone scams, and interviews on national media and local affiliates by the more than 100 BBBs in the communities they serve across North America. BBB would be happy to join a task force to work with others across all sectors to strike back at fraudulent and abusive robocallers with educational materials, unified messaging, and further sharing of data with entities working to bring enforcement actions. As industry continues to make technological advances, the task force could make consumers aware of new weapons they can use against robocall abuses.

From Senator Elizabeth Warren

In November 2015, Congress passed the Bipartisan Budget Act of 2015, which exempted robocalls calls “made solely to collect a debt owed to or guaranteed by the United States” from the Telephone Consumer Protection Act (TCPA)’s prior express consent requirement.¹ The Bipartisan Budget Act of 2015 authorized the Federal Communications Commission to adopt rules to “restrict or limit the number and duration” of any wireless calls made to collect debts owed to or guaranteed by the Federal Government, which included Federal student loans.

On August 11, 2016, the FCC released a Report and Order implementing Section 301 of the Bipartisan Budget Act of 2015, which limited the use of the exemption in several critical ways.²

Genie Barton

Thank you for your questions, Senator Warren, which are restated separately below.

BBB has two separate sources of data that may be pertinent to your questions: *consumer complaints* (BBB Complaint data base) and *consumer scam reports* (BBB Scam Tracker data base).³ We note that whenever a legitimate company engages in debt collection activities, scammers will often masquerade as the legitimate company. Accordingly, a number of our data points relate to scammers posing as a real

¹Section 301 of Public Law 114–74 amending Section 227(b)(2) of the Communications Act.

²“Report and Order: Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991,” Federal Communications Commission, last reviewed on October 12, 2017 available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-99A1.pdf.

³We note that BBB Scam Tracker “is a crowdsourced online tool that empowers the public to report scams and fraud and to explore reports submitted by others on an interactive “heat map.”” See generally Fletcher, Emma & Pessanha, Rubens, *2016 BBB Scam Tracker Annual Risk Report: A New Paradigm for Understanding Scam Risk* (2016) available at <https://www.bbb.org/globalassets/local-bbbs/council-113/media/scam-tracker/risk-report/bbbscamtrackerannualreport-022517-v3.pdf>. We also note that the BBB Complaint system takes complaints from consumers regarding any business, whether BBB accredited or not. See generally Better Business Bureau, Learn About Our Complaint Services, <https://www.bbb.org/council/consumer-education/complaints/> (last visited Nov. 29, 2017).

company. Sometimes it is impossible to tell whether the company is merely a scam or an actual business whose practices may be questionable.

While both the BBB Complaint and Scam Tracker data bases contain useful data, each data base has certain limitations with respect to providing accurate information that is responsive to the questions you are asking, as we explain below.

Unfortunately, neither the BBB Scam Tracker reporting form nor the BBB Complaint form asks the consumer whether the origination of the scam/complaint was via robocall. Therefore, although we have used our best efforts to make keyword searches to identify all robocalls, we may be under-reporting.

We also note that neither of our forms requests that consumers provide their specific age. The BBB Scam Report form asks consumers to State to which of the following age groups they belong: 18–24, 25–34, 35–44, 45–54, 55–64, and 65+. However, the BBB Complaint form only asks consumers to “check a box” if they are above the age of 65, and we have found that very few people appear to use this box to self-identify as over 65.

Additionally, we want to emphasize that because our data bases are based on self-reporting, the information provided here may have inherent limitations compared to data obtained through other research methods.

Because we are unable to identify all the private collection agencies authorized to collect debts owed to the Federal Government, we focused on those private debt collectors employed by the Department of Education to collect debts owed on Federal student loans.⁴

Where the question appeared to have a broader scope than student loans, we looked at complaints related to those same private collection agencies identified as contractors of the Department of Education above. Because we were not confident we could accurately differentiate between debts owed to the Federal Government and other debts, our responses to questions two and three include all complaints related to these companies’ debt collection practices.

With those caveats in mind, we hope that the information contained in the attached spreadsheets will be useful. These spreadsheets, which we have listed below for your reference under the section of this document entitled “Data Sets,” include the best data we can provide within the limitations we have noted.

In response to Question 1, we also draw your attention to the attached Data Set 1—Text of BBB Complaints on All Debt-Related Robocalls, and Data Set 3—Text of BBB Scam Tracker Reports about Purported Department of Education Private Collection Agencies. Data Set 1 provides data from our BBB Complaint data base, including the consumer’s own description of his or her complaint about a private collection agency employed by the Department of Education to collect on a Federal student loan. Data Set 3 provides data from the BBB Scam Tracker data base about consumer reports involving purported Department of Education private collection agencies. We also draw your attention to Data Set 4, which contains a list of BBB Complaints and BBB Scam Tracker reports that, based on our analysis of the language of the complaints and keyword searches, we infer are related to phone calls made to seniors by debt collectors about student loan debt.

Senator Elizabeth Warren

Question:

Now that federally contracted private debt collectors are allowed to robocall older Americans without their consent to collect Federal student loans, please share any complaint data or aggregate reports the Better Business Bureau Institute for Marketplace Trust has based on complaints received from older Americans about robocalls from Federal student loan debt collectors.

Answer:

Although, as noted above, neither the BBB Consumer Complaint data base nor the BBB Scam Tracker data base yields data that meet all the parameters of this question, we believe the five attached data sets described below contain information relevant to the question.

⁴ The list of private collection agencies we researched can be found in the drop down menu on the Department of Education website at <https://studentaid.ed.gov/sa/about/data-center/business-info/contracts/collection-agency#accountcontroltechnologyinc> with the addition of Sallie Mae/Navient, NelNet, Great Lakes and FedLoan.

Data Set 1—Text of BBB Complaints on All Debt-Related Robocalls***Timeframe: November 2014 to November 2017******Notations:***

- The complaints are derived from our BBB Complaint data base.
- Because the BBB Complaint system does not track the age of individual complainants, the complaints shown below are not senior-specific.
- The complaints below were identified by search parameters pertaining to robocalls (automated calls) regarding any loans/debts—not necessarily student loans.
- These data do not include reports that consumers filed with the BBB Scam Tracker data base, which is primarily comprised of reports addressing scams and fraudulent conduct.
- Of the approximately 900 total complaints, 60 complaints involve federally contracted debt collection companies that the Department of Education lists on their website as their contractors for the collection of Federal student loan debt.

Data Set 2—Tallies of BBB Complaints of Debt-Related Robocalls by Month and Year***Timeframe: December 2014 to October 2017******Notations:***

- The complaints are derived from the BBB Complaint data base. They may not include reports that consumers filed with the BBB Scam Tracker data base, which is primarily comprised of reports addressing scams and fraudulent conduct.
- The complaints below were identified by search parameters pertaining to robocalls regarding any loans/debts—not necessarily student loans.
- Because the BBB Complaint system does not track the specific age of individual complainants, these data include complaints from all consumers irrespective of age.

Data Set 3—Text of BBB Scam Tracker Reports about Purported Department of Education Private Collection Agencies***Timeframe: February 2015 to November 2017******Notations:***

- This data set comes from the BBB Scam Tracker Data base, as opposed to the BBB Complaint Data base.
- This data set has not been filtered by relevance to any particular type of debt collection, age of consumer, or other criteria.
- This data set only includes Scam Tracker reports that involve any of the federally contracted debt collection agencies we identify in endnote 2.
- Because the reports come from the BBB Scam Tracker data base, it is very likely that the reports described here involve fraudsters (e.g. criminal actors) representing themselves as legitimate companies.
- The BBB Scam Tracker program began beta testing in February 2015, so we note that we do not have Scam Report data prior to this month. We note that the first germane report was in May 2015.

Data Set 4—Complaints and Scam Reports Related to Seniors and Student Loan Debt***Timeframe: November 2014 to November 2017******Notations:***

- This data base contains combined BBB Scam Tracker and BBB Complaint data that we inferred to be related to debt collectors contacting seniors about student debt through phone calls (not limited to the use of robocall technology).
- We note that the data here consist of reports and complaints that address scenarios which are not limited to Federal student loan debt.

Data Set 5—Sample Student Loan Complaints and Scam Reports***Timeframe: November 2014 to November 2017******Notations:***

We believe these anecdotes illustrate, in consumers' own words, some of the challenges they face when engaging with student loan debt collectors or scammers who pose as such debt collectors.

Question:

Has the BBB Institute noticed any increases or other trends in complaint volume from older Americans regarding Federal student loan-related robocalls since Congress allowed Federal debt collectors to robocall seniors without their consent?

Answer:

Unfortunately, because of the limitations explained above around our current data-gathering processes and the limited number of responses available, we are unable to provide data that would show whether there has been an increase in the complaint volume from older Americans related to student loan debt repayment or to provide relevant insights on other possibly significant trends. Nonetheless, in case it could be helpful, in Data Set 2 we created a chart showing aggregated complaint data on all calls related to debt collection from December 2014 to October 2017. These data do not reveal any particular trends. Because the BBB complaint data base does not track the specific age of complainants, it is not possible to determine if older Americans as a cohort were affected differently from other age groups.

Data Set 5—Sample Student Loan Complaints and Scam Reports—provides sample narratives from consumers whom we were able to identify with confidence as older Americans who provide, in their own words, a complaint about a negative experience they suffered in connection with a robocall-initiated call to collect a student loan debt or by a robocall-initiated scam where the fraudster posed as a legitimate debt collection agent seeking repayment for a student loan.

Question:

Please share any complaint data, complaint information, or aggregate reports regarding complaints from older Americans about robocalls made by debt collectors on behalf of the Federal Government for any debts owed to or guaranteed by the United States.

Answer:

To answer this question, we searched both the BBB Consumer Complaint data base and the BBB Scam Tracker data base, using “robocall” and “student,” “debt,” and similar terms, e.g., “autodial” to find relevant data. We have attached the four Excel spreadsheets which we have described above on pages 5–7 of this document that the Committee may find useful in answering this question. We have also attached a document, entitled Data Set 5—Sample Student Loan Complaints and Scam Reports, which provides typical examples (in the consumer’s own words) of consumer complaints or scam reports. We hope these narratives will provide insight into subpar behaviors of private debt collection agencies or fraudsters imitating them.

From Senator Sheldon Whitehouse

Question:

Last election cycle, there were several reports of robocalls being made to voters falsely telling them their ballot would not be counted unless they updated their voter registration status. How can robocalling technology be used to suppress votes? What actions can Congress take to address that threat?

Answer:

Thank you for your question, Senator Whitehouse. BBB supports and commends the efforts of consumer educators, law enforcement, and the media to combat voter fraud. However, BBB does not have expertise in robocall technology, so we do not know how to counter the use of robocalling technology to prevent this from happening in the future. Moreover, as a non-partisan organization that is focused on marketplace trust and business self-regulation, voters do not contact BBB with concerns about voter suppression activities.

Additional Statements for the Record

iconectiv

October 10, 2017

The Honorable Susan M. Collins and the Honorable Bob Casey
United States Senate Special Committee on Aging
G31 Dirksen Senate Office Building
Washington DC 20510

Dear Chair Collins and Senator Casey,

On behalf of Telcordia Technologies, Inc. dba iconectiv ("iconectiv"), I am writing to request this letter be made part of the official record for the hearing on October 4, 2017 regarding robocalling. We write to provide the Committee with technical background regarding work in progress to develop tools to address harmful robocalls.

The Internet Engineering Task Force (IETF) and a joint taskforce of the Alliance for Telecommunications Industry Solutions (ATIS) and SIP Forum have developed the SHAKEN (Signature-based Handling of Asserted information using toKENs) standard that provides a framework for service providers to implement new certificate-based anti-spoofing measures. SHAKEN provides an industry framework for managing the deployment of Secure Telephone Identity (STI) technologies. The framework provides end-to-end cryptographic authentication and verification of the telephone identity and related information in a VoIP-based service provider network to avoid spoofing. As a result, consumers will be notified as to the caller's ID veracity and the consumer will retain the ability to decide whether to answer calls even if the call is not verified.

The technical work in these standards setting bodies has made significant progress on Caller ID Authentication standards. These efforts strive to have the SHAKEN/STIR standard be globally applicable. Beyond the development of the SHAKEN framework and associated governance structure, ATIS continues the ongoing work to examine SHAKEN-related Best Practices, Attestation and Origination Identifiers, and the development of a framework for the display of verified Caller ID. In addition, work is underway to develop the technical requirements and message flows for the Policy Administrator (PA) and to also document the Best Practices for Certificate Authorities.

We do recognize that not all Caller ID spoofing is done for fraudulent purposes. There are legitimate uses for spoofing, such as doctors calling back patients from their personal cell phone but displaying the office number on the Caller ID or call centers calling on behalf of a business displaying the number to call to make a do-not-call request, as required by FCC rules, instead of the number for the originating line used by the call center. Common business practices such as multi-homing must receive additional assessment to ensure that calls made by these telecom

iconectiv

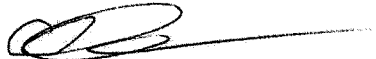
constituencies are properly handled and not blocked nor unanswered simply because their Caller IDs are not authenticated.

iconectiv has been an authoritative partner of the communications industry for more than thirty years. A U.S. based company, iconectiv has been a major architect of the United States' telecommunications system since it was formed at the divestiture of AT&T. We have first-hand knowledge of the intricacies and complexities of creating, operating and securing the country's telecommunications infrastructure. Our core competencies include highly scalable industry database management, numbering services, third-party authentication and fraud prevention for the telecommunications industry.

iconectiv participates in leadership positions across the industry including the ATIS Board of Directors and Executive Committee, the ATIS Technology and Operations (TOPS) Council and Testbed Landscape Team (TLT), the SIP (Session Initiation Protocol) Forum Board of Directors, and the TIA Board of Directors. We also serve as the Editor of the ATIS/SIP Forum IP NNI Taskforce IP Routing Document and SHAKEN Governance Model and Certificate Management Procedures. In addition, we both lead and participate on key industry committees that address robocalls and spoofing.

We thank you for your attention to our thoughts and efforts and look forward to working with you in the future. Please let us know if you have questions.

Sincerely yours,



CHRIS DRAKE
Chief Technology Officer

