

ABUSIVE ROBOCALLS AND HOW WE CAN STOP THEM

HEARING BEFORE THE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE ONE HUNDRED FIFTEENTH CONGRESS SECOND SESSION

APRIL 18, 2018

Printed for the use of the Committee on Commerce, Science, and Transportation



Available online: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2024

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JOHN THUNE, South Dakota, *Chairman*

ROGER WICKER, Mississippi	BILL NELSON, Florida, <i>Ranking</i>
ROY BLUNT, Missouri	MARIA CANTWELL, Washington
TED CRUZ, Texas	AMY KLOBUCHAR, Minnesota
DEB FISCHER, Nebraska	RICHARD BLUMENTHAL, Connecticut
JERRY MORAN, Kansas	BRIAN SCHATZ, Hawaii
DAN SULLIVAN, Alaska	EDWARD MARKEY, Massachusetts
DEAN HELLER, Nevada	TOM UDALL, New Mexico
JAMES INHOFE, Oklahoma	GARY PETERS, Michigan
MIKE LEE, Utah	TAMMY BALDWIN, Wisconsin
RON JOHNSON, Wisconsin	TAMMY DUCKWORTH, Illinois
SHELLEY MOORE CAPITO, West Virginia	MAGGIE HASSAN, New Hampshire
CORY GARDNER, Colorado	CATHERINE CORTEZ MASTO, Nevada
TODD YOUNG, Indiana	JON TESTER, Montana

NICK ROSSI, *Staff Director*

ADRIAN ARNAKIS, *Deputy Staff Director*

JASON VAN BEEK, *General Counsel*

KIM LIPSKY, *Democratic Staff Director*

CHRIS DAY, *Democratic Deputy Staff Director*

RENAE BLACK, *Senior Counsel*

CONTENTS

Hearing held on April 18, 2018	Page 1
Statement of Senator Thune	1
Letter dated April 16, 2018 to Hon. John Thune and Hon. Bill Nelson from Marc Rotenberg, EPIC President; Alan Rotenberg, EPIC Senior Counsel; and Christine Bannan, EPIC Administrative Law and Policy Fellow	96
Letter dated April 17, 2018 to Hon. John Thune and Hon. Bill Nelson from Richard Hunt, President and CEO, Consumer Bankers Association	98
Letter dated April 18, 2018 to Hon. John Thune and Hon. Bill Nelson from Meredith Atwell Baker, President and CEO, CTIA	99
Statement of Senator Blumenthal	3
Statement of Senator Markey	21
Statement of Senator Tester	24
Statement of Senator Klobuchar	24
Statement of Senator Cortez Masto	89
Statement of Senator Baldwin	93

WITNESSES

Adrian Abramovich, Former President, Marketing Strategy Leaders (Dis- solved 1/29/2016)	4
Prepared statement	6
Rosemary Harold, Chief, Enforcement Bureau, Federal Communications Com- mission	25
Prepared statement	27
Lois Greisman, Associate Director, Marketing, Practices Division, Bureau of Consumer Protection, Federal Trade Commission	28
Prepared statement	30
Kevin Rupy, Vice President, Law and Policy, USTelecom	54
Prepared statement	56
Scott Delacourt, Partner, Wiley Rein LLP, On Behalf of the U.S. Chamber Institute for Legal Reform	58
Prepared statement	59
Margot Freeman Saunders, Senior Counsel, National Consumer Law Center ..	65
Prepared statement	67

APPENDIX

Letter dated April 17, 2018 to Hon. John Thune and Hon. Bill Nelson from American Bankers Association, Consumer Bankers Association, Credit Union National Association, Electronic Transactions Association, Inde- pendent Community Bankers of America, National Association of Federally- Insured Credit Unions, National Council of Higher Education Resources, and Student Loan Servicing Alliance	103
Letter dated April 28, 2017 to Marlene H. Dortch, Secretary, Federal Commu- nications Commission from Brian Scarpelli, Senior Policy Council, ACT The App Association; Thomas E. Goode, General Counsel, ATS; Krista L. Witanowski, Assistant Vice President, Regulatory Affairs, CTIA; Kevin G. Rupy, Vice President, Law & Policy, USTelecom	104
Response to written questions submitted to Adrian Abramovich by: Hon. Catherine Cortez Masto	122
Response to written questions submitted to Rosemary Harold by: Hon. John Thune	123
Hon. Maria Cantwell	123

IV

	Page
Response to written questions submitted to Rosemary Harold by—Continued	
Hon. Catherine Cortez Masto	124
Response to written questions submitted to Lois Greisman by:	
Hon. Maria Cantwell	126
Hon. Tom Udall	127
Hon. Catherine Cortez Masto	127
Response to written questions submitted to Kevin Rupy by:	
Hon. Maria Cantwell	130
Hon. Richard Blumenthal	131
Hon. Tom Udall	131
Hon. Catherine Cortez Masto	133
Response to written questions submitted to Scott Delacourt by:	
Hon. John Thune	135
Hon. Maria Cantwell	136
Hon. Catherine Cortez Masto	137

ABUSIVE ROBOCALLS AND HOW WE CAN STOP THEM

WEDNESDAY, APRIL 18, 2018

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10:09 a.m. in room SR-253, Russell Senate Office Building, Hon. John Thune, Chairman of the Committee, presiding.

Present: Senators Thune [presiding], Wicker, Blunt, Heller, Gardner, Blumenthal, Nelson, Cantwell, Klobuchar, Tester, Udall, Baldwin, Markey, Peters, Hassan, and Cortez Masto.

OPENING STATEMENT OF HON. JOHN THUNE, U.S. SENATOR FROM SOUTH DAKOTA

The CHAIRMAN. Good morning. In the United States Senate, we often have heated disagreements over important issues facing our country. Even in the Commerce Committee, which has a long-standing tradition of reaching bipartisan compromise when possible, we don't always see eye-to-eye when it comes to contentious issues. But today we are here to address an issue that I'm sure we can all agree on: unwanted, abusive, and illegal robocalls have got to stop.

Unsolicited robocalls consistently rank among the top consumer complaints to the Federal Trade Commission and the Federal Communications Commission. Beyond just being annoying, many of those who send out unwanted robocalls do so with the intent to defraud consumers. As more phone systems move from copper wires to the Internet, it has become easier and cheaper for bad actors to make illegal robocalls from anywhere in the world.

These new technologies have also made it easier for scammers to hide from law enforcement and to seek to gain their victims' trust by displaying fake caller ID information. Known as "spoofing," this technique allows a fraudulent call to show up on recipients' caller ID as a number within their area code, or even with many of the same digits as their own phone number, making it appear like a trustworthy local number. I am sure that many of us, as well as many of our constituents, have experienced this phenomenon.

The goal of scammers using spoofed robocalls is often to get money out of unsuspecting recipients, and some of their methods can be particularly malicious. For instance, given that yesterday was tax day, one common scam, especially at this time of year, is the "IRS scam." This scam involves the caller pretending to rep-

resent the IRS in order to scare the victim into providing money or personal information to avoid phony tax penalties.

Perhaps the biggest negative effect of the increasing prevalence of unwanted robocalls is that they frustrate recipients to the point that they are less likely to answer legitimate calls.

It's important to remember that robocalls are not inherently negative. Many important services are carried out via robocall where companies and call recipients have pre-established relationships and where the consumer has agreed to participate in these types of calls. Indeed, some entities, like hospitals and pharmacies, use robocalls to remind a patient of an upcoming appointment or that a prescription is ready for pickup. In addition, automakers often use robocalls to warn vehicle owners of urgent safety recalls. Missing calls like these can have life-or-death consequences for recipients.

Today we have the opportunity to hear from enforcement officials responsible for combating illegal robocallers and from industry representatives who can speak to new methods for preventing consumers from receiving unwanted calls in the first place.

We also have the opportunity to hear from Mr. Adrian Abramovich, who, according to the FCC, allegedly made almost 100 million robocalls in a three-month period in 2016.

On October 10, 2017, the Committee sent Mr. Abramovich a letter of inquiry regarding the FCC's notice of apparent liability, asking several questions about his conduct. On November 3, 2017, through his counsel, Mr. Abramovich informed the Committee that he would not be providing information in response to the Committee's inquiry.

This past March, I invited Mr. Abramovich to appear voluntarily for today's hearing, but through his counsel, he declined. In light of Mr. Abramovich's decision to decline the Committee's invitation and refusal to provide information in response to the Committee's inquiry, a subpoena requiring Mr. Abramovich's appearance before the Committee was issued.

Mr. Abramovich, your participation in today's hearing is important. According to the FCC, you allegedly made nearly 100 million robocalls to American consumers purporting to be a well-known travel or hospitality company, such as TripAdvisor, Expedia, Marriott, or Hilton. If a robocall recipient answered and pressed "1" for more information, the consumer would be directed to a Mexican hotel and resort chain engaged in selling timeshares and vacation packages that had contracted with you, Mr. Abramovich, to receive calls generated by your network.

Mr. Abramovich, I expect that today you will shed some light on your past conduct and provide the Committee with your unique perspective on the technologies and practices behind abusive robocalls. With this information, and that of the second panel, the Committee should better understand this problem and what steps might be necessary to end this abusive practice.

Finally, before I turn to the Ranking Member, who today Senator Blumenthal is serving in that role, I would like to just note that the recent omnibus appropriations bill included Committee-approved legislation he sponsored and I say "he sponsored," Senator Nelson, with Senators Fischer, Klobuchar, Blunt, and Duckworth

to empower the FCC to combat spoofing originating from international locations. We'll be eager to hear how new law will be implemented and what more needs to be done.

So with that, I'm going to turn to Senator Blumenthal for an opening statement.

**STATEMENT OF HON. RICHARD BLUMENTHAL,
U.S. SENATOR FROM CONNECTICUT**

Senator BLUMENTHAL. Thank you, Senator Thune, and thank you for having this hearing today, which deals with a pernicious and prevalent problem. There is bipartisan loathing for robocalls, and today we will hear from some of the government officials who have responsibility for stopping them, but also from someone who has been responsible, Mr. Abramovich, for perpetrating them.

They are rightly abhorred by consumers. They are not only oppressive and obnoxious, but they are extraordinarily prevalent, despite enforcement efforts by the Federal Trade Commission under existing law. The simple fact is that the Do Not Call list is totally ineffectual against them. The evidence is that consumers still are plagued with them.

And that is why today I am introducing the ROBOCOP bill, Repeated Objectionable Bothering of Consumers on Phones Act. The ROBOCOP bill will require phone companies to offer effective tools to block robocalls to consumers at no extra cost to them. At the same time, it will enable emergency calls or others for legitimate purposes to continue as a robust mechanism.

And I'm very proud to be joined by a number of my colleagues, including Senator Markey, of this Committee, who has been a leader, and Senator Baldwin, who is also on the Committee.

I join Senator Thune in the hope that, Mr. Abramovich, you will answer fully and completely the questions that we have for you today. You have become the face of this problem. You may think it is unjust, and that your appearance here today, as you've said in your testimony, will impact your settlement with the FCC.

But the fact of the matter is that you have a duty to answer these questions, and Senator Thune has recited a proposed fine of \$120 million that the FCC has proposed. The fine is a result of more than 100 million illegal robocalls during a 3-month period in 2016. That is a phenomenal record of consumer abuse. The robocalls involved in this campaign displayed misleading or inaccurate caller ID information designed to make the calls appear to be originated locally to the recipient.

So I hope that you will help us, in fact, shed some light on this problem and that you will explain any inability to answer our questions. If you answer them selectively, you will, of course, jeopardize your Fifth Amendment right if you wish to invoke it, but you have an obligation to be forthcoming here today and to help alleviate some of the harm that you have done already. And I hope that we will learn more in support of the legislation that I've introduced, the ROBOCOP bill, but also other legislation that can take action against this continuing and abusive consumer harm that literally hits everyone.

No one is immune from robocalls. Whether you own a cell phone or a landline, there is no escaping them. Unwanted calls reach our

most vulnerable and susceptible populations, particularly I know this as a member of the Special Committee on Aging because seniors and older Americans are often targeted, and they are often victims of the scams that are advanced through robocalls.

In 2017, the FCC made it crystal clear that carriers can identify and block these calls from known scam numbers, and I hope that today's hearing will also result in more vigorous enforcement of existing laws along with support for new laws that will enable tougher penalties, stronger deterrents, and better consumer protection.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Blumenthal.

Mr. Abramovich, I understand you have an opening statement. And so we would ask you at this point to proceed with that. Welcome.

**STATEMENT OF ADRIAN ABRAMOVICH, FORMER PRESIDENT,
MARKETING STRATEGY LEADERS (DISSOLVED 1/29/2016)**

Mr. ABRAMOVICH. Yes, sir.

Good morning to everyone. Chairman Thune, Ranking Member Nelson, and other members of the Committee, my name is Adrian Abramovich. I have been engaged in business with long distance telephone providers, wireless services providers, and conducting marketing activities for more than 15 years.

On June 22, 2007, the FCC initiated a forfeiture action against me with a proposed penalty fine of \$120 million and alleging that I perpetrated one of the largest spoof robocall campaign ever. These allegations obviously have generated immense publicity, to the point that I am here today before a Senate Committee of the United States of America.

In no way did I seek more publicity or to engage in public discussion about the pending FCC action or my defenses. I filed a response to the FCC, I denied engaging in the fraudulent activities and the misrepresentation alleged by the FCC, and sought to reduce the amount of the proposed forfeiture. It was always my intent with the FCC to negotiate toward an appropriate fine within my ability to pay such amount.

I did not come here today to testify because putting a further spotlight on my pending case can only hurt my chances to resolve this matter with the FCC. Having to come here today will no doubt portray me as the face of these unwanted robocalls, will prejudice my ongoing case with the FCC, and might also incriminate me with potential criminal charges.

I am here now because the Committee served me with a subpoena. Instead of refusing to answer questions, I will make a good faith effort to answer questions within my industry-wide knowledge of telemarketing and the type of calls you are investigating. However, I will invoke my Fifth Amendment privilege not to answer questions seeking specific factual information regarding the allegations made by the FCC against me. With regard to the FCC allegations, I will refer to and incorporate my response to the FCC, which has been filed with this Committee.

Because the FCC allegations will certainly be discussed today, I will briefly address the main points of my defense.

I have denied and continue to deny any intent to defraud, cause harm, or wrongfully obtain anything of value. The resorts associated with telemarketing activities were indeed real resorts, offering real vacation packages. The packages were exclusively available to qualified persons, all the terms and conditions were clearly explained, including the timeshare presentation requirement. And the FCC does not cite a single complaint about the quality of vacation, accommodation, of amenities.

The extent of my activities has been significantly overstated. I am not the king pin of robocalling that is alleged. While the allegations made in my case might be the biggest the FCC investigated, the FTC also regulates the telemarketing activities and conducts enforcement. In my response, I cite to several other cases involving as much or more call volume than my case and the same exact spoofing.

One specific case is the *Caribbean Cruise Line*. This specific case alleges that the defendants made 15 more daily spoofed calls than the allegations against me, falsely claimed that they were associated with a political survey, and falsely claimed that the cruises were free, none of which is alleged in my case.

In the *Caribbean Cruise Line*, the enforcement efforts targeted all the participants in the autodial campaign, including lead generation, travel provider, and the carrier. In my case, I'm the only target, and my proposed fine is 10 times all the fines imposed in the *Caribbean Cruise* case against all the participants.

The effect on consumers has been also overstated in my case. The amount of actual calls getting through to consumers is much, much less than the number of calls dialed. Ninety percent of the calls detailed by the FCC were less than a minute. Less than 2 percent of any consumers have meaningful interaction with these calls.

In an effort to help the Committee here today, I can generally speak about these phone calls. One of the main issues you have in addressing these calls is that the technology is easy to obtain and can be used by anyone. There is available open software that allows anyone to make thousands of automated phone calls with a click of a button. This software is totally customizable. But the biggest issue to stop robocall is the availability of carriers to accommodate these type of calls. There are companies that advertise on the web right now that offer long distance carrier services for "Dialer/Short Duration Termination," also known as robocalls. To me, this is where the enforcement needs to focus on to stop this activity.

In conclusion, as you have noticed today, English is not my first language. And I have, of course, prepared this statement with the assistance of my counsel. Throughout my questioning, I might need for you to repeat or rephrase a question, and I might also need to confer with my attorney prior to answering a question. I will do my best to answer all your questions here and to cooperate in this hearing.

Thank you.

[The prepared statement of Mr. Abramovich follows:]

PREPARED STATEMENT OF ADRIAN ABRAMOVICH, FORMER PRESIDENT, MARKETING
STRATEGY LEADERS (DISSOLVED 1/29/2016)

Chairman Thune, Ranking Member Nelson and the other members of the Committee:

Introduction

My name is Adrian Abramovich, I have been engaged in business with long distance telephone providers, wireless service providers and conducting marketing activities for more than 15 years. On June 22, 2017, the Federal Communications Commission initiated a forfeiture action against me with a proposed penalty of \$120,000,000 and alleging that I perpetrated one of the largest spoofed robocall campaigns ever. These allegations obviously have generated immense publicity, to the point that I am here today before a Senate Committee of the United States of America.

In no way did I seek more publicity or to engage in public discussion about the pending FCC action or my defenses. I filed a response to the FCC, I denied engaging in the fraudulent activities and the misrepresentation alleged by the FCC and sought to reduce the amount of the proposed forfeiture. It was always my intent with the FCC to negotiate towards an appropriate fine within my ability to pay such amount. (A copy of my June 27, 2017 "Response" is attached hereto as Exhibit A).

I did not want to come here today to testify because putting a further spotlight on my pending case can only hurt my chances to resolve this matter with the FCC. Having to come here today will no doubt portray me as the face of these robocalls, will prejudice my ongoing case with the FCC and may also incriminate me with potential criminal charges.

I am here now because the Committee served me with a subpoena. Instead of refusing to answer questions, I will make a good faith effort to answer questions within my industry wide knowledge of telemarketing and the type of calls you are investigating. However, I will invoke my 5th amendment privilege to not answer questions seeking specific factual information regarding the allegations made by the FCC against me. With regard to the FCC allegations I will refer to and incorporate my Response to the FCC which has been filed with this Committee.

Conduct Alleged by the FCC

Because the FCC allegations will certainly be discussed today, I will briefly address the main points of my defense:

- (a) I have denied and continue to deny any intent to defraud, cause harm or wrongfully obtain anything of value. The resorts associated with my telemarketing activities were indeed real resorts, offering real vacation packages, the packages were exclusively available only to qualified persons, all the terms and conditions were clearly explained (including the timeshare presentation requirement); and the FCC does not cite to a single complaint about the quality of the vacation, accommodations or amenities;
- (b) The extent of my activities has been significantly overstated. I am not the king pin of robocalling that is alleged. While the allegations made in my case may be the biggest for the FCC, the Federal Trade Commission also regulates telemarketing activities and conducts enforcement. In my Response, I cite to several other cases involving as much or more call volume than my case and the exact same spoofing.
- (c) One Specific case is the Caribbean Cruise Line case. This specific case alleges that the defendants made 15 times more daily spoofed robocalls than the allegations against me, falsely claimed that they were associated with a political survey, and falsely claimed that the cruises were free. None of which is alleged in my case.
- (d) In the Caribbean Cruise Line case, the enforcement efforts targeted all the participants in the autodial campaign, including lead generation, travel provider and the carrier. In my case I am the only target and my proposed fine is ten times all the fines imposed in the Caribbean Cruise case against all the participants.
- (e) The effect on consumers has also been overstated in my case. The amount of actual calls getting through to consumers is much less than the number of calls dialed. 96 percent of all calls detailed by the FCC were less than 1 minute. The majority of those do not bother anyone. Less than 2 percent of any consumers have any meaningful interaction with these calls.

Information for the Committee

In an effort to help the committee here today, I can generally speak about these phone calls and how to help limit them. One of the main issues you have in addressing these calls is that the technology is easy to obtain and can be used by anyone. Anyone can start a large autodial campaign from a home office.

With regard to DIALING and SPOOFING

There is available open source software that can be misused by someone to make thousands of automated phone calls with the click of a button. This software is totally customizable based on the needs of any particular campaign.

There are also hosted auto-dialer services that are harder to be misused because of more control by the company, but they can still be improperly used and regulation of these companies may help.

There are websites right now you can find on google that offer volume pricing for using their “robocalling” system that can handle “millions upon millions of calls”. I found these advertisements using google a few days ago.

With regard to LONG DISTANCE PROVIDERS

Once you have this software all you need is to then install your now customized auto-dialer platform to a cloud service and using the right long distance company to start placing calls.

There are companies that advertise on the web right now that offer long distance carrier service for “Dialer/Short Duration Termination” calls. These are robocalls. Clearly regulation needs to address the carriers and providers and require the major carriers to detect robocalls activity.

Conclusion

As you have notice today, English is not my first language, and I have of course prepared this statement with the assistance of counsel. Throughout my questioning I may need for you to repeat or rephrase a question and I may also need to confer with my attorney prior to answering a question. I will do my best to answer your questions here today and to cooperate in this legislative hearing.

EXHIBIT A

LAW OFFICE OF
RODOLFO NUÑEZ, P.A.

OFFICE:
2100 SALZEDO STREET, SUITE 303
CORAL GABLES, FLORIDA 33134

PHONE: (305) 443-2440
FACSIMILE: (305) 443-2334
E-MAIL: RNUNEZ@ACG-LAW.COM

July 27, 2017

Via Overnight Delivery
Richard A. Hindman, Chief
Telecommunications Consumers Division
Enforcement Bureau
Federal Communications Commission
445 12th Street, SW, Rm. 4-C224
Washington, DC 20554

RE: In the Matter of Adrian Abramovich, Marketing Strategy Leaders,
Inc. and Marketing Leaders, Inc.
File No.: EB-TCD-15-00020488
NAL/Acct. No.: 0026627141

Dear Mr. Hindman:

Please be advised that undersigned counsel, a member in good standing of the Florida Bar, hereby appears on behalf of Adrian Abramovich, Marketing Strategy Leaders, Inc. and Marketing Leaders, Inc. (hereinafter collectively referred to as "Respondents") in the above referenced matter before the Federal Communication Commission (hereinafter referred to as the "FCC" or "Commission"). Any future notices or other written communications pertaining to this matter should be furnished and/or copied to my attention. The following constitutes a written statement in response to the Citation and Order and the Notice of Apparent Liability for Forfeiture that were Released on June 22, 2017.

Introduction

First and foremost, Adrian Abramovich denies the factual allegations made in the Notice of Apparent Liability for Forfeiture (hereinafter referred to as "NAL") and the Citation and Order (hereinafter referred to as "Citation") specifically regarding any intent on his part to defraud, cause harm or wrongfully obtain anything of value. For purposes of this written statement and in an attempt to amicably resolve the NAL, Mr. Abramovich neither admits nor denies the factual allegations of conducting telemarketing activities through the use of prerecorded calls and transmitting inaccurate caller ID information.

July 27, 2017
 FCC File No. EB-TCD-15-00020488
 Page 2 of 8

Both the NAL and Citation allege that Mr. Abramovich assisted travel companies by providing telemarketing efforts that would generate leads for live operators to offer discounted vacation packages to consumers. These live operators were employed and directed by unrelated third parties that were clients of Mr. Abramovich.

In response to the Citation, the affidavit of Mr. Abramovich is contemporaneously being submitted. In the Affidavit, Mr. Abramovich states that on the release date of June 22, 2017, he became aware of the Citation and immediately ceased to conduct any activity that could possibly be associated with the violations described in the Citation, specifically any violation of the Act and Rules that govern solicitations, prerecorded, and autodialed telephone calls and the federal wire fraud statute. As of June 22, 2017, Mr. Abramovich ceased any and all telemarketing or lead generation activities.

With regard to the Notice of Apparent Liability for Forfeiture, and as more fully set forth below, Mr. Abramovich contends that the proposed forfeiture amount fails to properly apply the factors necessary for the imposition of a forfeiture order against Mr. Abramovich, including his ability to pay the proposed forfeiture amount and is otherwise unconstitutional. Based on the facts and arguments presented below, Respondents contend that a significant reduction of the proposed forfeiture amount is warranted. Moreover, Mr. Abramovich stands ready to engage in negotiations with the Commission for the purpose of reaching a consent judgment concerning the acts alleged in the Citation and NAL.

Detailed Factual Statement

1. The Commission's Notice of Apparent Liability for Forfeiture (hereinafter referred to as "NAL") relies on call records subpoenaed for the period time between October 1, 2016 through December 31, 2016.¹
2. During the applicable period of time relied upon in the NAL, Mr. Abramovich was engaged in the business of lead generation for unrelated third-party clients.² Mr. Abramovich conducted these operations through two companies, namely Exclusive Leads Services, Inc. (hereinafter referred to as "Exclusive Leads") and Emerald Media, Inc. (hereinafter referred to as "Emerald Media").³
3. Mr. Abramovich ceased conducting any business through his prior company, Marketing Strategy Leaders, Inc. (hereinafter referred to as "MSL"), on or about December 23, 2015, and the company was voluntarily dissolved on January 29, 2016.⁴

¹ Notice of Apparent Liability for Forfeiture at ¶9.

² Adrian Abramovich Affidavit at ¶ 2.

³ *Id.*

⁴ *Id.* at ¶ 3.

July 27, 2017
FCC File No. EB-TCD-15-00020488
Page 3 of 8

4. For purposes of the analysis involving the claim that Mr. Abramovich is unable to pay the proposed forfeiture the following financial information is being provided:

5. On June 22, 2017, Mr. Abramovich became aware of the Citation and NAL and in response ceased any and all telemarketing or lead generation activities.⁶

Appropriateness of Proposed Forfeiture Amount

Assuming for purposes of this response that the factual allegations of conducting telemarketing activities through the use of prerecorded calls and transmitting inaccurate caller ID information can be proven at a trial de novo, the forfeiture amount is excessive and should be reduced. The Communications Act requires the FCC to appropriately consider and properly balance "the nature, circumstances, extent, and gravity of the violation, and with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require." 47 U.S.C. § 503(b) (2)(E). *See also United States v. Unipoint Technologies, Inc.*, 159 F. Supp.3d 262, 273 (D. Mass. 2016). In this matter, the FCC has placed undue emphasis on the sheer volume of calls made by Mr. Abramovich instead of the calls that actually affected consumers, the FCC wrongly ascribed to Mr. Abramovich the entire responsibility for the telemarketing operations, the FCC improperly attributed to Mr. Abramovich a prior offense factor, and the FCC failed to assess Mr. Abramovich's ability to pay the historic proposed forfeiture amount.

Extent and Gravity of the Violation

The FCC has placed a disproportionate amount of emphasis on the volume of outgoing lead generating calls. In paragraph 25 of the NAL, the Commission places great weight on the call volume and the asserted egregiousness of the massive amount of activity in imposing a

July 27, 2017
 FCC File No. EB-TCD-15-00020488
 Page 4 of 8

proposed base forfeiture amount of \$80 million. Then again in paragraph 26 the same volume of calls and the same egregiousness is cited as the primary reason to assess an upward adjustment of an additional \$40 million. The FCC analysis seemingly imposes the proposed forfeiture amount without any regard to the amount of calls that had any actual and meaningful impact on consumers.

The FCC is imposing the proposed forfeiture amount on a sample of 80,000 calls and such calls are set forth in the Carrier Call Detail Records cited in the NAL and provided to the Respondents. A cursory glance through the Carrier Call Detail Records reveals that the vast majority of calls depict a duration of less than one minute. Enclosed herein as Exhibit A is a breakdown of the calls identified in the Carrier Call Detail distinguishing calls by duration in accordance with the carrier provided information.⁷ Calls identified by the carrier with a duration of 54 seconds or less comprise 76,814 calls, representing 95.99% of the entire sample upon which the forfeiture is based.⁸ These short duration calls result from a combination of out of service or disconnected phone lines with messages, facsimile machines, voice mail, or consumers that immediately hung up the phone. In other words, less than five percent of the consumers who received calls were subjected to a prerecorded message of any kind. There were only 1,448 calls in excess of five minutes, where the consumer is likely to have listened to the initial presentation. These longer more meaningful calls represented 1.81% of the entire 80,000 call sample.

It is understandable that the FCC would be concerned with the sheer volume of calls and reacted accordingly in imposing a proposed forfeiture amount on the full sample of 80,000 calls. However, in a future *de novo* proceeding, the proper forfeiture amount is a question for the factfinder. See *Unipoint Technologies, Inc.*, 159 F. Supp.3d at 273. In this case, the fact finder could determine that basing the proposed forfeiture amount on calls that were not received or otherwise ignored by consumers is not reasonable and results in a proposed forfeiture amount that is just too high. A more reasonable approach would be to determine the amount of consumers that were more likely to have been subjected to the marketing efforts of the Respondents and the travel companies.

This approach would have also been more representative of the actual harm caused by the acts allegedly committed by the Respondents. The FCC investigation revealed that only 66 robocall complaints made in late 2016 could be matched to the 96,000,000 calls allegedly made by Mr. Abramovich during the three month period of call records obtained by the Commission.⁹ Respondents are mindful that responsibility is based on the call but the actual harm to consumers is also an important factor. However, as set forth above, the volume of calls does not correspond to the number of consumers actually being affected by such calls. It is telling that the Commission has not identified a single consumer complaining about the actual vacation

⁷ Undersigned was provided with an Excel-formatted file containing the records of the 80,000 calls at issue for use in creating the enclosed exhibit.

⁸ Calls identified by the carrier with a duration of 30-seconds were by far the most common, comprising 43,942 calls representing 54.92% of the entire sample.

⁹ FCC Abramovich Citation at page 6.

July 27, 2017
 FCC File No. EB-TCD-15-00020488
 Page 5 of 8

packages offered by the travel companies or the fulfilment of such travel arrangements. In combination, the FCC overemphasized the volume of calls in determining the gravity of the violation for purposes of setting the proposed forfeiture amount and failed to address the amount of meaningful calls actually affecting consumers. The gravity of the violation is materially minimized through the suggested approach and a reduction in the proposed forfeiture amount is warranted.

Degree of Culpability/Participation

The Citation and NAL make explicitly clear that Mr. Abramovich is but one piece of a complicated puzzle involving the marketing of vacation packages. The Respondents played a specific role, namely conducting the lead generation activities. The complete telemarketing enterprise also involved the sales of the vacation packages by live operators under the direction of third-party travel companies. Also comprising an important piece, is the carrier utilized by Mr. Abramovich. The FCC's allegations clearly establish that Mr. Abramovich's participation was limited to the making of the offending phone calls. The allegations are equally clear that Mr. Abramovich was merely providing services to the third-party travel companies. Finally, the Call Records Detail obtained from the carrier, reveal that the carrier must have had knowledge of the improper caller ID information provided to the consumers receiving calls, and facilitated the operations by allowing the calls to continue. The Citation and NAL recognize Mr. Abramovich's specific role but nevertheless proceed to impose on him and his companies culpability for the entire process. The FCC did not properly segregate the actions of Mr. Abramovich from those of the other participants and therefore a reduction in the proposed forfeiture amount is warranted.

History Prior Offenses

The Commission has also improperly attributed to Mr. Abramovich a prior offense for purposes of an upward adjustment of the proposed base forfeiture amount; increasing the proposed forfeiture amount from \$80 million to \$120 million. First and foremost, the civil case cited in footnote 60 of the NAL did not involve the Commission, did not involve the spoofing activities present in this case, and occurred over a decade ago. The reference to this prior civil case is misplaced and should not be utilized as an aggravating factor.

Mr. Abramovich Does Not Have the Ability to Pay Proposed Forfeiture Amount

The FCC by its own admission seeks to impose on Mr. Abramovich and his companies the largest fine ever sought by the Commission. This record setting penalty was decided upon by the Commission without any consideration of Mr. Abramovich's ability to pay the proposed forfeiture amount. Without any question, only the largest of corporate entities would have the ability to pay the proposed forfeiture amount. Mr. Abramovich's activities do not generate the revenues necessary to pay but a fraction of one percent of the proposed forfeiture amount. Contrary to the implied assumption that the lead generating activities generate a per-call revenue, such is not the case. As set forth above, the lead generation calls result in leads that have

July 27, 2017
 FCC File No. EB-TCD-15-00020488
 Page 6 of 8

substantial contact with the client travel companies in less than 2% of all calls made. Accordingly, Mr. Abramovich's compensation from the third-party travel companies does not correlate with the number of calls made.

In seeking the Commission to reduce the proposed forfeiture amount, Mr. Abramovich

Respondents are cognizant of the Commission's precedent that requires consideration of factors beyond a company's financial position.¹¹ In this case, Mr. Abramovich has ceased all telemarketing or lead generation activities, in other words he is no longer conducting the revenue generating activities that resulted in the issuance Citation and NAL, thereby further hindering his ability to pay the proposed forfeiture amount.¹² In this regard, and in an effort to further warrant a reduction in the proposed forfeiture amount, Mr. Abramovich would be willing to stipulate to a permanent bar to any and all telemarketing activities and provide assistance to the Commission in any related enforcement action.

Unconstitutionality of Proposed Forfeiture Amount

The forfeiture amount sought by the FCC violates the due process protections afforded by the U.S. constitution because it is grossly disproportional to the gravity of the alleged actions taken by Mr. Abramovich. In the oft cited case of *St. Louis, I.M. & S. Ry. Co. v. Williams*, 251 U.S. 63, 66-67 (1919) the Supreme Court held that a statutory damages award violates due process "where the penalty prescribed is so severe and oppressive as to be wholly disproportioned to the offense and obviously unreasonable." The Court held that due process "places a limitation upon the power of the states to prescribe penalties for violations of their laws." *Id.* at 66.

In this matter, the Commission for the first time is considering how to calculate a proposed forfeiture amount for spoofing under the Truth in Caller ID Act ("TCID").¹³ Although the Commission may not have calculated or imposed forfeiture penalties under the TCID before, the Federal Trade Commission (hereinafter referred to as "FTC") has imposed civil penalties against telemarketing activities almost identical to the allegations presented against

¹⁰ Accompanying this written statement is a specific Request for non-disclosure pursuant to 47 CFR § 0.459.

¹¹ *In the Matter of Advantage Telecommunications Corp.* (FCC File No.: EB-TCD-12-00004803).

¹² See Affidavit of Adrian Abramovich at ¶ 7.

¹³ NAL at ¶ 23.

July 27, 2017
 FCC File No. EB-TCD-15-00020488
 Page 7 of 8

Respondents.¹⁴ The proposed forfeiture in this case is far in excess of the previous government imposed civil penalties that involved spoofing activities similar to those presented here. The proposed forfeiture amount at issue can only be described as disproportionate to the offense and unreasonable when comparing past FTC civil penalties for similar activities.

For example, in the case of *Federal Trade Commission v. Caribbean Cruise Line, Inc., et al.*, Case No. 15-cv-60423 (S.D. Fla.), the FTC was faced with a telemarketing campaign that “bombarded consumers with an average of 12-15 million calls per day”.¹⁵ The telemarketing campaign in the *Caribbean* case involved spoofed robocalls masquerading as political surveys for the purpose of offering so called “free” cruise vacations.¹⁶ In almost all respects the activities involved in the *Caribbean* case are even more egregious than those alleged against the Respondents. One notable difference is that in *Caribbean* all the participants involved in the telemarketing campaign were included in the enforcement action. In the *Caribbean* case the FTC stipulated to civil penalties against certain defendants as follows: Caribbean Cruise Line (Travel Provider) in the amount of \$7,730,000 suspended upon the payment of \$500,000; LSS Defendants (Lead Generators) in the amount of \$5,000,000 suspended upon the payment of \$25,000; and Pacific Telecom (Carrier) in the amount of \$1,354,000 suspended upon the payment of \$2,500.¹⁷

The case of *U.S. v. Sonkei Communications, Inc., et al.*, Case No. SACV-11-1777 (C.D. CA) involved a lead generation business similar to that alleged against the Respondents. The telemarketing campaign conducted by the *Sonkei* defendants consisted of prerecorded robocalls that manipulated caller identification similar to the alleged spoofing here. While the alleged facts and activities are similar to those of the Respondents, the civil penalty imposed by the FTC was for \$395,000, a tiny fraction of the proposed forfeiture amount sought against the Respondents in this matter.¹⁸ A final example of a similar telemarketing enforcement action is found in the case of *U.S. v. Cox*, Case No. SACV-11-1910 (C.D. CA). Another telemarketing campaign almost identical to that alleged against the Respondents, including the transmission of false and misleading caller identification information. The civil penalty entered against the individual defendant, namely Mr. Cox, was \$1,125,741 which was also suspended pending future compliance.

Respondents had no knowledge or warning prior to the imposition of the massive proposed forfeiture amount. This is especially problematic because as addressed above the FTC has imposed penalties on similar spoofing activities that while significant, were a small

¹⁴ Both the FCC and FTC have been involved in the regulation of telemarketers and telemarketing in general. See *Mainstream Marketing Services, Inc. v. FTC.*, 358 F.3d 1228 (10th Cir. 2004).

¹⁵ See ¶ 12 Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief (D.E. 1; 3/3/2015). The call volume in the *Caribbean* was more than 10 times the call volume alleged against Mr. Abramovich.

¹⁶ *Id.* at ¶ 13-16.

¹⁷ *Federal Trade Commission v. Caribbean Cruise Line, Inc., et al.*, Case No. 15-cv-60423 (S.D. Fla.), see Stipulated Orders for Permanent Injunction and Civil Penalty (D.E. 6-1; 6-4; & 90-1). The remaining defendants stipulated to civil penalties less than one million dollars, also suspended upon the making of minimal actual payment.

¹⁸ *U.S. v. Sonkei Communications, Inc., et al.*, Case No. SACV-11-1777 (C.D. CA)(D.E. 63).

July 27, 2017
FCC File No. EB-TCO-15-00020488
Page 8 of 8

percentage of the proposed forfeiture in this matter. Moreover, the proposed forfeiture amount here was calculated on a per call basis regardless of whether the call was answered much less whether the call had any impact on consumers. Because the proposed forfeiture is so disproportionate to the actual harm to consumers and so far in excess of previous governmental statutory penalties for similar activity, a significant reduction is required.

Conclusion and Request to Engage in Continuing Negotiations

There can be no dispute that the allegations against the Respondents if proven would result in civil penalties. The primary purpose of this written statement is to seek a significant reduction based on the arguments presented herein. The most compelling of arguments is the absolute inability for Mr. Abramovich to make payment of the proposed forfeiture amount. A reduction is appropriate to an amount proportionate to the gross revenues disclosed by the Respondents' federal tax returns. Moreover, Mr. Abramovich would anticipate that any consent judgment with an agreed amount would impose a ban on future telemarketing activities making it all the more difficult to make payment of the proposed forfeiture amount. Respondents would welcome engagement with the Commission staff in an effort to arrive at a consent judgment resolving this matter.

Sincerely,



Rodolfo Nuñez

Enclosures

cc: Via Email Only
Kristi Thompson, Deputy Division Chief
Telecommunications Consumers Division
Kristi.Thompson@fcc.gov

Amount of calls	Duration	%
2730	6 sec	3.4125
16136	12 sec	20.16
6277	18 sec	7.846
4660	24 sec	5.825
43942	30 sec	54.92
2123	36 sec	2.65
492	42 sec	0.615
257	48 sec	0.3125
197	54 sec	0.2462
1738	1 min to 5 min	2.1725
641	5.1 to 10 mins	0.8012
498	10.1 to 20 mins	0.6224
96	20.1 to 30 mins	0.12
59	30.1 to 40 mins	0.07375
37	40.1 to 49.3 mins	0.04625
39	50 to 60 mins	0.04874
57	60.5 mins to 100 mins	0.07125
21	101 mns to 151 mins	0.02625

80,000

TOTAL CALLS

The CHAIRMAN. Thank you, Mr. Abramovich.

Mr. ABRAMOVICH. Thank you.

The CHAIRMAN. In your prepared testimony, you say that you have been engaged in business with long distance telephone providers, wireless service providers, and conducting marketing activities for more than 15 years.

Mr. ABRAMOVICH. Yes, sir.

The CHAIRMAN. How many robocalls would you estimate to have made during that time?

Mr. ABRAMOVICH. I'm not going to answer that specific question for my activities, and I invoke the privilege not to answer, no.

The CHAIRMAN. In your prepared testimony, you state that the effect on consumers has been overstated in your case because fewer than 2 percent of consumers had a meaningful interaction with these calls, and 2 percent perhaps sounds small, but if the allega-

tions against you are correct, that means you made nearly 100 million robocalls during one 3-month period.

Mr. ABRAMOVICH. Mm-hmm.

The CHAIRMAN. So 2 percent would be nearly 2 million people. Over a year, that would be nearly 8 million people.

Mr. ABRAMOVICH. Mm-hmm.

The CHAIRMAN. Does that sound like a small effect on consumers?

Mr. ABRAMOVICH. Again, I'm not here to talk about my specific case. I invoke my privilege not to testify about things that might be used against me in the forfeiture case. But I can talk about general questions you might have about robocallings, telemarketing activities, and maybe can give you some insight on how those work.

I'm not prepared to discuss my specific case because I am subject to a \$120 million forfeiture against me right now. So I cannot talk about my specific case. But I'm here on a good faith effort to help the Committee to somehow come at these robocalls.

The CHAIRMAN. Mr. Abramovich, based on the information that you provided in your opening statement, I believe you may have waived your Fifth Amendment privilege.

Mr. ABRAMOVICH. Hmm?

The CHAIRMAN. In fact, during your opening statement, you just spoke in detail about the core issues under consideration at this hearing. You cannot now claim privilege to avoid answering questions on the subject matter contained in that statement. You are also here under subpoena, and, therefore, must answer. So if you refuse to answer this question, the Committee may seek to hold you in contempt of Congress for failing to respond.

Mr. ABRAMOVICH. Yes, but—

[Mr. Abramovich speaking with his counsel.]

Mr. ABRAMOVICH.—under advice of my Counsel, I'm not going to answer specific questions.

The CHAIRMAN. All right. I'm going to try one more time, and then I'm going to flip it to Senator Blumenthal.

Mr. Abramovich, the FCC alleges that your calls falsely claim to be affiliated with well-known travel and hospitality companies, including TripAdvisor, Expedia, Marriott, and Hilton.

Mr. ABRAMOVICH. Mm-hmm.

The CHAIRMAN. However, in your prepared testimony, you state that the resorts associated with your telemarketing activities were indeed real resorts.

Mr. ABRAMOVICH. Mm-hmm.

The CHAIRMAN. Which resorts did you work with? Did TripAdvisor, Expedia, Marriott, or Hilton ever authorize you to use their names during these calls?

Mr. ABRAMOVICH. I never misrepresented any of those hospitality companies. All the resorts are legitimate. Everything was included in the vacations. There was no fraudulent activity. The customers knew what packages they were purchasing. It's not a good business practice call customers saying that this is a promotion from Marriott, and then one of the agents might come back and say, "No, this is not Marriott, this is another resort in Mexico," and this type of business is not going to work. This is going to be flooded by chargebacks by misrepresentation. So it's not going to work.

They are—on the web pages, everything is clearly stated. They know what they're purchasing. They're getting discount vacations because they're going to have a 90-minute timeshare presentation. I mean, there is not a single complaint of customers saying that they did not receive what they paid for.

The CHAIRMAN. The FCC alleges that you received payment for your work, and your response to the FCC's charges, which you submitted as an appendix to your testimony, you state that lead-generating activities do not generate per-call revenue. So how are you compensated?

Mr. ABRAMOVICH. This is a misunderstanding. Some companies might offer a per-call service, which is very different. Those companies usually use what they call the avatar service where it's a voice recognition system, there is no robocalling involved. And they, in fact, indeed get paid maybe a dollar or two dollar per minute because they are somehow profiling the client before they get transferred to a call center.

In my case, I cannot answer the question because it's specific to my activities.

The CHAIRMAN. Do you know how many of those consumers actually received the vacations that were pitched to them?

Mr. ABRAMOVICH. How many?

The CHAIRMAN. Yes.

Mr. ABRAMOVICH. Excuse me?

The CHAIRMAN. How many of the consumers that got calls where they had vacations pitched to them, how many of them actually received or took those vacations?

Mr. ABRAMOVICH. They all received the vacation. Let me explain how it works. Once they are explained to about the vacations and the hotels where they're going to stay, it's all-inclusive, and the customer must submit a copy of their credit cards. He has a voucher signed by the client accepting the terms and conditions. If that document is not faxed back to the resort or the company, they will eventually refund the money to the client.

They must have a signature from the client accepting all the terms and conditions for these packages. We cannot control all the agents. In some cases, if the client is not happy with the vacation or the services, they might call their credit card company and get their money back. I mean, they are protected. There is no fraud in this case.

The CHAIRMAN. Mr. Abramovich, can you explain what neighborhood spoofing is?

Mr. ABRAMOVICH. Yes. Neighborhood spoofing is when you are making a phone call and make it look like it's coming from your local area.

The CHAIRMAN. Do you engage in that practice?

Mr. ABRAMOVICH. Again, I'm not going to answer questions specific to my activities. Remember, I have a pending FCC investigation forfeiture amount for \$100 million. I might be facing criminal fines.

The CHAIRMAN. Thank you.

Mr. ABRAMOVICH. I can give you some explanation, like I said, general questions that you might have.

The CHAIRMAN. Just one final question. In your written testimony, you state that regulation may help with respect to hosted autodialer services and companies that provide long distance carrier service. Can you comment on whether you think that—

Mr. ABRAMOVICH. Yes. I was watching a lot of hearings on the C-SPAN channel lately, and I think that they come with this idea that they do not originate on the technological side. But I think that the most important factor on these robocalls are the voice over IP carriers that are advertising the short duration call. When they advertise short duration call, that means they're going to accept all the calls you can throw at them. It doesn't matter what caller ID you use, they never ask.

It's going to be profitable for the long distance. For example, if you call AT&T directly, they're not going to accept that type of traffic because that type of company does not deal with those type of calls. But if you call a small voice over IP carrier, they're going to somehow blend the dialer traffic with the conversational calls and make it look like everything is normal. So that way they are fueling the robocalls.

And I think a good idea would be to focus on those five or six companies that are actually offering services. And they actually clearly state on the page, We accept short duration call for robocalling. Start your company today. Prepayment accepted. You can use any caller ID you want. And you can customize the software too, spoofing is very easy. You can do that within a day. It's very simple. So if those carriers allow all those calls to go through, the major networks won't see that the calls are coming from a robocaller.

The CHAIRMAN. Yes.

Senator Blumenthal.

Senator BLUMENTHAL. Thanks, Mr. Chairman.

Mr. Abramovich, you say in your statement, quote, I have denied and continue to deny any intent to defraud, cause harm, or wrongfully obtain anything of value, end quote. That statement relates to the activities involved in the FCC action, does it not?

Mr. ABRAMOVICH. Yes. I have submitted my response to the FCC as well as the Committee. And I have nothing additional—

Senator BLUMENTHAL. Do you understand, Mr. Abramovich, that that statement, in effect, is a response that waives a Fifth Amendment privilege as to questions pertaining to those activities?

Mr. ABRAMOVICH. May I consult with my lawyer for a second?

[Mr. Abramovich speaking with his counsel.]

Mr. ABRAMOVICH. I'm not a lawyer, and I cannot answer that question.

Senator BLUMENTHAL. You cannot selectively invoke a Fifth Amendment privilege. You can't decide to answer some questions and then decide you don't want to answer other questions about the same activities involving the same legal culpability. Do you understand that fact?

[Mr. Abramovich speaking with his counsel.]

Mr. ABRAMOVICH. Same answer. I'm not an attorney and—

Senator BLUMENTHAL. Let me try a couple of specific questions then, Mr. Abramovich. The robocalls involved in your activities involved misleading or inaccurate information, caller ID information,

designed to make the calls seem like they appeared from one location when in fact they came from another, correct?

Mr. ABRAMOVICH. Well, most robocallers use that technology because there's not a legal way to make a solicited phone call.

Senator BLUMENTHAL. Doesn't that mislead the recipient of the call as to location?

[Mr. Abramovich speaking with his counsel.]

Mr. ABRAMOVICH. I cannot speak to that and I'm not going to answer that question.

Senator BLUMENTHAL. You're invoking the Fifth Amendment?

Mr. ABRAMOVICH. I'm invoking the Fifth Amendment, yes. I can't answer that—

Senator BLUMENTHAL. Mr. Abramovich, the FCC has also alleged that these calls were harmful to carriers.

Mr. ABRAMOVICH. To carriers?

Senator BLUMENTHAL. Because they burdened or overwhelmed networks, and they alienated customers of those carriers. Do you deny it?

Mr. ABRAMOVICH. In general terms, I can talk about that. They are actually small carriers?

Senator BLUMENTHAL. No. I'm asking about your specific activities.

Mr. ABRAMOVICH. But I cannot talk about my specific activity.

Senator BLUMENTHAL. But you've denied that there is any harm to anyone from your activities, correct?

Mr. ABRAMOVICH. Um, I'm not denying there is no harm. What I'm saying is that—Senator, you're asking about the carriers, right? The carriers and the flood of the calls? I don't think there is any harm to the carriers. They are actually offering short duration calls. They know they are going to receive a massive amount of calls, and then they're going to profit from those calls.

Senator BLUMENTHAL. So you're not invoking the Fifth Amendment privilege as to that question.

Mr. ABRAMOVICH. Because it's in general terms.

Senator BLUMENTHAL. No, I'm asking about your activities. Did they cause harm to carriers?

Mr. ABRAMOVICH. I cannot answer to that question.

Senator BLUMENTHAL. And I'm asking about your activities. Isn't it a fact they caused harm to consumers?

Mr. ABRAMOVICH. I plead the Fifth Amendment. I cannot answer to that question. Like I said earlier, I have a pending investigation with the FCC, and all I say will probably hurt me.

Senator BLUMENTHAL. Let me ask you, What are the companies that you used to undertake your robocalling operations?

Mr. ABRAMOVICH. Again, I invoke my Fifth Amendment.

Senator BLUMENTHAL. Would you agree with me, Mr. Abramovich, that some of the consumers who were called and solicited for resort activities were unqualified?

Mr. ABRAMOVICH. In the timeshare industry, they are usually looking for young people between the years of 30, 45 years old, people that can actually buy a timeshare. There is no obligation whatsoever.

Senator BLUMENTHAL. In your activities, isn't it a fact that some of the consumers who were called were unqualified for those solicitations by their economic and income measures?

Mr. ABRAMOVICH. But I cannot talk about my activities, Senator. I'm sorry.

Senator BLUMENTHAL. Let me just finally ask you a question about the impact of people who receive robocalls. I have heard from many of my constituents, like many members of this panel, about the intrusive and invasive effect of these calls. One was Catherine Larson of Sandy Hook, Connecticut. She was getting an average of 7 to 10 robocalls a day, and she had to take them because her son was deployed abroad in the military. In fact, he was in a war zone. She had to change her number, her phone rang so often. The effect of these calls was pernicious and intrusive. Can you say these robocalls harm no one?

Mr. ABRAMOVICH. Um—

Senator BLUMENTHAL. That's what you say in your testimony.

Mr. ABRAMOVICH. Yes. From a general point of view, not from my case, from a general point of view, I think bad guys like Rachel or the IRS or the alarm companies, they are defrauding customers. I think it might be harmful for consumers. But I think there should be somehow a law where the good guys offering solicitation over the phone should be able to make some calls offering legitimate services or products where, for example, the government might have some control over them, say, "OK," for example, and just an idea, and I'm talking off the top of my head. Okay, you're going to have this car or this, this is what you're going to offer, this is the message that you're going to play, right? And the government or the FTC can have control at least of the good guys.

I mean, because this is the thing, when there's a robocall, automatically they are criminals. They don't leave a message, they're criminals, it's a scam. There are scams, but not all are scams, some are legitimate people trying to sell something.

Senator BLUMENTHAL. Well, it strikes me, Mr. Abramovich, that without prejudging the result in your case, that a high percentage of the calls were not only intrusive, but potentially scams, and that's why the FCC has levied a fine that is virtually unprecedented in its history, and that's why you're here today. And although you say you are not the king pin, certainly you're not the only one, but you are the face of this problem today, and I am going to ask the Chairman to consider a contempt proceeding because of your selective invocation of the Fifth Amendment. And I thank you for being here today.

The CHAIRMAN. Thank you, Senator Blumenthal.

Senator Markey evidently has a couple questions that he would like to ask as well.

**STATEMENT OF HON. EDWARD MARKEY,
U.S. SENATOR FROM MASSACHUSETTS**

Senator MARKEY. Thank you, Mr. Chairman, very much.

Mr. Abramovich, you represent nearly 100 million reasons why we need robust protections from the epidemic of robocalls and robotexts afflicting the Nation. You and the companies you control are alleged to have made almost 100 million spoofed robocalls

where you configured the calls in such a manner that the caller ID suggested that the calls were local calls.

Mr. ABRAMOVICH. Mm-hmm.

Senator MARKEY. And that's what the Telephone Consumer Protection Act of 1991 is designed to stop. I am the author of that law, which you are charged with violating. And I support the actions which the Federal Communications Commission has taken to enforce my law. The efficiency and the magnitude of your robocall campaign is truly historic. And you were able to become the king pin of robocalls because these technologies are so readily available and easily usable.

In your testimony, you stated that many of the calls you orchestrated were only for a short duration, but that misses the point, Mr. Abramovich. The interruption to consumers comes the moment the phone starts to ring, whether it's during dinner or it's at a time when you're on the go. That's what the problem is. It might only last a minute, but it's a minute that is completely disturbing to the receiver of the call. Do you agree with that, Mr. Abramovich?

Mr. ABRAMOVICH. In a general context, I agree to that. I'm not talking about specifics on my case, but I have been receiving four or five robocalls a day from my local number lately, and more after the FCC headlines, I'm receiving more spoofed calls than ever, myself.

Senator MARKEY. And you don't like it when you get those calls.

Mr. ABRAMOVICH. I just decline the call. I never answer the phone.

Senator MARKEY. But do you understand why it irritates people? Do you understand why they don't want these unwanted calls, Mr. Abramovich?

Mr. ABRAMOVICH. Yes, I understand.

Senator MARKEY. Well, that's what this is all about. That's what the intent of the law is meant to achieve, it's to protect people at home, to protect people in their own privacy from having unwanted calls come in. And your understanding of that is obviously key, and your business model was obviously meant to circumvent that sense of protection which people want.

So how easy would it be, Mr. Abramovich, for me to go back to my office, download automated phone call technologies and begin calling thousands of consumers with spoofed numbers? How hard would that be?

Mr. ABRAMOVICH. How easy?

Senator MARKEY. Or how easy?

Mr. ABRAMOVICH. Right now, I understand that you, Senator, asked how easy it was. You can find several options on the Internet. For example, you have software that is open source, it's totally customizable to your needs. All you do is Google, and try for example, "voice over IP provider, short duration calls," and it will pop up probably five, six, seven, and most of them are U.S.-based.

Senator MARKEY. How many people would I have to employ if I wanted to make, say, 10,000 robocalls a day?

Mr. ABRAMOVICH. Uh, on the systems side?

Senator MARKEY. Yes.

Mr. ABRAMOVICH. I would say from the general knowledge that I have, I would say one.

Senator MARKEY. One person.

Mr. ABRAMOVICH. One, and probably some technical support.

Senator MARKEY. And how would consumers stop these calls absent an enforcement action by the Federal Communications Commission?

Mr. ABRAMOVICH. Uh—

Senator MARKEY. Can they say, “Stop”?

Mr. ABRAMOVICH. No. I heard some on the hearings that they said that they tried to stop the voice over IP providers, and they said it was tough because I guess there are so many. But at the end of the day, the people who made those calls need the voice over IP, which is not AT&T, Verizon, they are the smallest ones. They’re actually looking for that type of business because it’s lucrative. They can make easily \$1 or \$2 million a year just by charging the robocaller for those calls. People say it’s a penny of the dollar. Yes, but in such amounts, generally speaking, it’s a lot of money for the carriers, and they just look the other way because it’s profitable for them.

Senator MARKEY. So you can make a lot of money compromising the privacy of families all across America. And, you know, that was the intent of the law that I authored, and that’s what the Federal Communications Commission is now enforcing. But here’s what I would say, because I led a letter with 14 of my Senate colleagues today calling on Chairman Pai at the FCC to adopt key protections: one, a comprehensive definition of “autodialer,” ensuring all callers must receive permission before robocalling or robotexting a consumer, and preserving consumers’ right to revoke consent should they no longer wish to receive calls or texts. I think that the Federal Communications Commission needs to take that action as soon as possible to stop the use of these technologies that harass consumers. Would those actions help to limit, Mr. Abramovich—

Mr. ABRAMOVICH. This is—

Senator MARKEY.—the ability of companies to be able to harass individuals?

Mr. ABRAMOVICH. There was a problem because a few years ago before they came back with the express consent, it’s the common knowledge that the robocalls has been increasing over the years right?

A few years ago, I remember that there were lead providers that would provide you with leads that people actually wanted to receive, they were associated with the business partners, and somehow some people could call them, and there was no need for other people to make millions and millions of calls. You could make thousands of calls with those leads without making millions. I think that it is increasing now because the express consent law was passed. They basically killed the lead list provider, they went out of business, there were no more leads. Now they go and start dialing randomly.

Senator MARKEY. Right.

Mr. ABRAMOVICH. This is true, most of the numbers are bad, they don’t even connect, it’s voice-mails, most of them go to voice-mails, and others are busy, others just simply don’t answer the phone. There’s no way that the legal telemarketing can offer any product anymore.

Senator MARKEY. Exactly. That's the point. People don't want to have the phone start ringing at 7 at night and go all night long. They have a right to not be called. They shouldn't have to hang up time after time night after night. It is not a business model that's consistent with how American families want to have their lives lived in the evening. And so that's why we need these laws, and that's why we need the FCC to tighten up these definitions even more.

I think you, Mr. Chairman.

The CHAIRMAN. All right. Thank you, Senator Markey.

Actually, we have a second panel to get to. We have votes at noon, so we have a hard stop there. I, frankly, personally, and I think other members of the panel would say, too, that we're disappointed in the failure to provide answers to a lot of what I think are good faith questions. But as I stated previously, it's my opinion that you may have waived your Fifth Amendment rights based on the information you provided in your opening statement. The Committee may seek to hold you in contempt of Congress for failing to respond, but because I do want to get to the——

**STATEMENT OF HON. JON TESTER,
U.S. SENATOR FROM MONTANA**

Senator TESTER. Mr. Chairman, can I just——

The CHAIRMAN. Yes.

Senator TESTER. Just give me 20 seconds. No question.

The CHAIRMAN. All right.

Senator TESTER. First of all, Mr. Abramovich, if you didn't want to draw attention to yourself, you should have sent back the request that the Chairman made and answered the questions. Then you potentially would not have been here today and you would not have the cameras focused on you.

Second of all, if you don't think 2 percent is a lot, that's twice the population that lives in Montana, 2 million people—that you hit.

Third of all, if I want to buy something, I'll call you, don't call me.

Thank you, Mr. Chairman.

The CHAIRMAN. All right. Senator Klobuchar.

**STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA**

Senator KLOBUCHAR. Yes. Also I want to join in with what Senator Tester just said, Mr. Abramovich. This whole business model is put up to make you money and then to violate the privacy of 229 million numbers which are now registered on the Do Not Call list, that's 229 million people. And what's been happening is that we've gotten increased complaints because people like you have found ways to get around it, and it's violating their privacy and it's often-times selling them stuff that they shouldn't be buying and that they're not initiating their own calls. And with the world changing, with texts and autotexts, and with the world changing with the scams, we are reintroducing and updating some of the legislation we have, and that's one thing that we can do.

But I am pleased that the Chairman had this hearing and that Senator Nelson did as well because I think that we also have to hold people accountable who have been skirting the law and getting around the law and potentially violating the law at others' expense.

The CHAIRMAN. Thank you.

Mr. Abramovich, we're going to dismiss you and ask our second panel to come forward at this time.

Mr. ABRAMOVICH. Can I say just one last thing?

The CHAIRMAN. Mm-hmm.

Mr. ABRAMOVICH. I think there's a lot of publicity around my case. Like I said before, the FCC enforced action to other people in the past that made 15, 20 million calls a day, and they are not here. I think the publicity is harming my case in some way. They made me the face of the robocalls and I think it's not the case. I mean, there are people that made 20, 30 million calls a day, and they just receive a fine from the FTC for \$7 million, and they settled for \$5-, \$400,000. And they are punishing me with a forfeiture fine of \$120 million.

The CHAIRMAN. We'll have a chance to ask them about that on the next panel. We have the FTC and the FCC both here.

Mr. ABRAMOVICH. I would like to hear. OK.

The CHAIRMAN. Thank you.

[Panel 2 coming forward.]

The CHAIRMAN. Welcome. We have Ms. Rosemary Harold, who is Chief of Enforcement Bureau at the FCC; Ms. Lois Greisman, who is the Associate Director, Marketing Practices Division, Bureau of Consumer Protection, at the FTC; Mr. Kevin Rupy, who is Vice President of Law and Policy at the USTelecom Association; Mr. Scott Delacourt, who is a Partner with Wiley Rein representing the U.S. Chamber of Commerce; and Ms. Margot Saunders, who is the Senior Counsel of the National Consumer Law Center.

So thank you all for being here. And in the interest of time, if you could move fairly quickly through your oral remarks and confine those, if possible, to 5 minutes, and then we'll make sure that your entire statements get included as a part of the written record.

So we'll start on my left, and your right.

Ms. Harold, thank you and welcome.

STATEMENT OF ROSEMARY HAROLD, CHIEF, ENFORCEMENT BUREAU, FEDERAL COMMUNICATIONS COMMISSION

Ms. HAROLD. Good morning, Chairman Thune and other members of the panel. I am happy to speak with you and answer questions about our enforcement activities at the FCC regarding illegal robocalls and spoofed calls.

As many people have already said, unwanted unlawful calls are not merely a serious irritation, they also can trick people out of significant amounts of money and often target vulnerable populations. Unwanted robocalls are our FCC's number one source of complaints.

The recent omnibus legislation will assist our enforcement efforts. It allows us to act against spoofed calls that originate outside of the United States as well as against spoofed text messages.

Thank you, Chairman Thune and other members of the Committee, for your leadership in the area.

The FCC uses several statutory provisions to take action against unlawful calls. The Consumer Protection Act of 1991, or TCPA, and accompanying FCC rules generally prohibit autodialed calls or prerecorded or artificial voice messages to emergency telephone lines, hospitals, and cell phones. The law also generally prohibits unsolicited, prerecorded advertising messages to residential telephones.

The Truth in Caller ID Act prohibits callers from falsifying or spoofing caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value. Consumers depend on caller ID information to help them decide whether to answer a phone call and whether to trust the caller on the other end of the line. Most large-scale unlawful robocall schemes today also employ spoofing.

We, at the FCC, have extensive ongoing enforcement efforts underway. Last year, we issued two notices of apparent liability and citations against two robocallers. In addition to Mr. Abramovich, Mr. Philip Roesel was a target of a different case. The evidence there showed that these individuals, along with their affiliated companies, made a total of more than 117 million apparently illegal spoofed calls. Because those cases remain ongoing, I cannot discuss the status of the case or much about them.

The FCC does work with the FTC on investigations and other actions. The agencies cooperate and share information pursuant to an MOU, a memorandum of understanding, and our roles are largely complementary, not duplicative. For example, the FCC has exclusive jurisdiction to enforce the anti-spoofing law.

The two agencies also co-host events to raise awareness. On April 23rd, we are co-hosting an industry expo where private companies will showcase innovative products that consumers can use to combat illegal robocalls themselves. In addition, the FCC has established relationships with industry to help us with our enforcement.

Telephone carriers have access to information and technical expertise that helps us to pinpoint the source of unlawful calls. Some of our most important efforts are ones you may never hear about. Together with the industry, we have been unable to shut down some unlawful robocall schemes early on.

Major telephone carriers and industry associations have banded together to share critical information about fraudulent activity. We also appreciate the significant effort of consumer protection groups to educate consumers.

With respect to rulemakings, the FCC, under Chairman Pai, is looking at ways to stop illegal robocalls before they even reach consumers. Last November, the FCC decided that voice service providers may block calls where spoofed caller IDs are invalid or unassigned or numbers that we know don't originate calls, such as in the recent IRS scams. Such calls are almost certainly illegal. In addition, the FCC right now is asking about other ways to identify and block illegal calls without also blocking legal ones.

The FCC is working closely with industry also to adopt the adoption of call authentication, a technological means by which tele-

phone calls can be securely “signed” by their senders to ensure that caller ID isn’t being spoofed.

The FCC has brought together experts and stakeholders in various ways to discuss the issues and try to solve at least parts of the problem, including the Robocall Strike Force, an ongoing inquiry proceeding, and most recently through a North American Numbering Council working group.

Moreover, we’ve moved to help responsible lawful callers avoid calling numbers that have been reassigned to a new consumer.

Last month, the FCC proposed a reassigned numbers data base that legit callers should check to avoid calling the wrong consumer.

Finally, as you know, the D.C. Circuit recently issued a decision regarding the Commission’s 2015 TCPA Omnibus Order. The Commission is actively reviewing that decision and determining what responsive actions would be appropriate. We are confident, however, that the court decision does not affect the enforcement actions that are ongoing against Mr. Abramovich or Philip Roesel because those actions were based on legal authority that the court did not address.

Thank you for your time. And I’m happy to take any questions you may have for me.

[The prepared statement of Ms. Harold follows:]

PREPARED STATEMENT OF ROSEMARY HAROLD, CHIEF, ENFORCEMENT BUREAU,
FEDERAL COMMUNICATIONS COMMISSION

Good morning Chairman Thune, Ranking Member Nelson, and Members of the Committee. My name is Rosemary Harold, and I am Chief of the Enforcement Bureau of the Federal Communications Commission. I am happy to speak with you and answer questions about the Commission’s enforcement actions and authority to combat illegal robocalls and spoofed calls.

Unwanted, unlawful calls are not merely a serious aggravation; many robocall and spoofing schemes are designed to trick people out of significant amounts of money. These schemes often are most effective in harming vulnerable populations, such as senior citizens. Unwanted robocalls are the Commission’s number one source of consumer complaints. The recent Omnibus legislation will provide significant assistance in our enforcement efforts. It allows us to take action against spoofed calls that originate outside the United States, and against spoofed text messages. Chairman Thune and Ranking Member Nelson, we are especially grateful for your leadership in this area.

FCC Regulatory Authority. The FCC uses several statutory provisions to take action against unlawful calls. The Telephone Consumer Protection Act of 1991, or TCPA, and accompanying Commission rules generally prohibit autodialed calls or prerecorded or artificial voice messages to emergency telephone lines, hospitals, and cell phones. The law also prohibits unsolicited, prerecorded advertising messages to residential telephone lines, except under limited circumstances. The Commission’s Do-Not-Call rules require telemarketers to honor consumers’ desires not to receive telemarketing calls.

The Truth in Caller ID Act prohibits callers from falsifying or “spoofing” caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value. Consumers depend on caller ID information to help them decide whether to answer a phone call and whether to trust the caller on the other end of the line. Unlawful spoofing can deceive recipients about the true identity of the caller and impede the ability of carriers and law enforcement to pinpoint the source of abusive calls. Most large-scale unlawful robocall schemes employ caller ID spoofing. In particular, many schemes utilize neighbor spoofing where the spoofed caller ID matches the area code and first three numbers of the phone number being called.

FCC’s Enforcement Work. The Commission has extensive ongoing enforcement efforts, although much of the work is conducted behind the scenes, long before a formal, public action. Last year, for example, the Commission issued notices of apparent liability (NALs) and citations against two massive robocallers and spoofers, Adrian Abramovich and Philip Roesel. The evidence in those investigations showed

that these two individuals, along with their affiliated companies, made more than 96 million and 21 million apparently illegal, spoofed robocalls, respectively. And the Commission has proposed forfeitures of \$120 million and \$82.1 million, respectively, in these cases. Because the details of these ongoing investigations are not public, I cannot provide further information about these cases at this time.

FCC/FTC Coordination: The FCC works with the Federal Trade Commission (FTC) throughout ongoing investigations and other actions. The agencies cooperate, share information, and render assistance pursuant to a Memorandum of Understanding. The FCC and FTC roles are largely complementary, and not duplicative. For example, the FCC has exclusive jurisdiction to enforce the Truth In Caller ID Act's provisions against spoofing. On March 23, we co-hosted with the FTC a Joint Policy Forum to learn what is being done to help consumers and the challenges that remain. On April 23, we are co-hosting with the FTC the "Stop Illegal Robocalls Expo," where 17 tech companies will showcase their innovative technologies, devices, and applications for consumers to combat illegal robocalls. In addition to FTC coordination, the Enforcement Bureau regularly coordinates with the CFPB, Department of the Treasury, Department of Justice, and Department of Homeland Security.

Industry Cooperation: We have also established relationships with industry to assist in enforcement. Telephone carriers have access to information and technical expertise that can help with early detection of potentially unlawful calls and pinpoint the source of the calls. Frankly, some of our most successful efforts are the ones you may never hear about: when we work with industry to identify and shut down unlawful robocall schemes early on. Major telephone carriers and their industry associations have banded together to share critical information about fraudulent call activity. We also appreciate the critical effort of consumer protection groups to inform and educate consumers.

Rulemakings. Stopping illegal robocalls before they even reach consumers can put a big dent in the problem, and under Chairman Pai's leadership, the Commission is looking at different ways to make that happen.

Last November, the Commission decided that voice service providers may block calls where spoofed Caller ID displays invalid or unassigned numbers, or numbers that we know don't originate calls, as in the recent IRS scam. Such calls are almost certainly illegal and can be blocked.

The Commission is also asking about other ways to identify and block illegal calls, without blocking lawful calls. For example, can call analytics reliably identify calling patterns that result from illegal calls—such as large bursts of calls over a short time from numbers that don't usually make calls that way?

The Commission is also working closely with industry to speed the adoption of call authentication—a means by which telephone calls can be securely "signed" by their senders, so that we know that the Caller ID isn't being spoofed. The Commission has worked to bring the relevant experts and stakeholders together, through the Robocall Strike Force; a Notice of Inquiry; and most recently through a North American Numbering Council working group.

We've also moved to help responsible, lawful callers avoid calling phone numbers that have been reassigned to a new consumer. Just last month, the Commission proposed a reassigned numbers database that callers could check to avoid calling the wrong consumer.

ACA International Decision. The DC Circuit recently issued a decision regarding the Commission's 2015 *TCPA Omnibus Order*. The Commission is reviewing that decision and determining what responsive actions might be appropriate. We are confident, however, that the court decision does not affect the enforcement actions against Adrian Abramovich or Philip Roesel or other investigations we are pursuing because those actions were based on legal authority outside the scope of the recent D.C. Circuit decision.

Thank you again for the opportunity to speak with you this morning. I welcome any questions you may have.

The CHAIRMAN. Thank you, Ms. Harold.
Ms. Greisman.

**STATEMENT OF LOIS GREISMAN, ASSOCIATE DIRECTOR,
MARKETING PRACTICES DIVISION, BUREAU OF CONSUMER
PROTECTION, FEDERAL TRADE COMMISSION**

Ms. GREISMAN. Good morning, Chairman Thune, Ranking Member Blumenthal, and members of the Committee. I'm honored to

have the opportunity this morning to discuss the FTC's work to fight illegal robocalls. As each of you has made clear, there is no shortage of adjectives to describe the detested robocalls that batter our phones and mobile devices. At best, these calls cause intense annoyance; at worse, fraudulent calls cause wrenching economic harm.

In 2017, the FTC received more than 7 million complaints about unwanted calls. Consistently, more than 60 percent of those complaints are about robocalls. In just the first 3 months of 2018, we've received 1.4 million complaints, with robocalls driving the numbers. Some 900,000 of the 1.4 million complaints are about robocalls. The complaint numbers are compelling and demand action. That's precisely what the FTC has been doing, deploying a three-pronged approach to tackle illegal robocalls; namely, law enforcement, the promotion of technological solutions, and, of course, robust consumer and business education.

First, law enforcement. I submit to you that the Commission has been relentless in its attacks against unwanted calls. Since 2014, when we started enforcing Do Not Call provisions, no less than 135 enforcement actions against 439 companies and 356 individuals have been filed. 125 of those cases have been resolved, and the Commission has collected \$121 million in monetary relief in civil penalties, and that amount does not include the historic \$280 million civil penalty judgment against Dish.

The recent cases alone have stopped literally billions of illegal robocalls, many of which use spoofed caller ID. We have targeted many pernicious king pins in the robocall ecosystem, many of whom are interconnected and providing dialing platform, lead generators, telemarketers, and sellers. Many of the people recently sued by the FTC have known and worked with one another for years. One was so bold as to use his own voice for the robocall recording. Another ensured that his dialer was programmed so as not to call anyone at the FTC.

These connections are highlighted in a recently filed case against Alliance and its founder, Joe Gotra, who are alleged to have bombarded consumers with illegal calls for home alarm systems. These calls so outraged consumers that some of them went so far as to schedule an appointment for installation so that they could tell the person to their face to stop calling them.

We will continue to coordinate our work with State enforcers, with Federal law enforcement, the FCC, the IRS, Postal Inspection Service, and Department of Justice.

Still, we know sustained law enforcement alone will not solve the problem. The second prong focuses on technological solutions. Toward that end, the FTC has hosted four robocall contests. In fact, two of the winners brought call-blocking products to the market, Nomorobo and RoboKiller. Moreover, the FTC has supported industry initiatives, such as the industry-led Robocall Strike Force, and has provided comment on the FCC's rulemaking efforts to expand voice service providers authorization to block unwanted calls. The recent joint FTC-FCC forum highlighted much of this work.

No silver bullet is in sight, but real progress is being made. Indeed, when the FTC announced its first robocall challenge in 2012, few, if any, call-blocking tools were in the marketplace. Today, hun-

dreds are available. The upcoming April 23 expo that Ms. Harold mentioned that we're jointly hosting will highlight these tools to the public.

The FTC has also implemented a strategy to facilitate technological solutions. Each business day, the agency releases about 22,000 phone numbers that consumers complain about. This data is used to improve the functionality of call-blocking solutions.

The third prong of the FTC's work is consumer and business education. Often with assistance from your offices, the FTC continues to push out a large quantity of—a large quantity of high quality educational messages to consumers and businesses. In connection with the recent forum, we released information on call-blocking tools, infographics on what's available for landlines and mobile devices, and how to choose the right one. We also work closely with sellers and telemarketers so they have clarity about what is legal and what is illegal.

In short, I'm very proud of the work the FTC has done to curb illegal robocalls, halting billions and spurring innovation. But I am keenly aware that we must steadfastly tackle this vexing consumer protection problem, and I commit to you that we will do just that.

Thank you very much.

[The prepared statement of Ms. Greisman follows:]

PREPARED STATEMENT OF LOIS GREISMAN, ASSOCIATE DIRECTOR, DIVISION OF MARKETING PRACTICES, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Chairman Thune, Ranking Member Nelson, 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.

In 2003, the FTC responded to enormous public frustration with unsolicited sales calls and amended the Telemarketing Sales Rule ("TSR") to create a national Do Not Call Registry.² The Registry, which includes more than 229 million active telephone numbers,³ has been tremendously successful in protecting consumers' privacy from unwanted calls by the thousands of legitimate telemarketers who subscribe to the Registry each year.⁴ Subsequently, 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.⁵ In 2008, the Commission responded by amending the TSR to prohibit the vast majority of prerecorded sales calls.⁶

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 Fiscal Year 2017 the FTC received more than 4.5 million robocall complaints.⁷ The FTC is using every tool at its disposal

¹ The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or any individual Commissioner.

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

³ See Do Not Call Registry Data Book 2017: Who is using the Do Not Call Registry available at <https://www.ftc.gov/policy/reports/policy-reports/commission-staff-reports/national-do-not-call-registry-data-book-fy-3>.

⁴ For example, in Fiscal Year 2017, more than 17,000 telemarketers accessed the Do Not Call Registry. See *id.*

⁵ See Section II(A), *infra*.

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

⁷ The FTC's Fiscal Year 2017 began October 1, 2016 and ended September 30, 2017. Total unwanted-call complaints for FY 2017 including both robocall complaints and complaints about live

to fight these illegal calls.⁸ 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.

I. LAW ENFORCEMENT

Since establishing the Do Not Call Registry in 2003,⁹ 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 135 enforcement actions seeking civil penalties,¹⁰ restitution for victims of telemarketing scams, and disgorgement of ill-gotten gains against 439 corporations and 356 individuals. From the 125 cases that have been resolved thus far, the Commission has collected over \$121 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.¹¹ The robocall provisions cover prerecorded calls to all consumers, including those who have not registered their phone number on the Do Not Call Registry. The Commission has been aggressive in enforcing prohibitions against robocalls, filing 45 cases against 163 companies and 121 individuals responsible for *billions of illegal robocalls*.¹² From the 42 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 recent robocall enforcement actions.

1. Recent Enforcement Activities

i. Alliance Security

Just a few weeks ago, the FTC filed a complaint and motion for preliminary injunction in Federal district court alleging that Alliance Security Inc. ("Alliance") and its founder, Jasjit "Jay" Gotra, directly and through its authorized telemarketers, called more than a million consumers whose numbers are on the Do Not Call Registry.¹³ Alliance installs home security systems, and makes outbound calls to solicit the sale of the systems and associated security monitoring services.

calls from consumers whose phone numbers are registered on the Do Not Call Registry, exceed 7million. Note, however, that the FTC identified a technical problem with complaint submissions that resulted in artificially high complaint counts in July and August. See Do Not Call Registry Data Book 2017: Complaint Figures for FY 2017 available at <https://www.ftc.gov/policy/reports/policy-reports/commission-staff-reports/national-do-not-call-registry-data-book-fy-1>.

⁸See FTC Robocall Initiatives, <https://www.consumer.ftc.gov/features/feature-0025-robocalls>.
⁹In 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>.

¹⁰As 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).

¹¹Like the other provisions of the TSR, the robocall provisions do not apply to non-sales calls, such as calls placed calls that are purely political, informational, or survey calls. Also, the provisions allow robocalls to members or prior donors of charities. 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).

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

¹³Alliance and Gotra are recidivist violators of the Telemarketing Sales Rule that were under a 2014 FTC order for prior illegal calling practices. See *U.S. v. Versatile Marketing Solutions, Inc.*, 1:14-cv-10612-PBS (D. Mass. Mar. 10, 2014) available at <https://www.ftc.gov/enforcement/>

Continued

The FTC's complaint alleges that since 2014, Alliance and Gotra made or helped others make at least two million calls to consumers that violate the TSR, including more than a million calls to numbers on the DNC Registry.¹⁴ Many of these calls began as illegal robocalls using "spoofed" Caller ID numbers and information.¹⁵ Defendants then transferred the calls to a live agent, but continued to hide the identity of the caller—even taking pains to prohibit agents from naming Alliance.¹⁶ In some cases, Alliance's agents deceptively held themselves out as a competitor, such as ADT, when calling consumers.¹⁷ Some consumers were so frustrated by the barrage of unwanted calls from Alliance that they scheduled an alarm installation just to plead in person for an end to the calls.¹⁸

The FTC's complaint alleges that Alliance's disregard for consumers' privacy went beyond the telephone and reached into their personal data.¹⁹ Alliance also performed undisclosed, unauthorized credit checks on consumers who received unsolicited telemarketing calls from Alliance or its telemarketers, in violation of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681 *et seq.*²⁰ Alliance typically ran a credit check on every consumer who "pressed 1" in response to a call placed by Alliance or one of its telemarketers and expressed interest in obtaining an alarm system—without informing the consumer.²¹

Two of Alliance's authorized telemarketers and their principals agreed to settle charges that they made illegal calls on Alliance's behalf.²² One telemarketer and its principal will be permanently barred from telemarketing and is subject to a civil penalty of \$2,296,500, that is suspended based on inability to pay.²³ The second telemarketer and its principal will be permanently banned from selling home security and medical alert devices, making robocalls or helping anyone else make them, using spoofed caller ID numbers, and calling phone numbers on the Do Not Call Registry, unless a consumer directly contacts the principal to request a call.²⁴ The second telemarketer is also subject to a civil penalty of \$3,293,512, which will be partially suspended due to their inability to pay, upon payment of \$300,000 to the Commission.²⁵ The FTC is seeking strong injunctive relief and civil penalties against the remaining defendants, Alliance and Gotra, in Federal district court.²⁶

ii. Higher Goals Marketing

In December 2017, the FTC filed an action in Federal district court against Higher Goals Marketing LLC to halt an alleged debt-relief scam that defrauded numerous consumers struggling with credit card debt.²⁷ The complaint alleges that the Higher Goals Marketing defendants used illegal robocalls to contact consumers, pitching their fake debt-relief services and charging hefty up-front fees, causing millions of dollars in injury.²⁸ Defendants guaranteed that consumers would substantially and permanently lower their credit card interest rates, and would save thou-

cases-proceedings/122-3162/versatile-marketing-solutions-inc-also-dba-vms-alarms-et-al. Based on this pattern of behavior, the FTC's most recent enforcement action seeks a preliminary and permanent injunction that bans Alliance and Gotra from telemarketing. *FTC v. Jasjit Gotra*, 1:18-cv-10548 (D. Mass. Mar. 23, 2018) available at <https://www.ftc.gov/enforcement/cases-proceedings/x140022/jasjit-gotra-alliance-security>.

¹⁴ *FTC v. Jasjit Gotra*, 1:18-cv-10548 (D. Mass. Mar. 23, 2018) available at <https://www.ftc.gov/enforcement/cases-proceedings/x140022/jasjit-gotra-alliance-security>.

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ To protect consumers' privacy and safeguard their financial information, the FCRA prohibits unauthorized access to credit reports and credit scores. Under the FCRA, 15 U.S.C. § 1681b(f), it is unlawful for any "person to use or obtain a consumer report for any purpose unless" that person has a specific permissible purpose enumerated in 15 U.S.C. § 1681b(a).

²¹ *FTC v. Jasjit Gotra*, 1:18-cv-10548 (D. Mass. Mar. 23, 2018) available at <https://www.ftc.gov/enforcement/cases-proceedings/x140022/jasjit-gotra-alliance-security>. Indeed, the complaint further alleges that defendants attempted to pull credit reports or scores on President Trump and former President Obama, and Vice President Pence and former Vice President Biden, among others.

²² *Id.*

²³ *Id.*

²⁴ *Id.*

²⁵ *Id.*

²⁶ *Id.*

²⁷ See *FTC v. Higher Goals Marketing LLC*, 6:17-cv-02048-GAP-KRS (M.D. Fla. Dec. 4, 2017) available at <https://www.ftc.gov/enforcement/cases-proceedings/172-3045/higher-goals-marketing-llc>.

²⁸ *Id.*

sands of dollars in interest payments.²⁹ In reality, the complaint alleges, the scheme was unable to deliver the promised results to most consumers.³⁰ Since the FTC filed this action, all defendants stipulated to a Preliminary Injunction, which the Court entered on December 28, 2017.³¹ Thanks to the filing of the FTC's enforcement action, the defendants' operation is shut down, and the Court has appointed a receiver to oversee the two corporate defendants.³²

iii. *Jones and Ramsey Cases*

Also in 2017, the Commission filed two lawsuits, *FTC v. Justin Ramsey* and *FTC v. Aaron Michael Jones*, that shut down operations responsible for *billions* of illegal robocalls. The *Ramsey* and *Jones* defendants bombarded consumers with robocalls pitching home security systems and extended auto warranties.³³ The FTC obtained a settlement order in the *Ramsey* action that bans Ramsey and his company from placing robocalls to individuals to sell goods or services, initiating sales calls to numbers listed on the DNC Registry, and selling data lists containing phone numbers listed on the Registry.³⁴ Ramsey and his company also agreed to a \$2.2 million civil penalty, suspended upon payment of \$65,000.³⁵ In the *Jones* action, the court entered final orders permanently banning Jones and his companies from all telemarketing activities, including initiating robocalls, calling numbers on the DNC Registry, and selling data lists containing consumers' phone numbers and other information.³⁶ The default judgment order against Jones also imposes a \$2.7 million civil penalty against him, payable to the Commission.³⁷

Over the past three years the FTC, often in conjunction with its law enforcement partners, initiated eleven 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.³⁸ Many of the defendants in these cases are now banned from robocalling or telemarketing.³⁹

²⁹ *Id.*

³⁰ *Id.* The Commission also alleges that several defendants previously worked for a nearly identical telemarketing operation shut down in 2016 by court order at the request of the FTC. These defendants set up a new operation selling similar bogus credit-card interest-rate-reduction services within weeks of the court order shuttering the earlier operation. *Id.*

³¹ *Id.*

³² *See id.*

³³ *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 Jones*, 8:17-cv-00058 (M.D. Fla. Jan. 13, 2017), available at <https://www.ftc.gov/enforcement/cases-proceedings/152-3152/alloreys-inc>. Evidence reviewed by FTC staff in connection with the *Ramsey* case indicated that a portion of the unlawful telemarketing calls targeted “distressed seniors.”

³⁴ *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>.

³⁵ *Id.*

³⁶ *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>.

³⁷ *Id.*

³⁸ *FTC v. Jasjit Gotra*, 1:18-cv-10548 (D. Mass. Mar. 23, 2018) available at <https://www.ftc.gov/enforcement/cases-proceedings/x140022/jasjit-gotra-alliance-security>; *FTC v. Higher Goals Marketing LLC*, 6:17-cv-02048-GAP-KRS (M.D. Fla. Dec. 4, 2017) available at <https://www.ftc.gov/enforcement/cases-proceedings/172-3045/higher-goals-marketing-llc>; *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 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-education-info-inc>; *FTC et al., 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 et al., 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>.

³⁹ *See, e.g., U.S. v. KFJ Marketing Inc.*, 2:16-cv-01643 (C.D. Cal. Nov. 7, 2017), available at <https://www.ftc.gov/enforcement/cases-proceedings/152-3166/kfj-marketing-llc> (final order permanently banning corporate defendants and individual ringleader from all telemarketing); *FTC*

iv. Historic Victory in Dish Network

In addition to initiating new enforcement actions, the FTC and our law enforcement partners also achieved an historic win in a long-running 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.⁴⁰ 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.⁴¹ The litigation centered on allegations that Dish and its telemarketers made tens of millions of calls—often robocalls⁴²—to telephone numbers on the Do Not Call Registry and called consumers who previously asked Dish and its telemarketers to stop calling.⁴³ 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.⁴⁴ 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.⁴⁵ 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. 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

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).

⁴⁰ 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>.

⁴¹ *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>.

⁴² 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 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.

⁴³ *U.S. v. Dish Network, LLC*, No. 3:09-cv-03073 (C.D. Ill. Mar. 25, 2009), available at <https://www.ftc.gov/enforcement/cases-proceedings/052-3167/dish-network-llc-united-states-america-federal-trade>.

⁴⁴ *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>.

⁴⁵ 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>.

of related individuals and entities to avoid detection by law enforcement. In addition, defendants in many of our 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.⁴⁶

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.⁴⁷ 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.⁴⁸

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. The Commission coordinates with various partners to bring law enforcement actions. Many of the recent robocall enforcement actions the FTC has led involved collaboration with the Department of Justice or our state partners.⁴⁹ The FTC also leads robocall law enforcement “sweeps”—coordinated, simultaneous law enforcement actions—in conjunction with state and Federal partners.⁵⁰

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. Also, on May 17, for the third year in a row, the FTC is coordinating a meeting among stakeholders specifically to tackle Indian call-center fraud.

⁴⁶ See *FTC v. Jasjit Gotra*, 1:18-cv-10548 (D. Mass. Mar. 23, 2018) available at <https://www.ftc.gov/enforcement/cases-proceedings/x140022/jasjit-gotra-alliance-security>; *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) or assisted others in doing the same.

⁴⁷ *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>.

⁴⁸ *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>.

⁴⁹ See *supra* n. 38.

⁵⁰ For example, the FTC led a multinational robocall sweep announced in June 2016 that took action against operations estimated to be responsible for billions of illegal robocalls.⁵⁰ 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. 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).

Just last month, the FTC and FCC co-hosted a Joint Policy Forum on Illegal Robocalls on March 23, 2018.⁵¹ The purpose of the forum was to discuss the regulatory and enforcement challenges posed by illegal robocalls and what the FCC and FTC are doing to protect consumers and encourage the development of private-sector solutions.⁵² Discussion topics included the factors driving the volume of illegal robocalls; Caller ID spoofing; new threats to consumers, such as “neighbor spoofing”; protections for callers placing legal calls; FCC rulemakings; enforcement challenges; third-party solutions and other resources available to empower consumers; and industry efforts to develop Caller ID authentication.⁵³ The forum included policy and regulatory experts from both agencies, enforcement leaders from both agencies and the Florida Office of Attorney General, representatives from voice service providers, representatives from companies providing call-blocking solutions, as well as representatives from the call originators.⁵⁴

II. POLICY AND MARKET STIMULATION INITIATIVES

A. Understanding the Landscape of the Robocall Problem

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.⁵⁵ That number has now more than quadrupled—in Fiscal Year 2017, the FTC received an average of nearly 400,000 robocall complaints per month.⁵⁶

Recognizing that law enforcement, while critical, is not enough to solve the problem, FTC staff has aggressively sought new strategies in ongoing discussions with academic experts, telecommunications carriers, industry coordinating bodies, technology and security companies, consumers, and counterparts at federal, state, and foreign government agencies. The Commission ramped up these efforts in October 2012, when the FTC hosted a public summit on robocalls to explore these issues (the “Robocall Summit”).⁵⁷ 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. Technological Developments Have Made Robocalls Extremely Inexpensive

Until relatively recently, telemarketing required significant capital investment in specialized hardware and labor.⁵⁸ Now, robocallers benefit from automated dialing technology, inexpensive international and long distance calling rates, and the ability to move internationally and employ cheap labor.⁵⁹ The only necessary equipment is a computer connected to the Internet.⁶⁰ The result: law-breaking telemarketers can place robocalls for a fraction of one cent 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 auto-

⁵¹See Press Release, FTC and FCC to Host Joint Policy Forum on Illegal Robocalls (Mar. 22, 2018) available at <https://www.ftc.gov/news-events/press-releases/2018/03/ftc-fcc-host-joint-policy-forum-illegal-robocalls>.

⁵²*Id.*

⁵³See Press Release, Agenda Announced for the March 23, 2018 FTC-FCC Joint Policy Forum on Fighting the Scourge of Illegal Robocalls (Mar. 19, 2018) available at <https://www.ftc.gov/news-events/press-releases/2018/03/ftc-fcc-host-joint-policy-forum-illegal-robocalls>.

⁵⁴*Id.* A video recording of the event is available on the FCC’s website at <https://www.fcc.gov/fcc-ftc-robocalls-forum>.

⁵⁵National 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.

⁵⁶See *supra* n. 8.

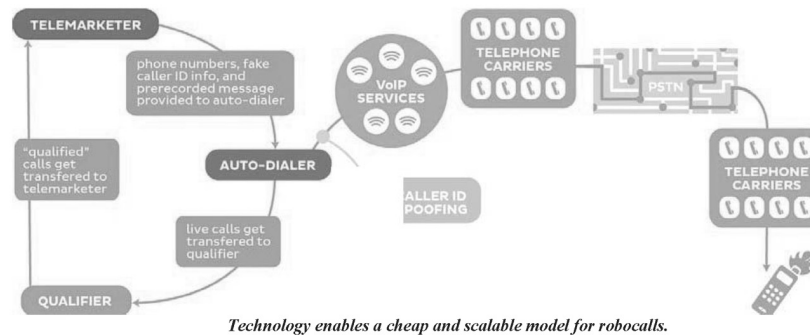
⁵⁷See generally FTC Workshop, *Robocalls: All the Rage* (Oct. 18, 2012), available at <https://www.ftc.gov/news-events/events-calendar/2012/10/robocalls-all-rage-ftc-summit>. A transcript of the workshop (hereinafter “Tr.”) is available at https://www.ftc.gov/sites/default/files/documents/public_events/robocalls-all-rage-ftc-summit/robocallsummittranscript.pdf.

⁵⁸Herrmann, Tr. at 58–59; Schulzrinne, Tr. at 24.

⁵⁹Schulzrinne, Tr. at 24.

⁶⁰Herrmann, Tr. at 59–61.

mated calls, gathering consumers' personal information, or selling products.⁶¹ Because of the dramatic decrease in upfront capital investment and marginal cost, robocallers—like e-mail spammers—can make a profit even if their contact rate is very low.⁶²



2. Technological Developments 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.⁶³ These circuitous paths make it cumbersome to trace a call to its inception.⁶⁴ All too often, this process to trace the call fails because one of the carriers in the chain has not retained the records necessary for a law enforcement investigation.⁶⁵

Second, callers can easily manipulate the Caller ID information that appears with an incoming phone call.⁶⁶ While “Caller ID spoofing” has some beneficial uses,⁶⁷ it also allows telemarketers to deceive consumers by pretending to be an entity with a local phone number or a trusted institution such as a bank or government agency.⁶⁸ In addition, telemarketers can change their phone numbers frequently in an attempt to avoid detection.⁶⁹ Today, many illegal callers rely on “neighbor spoofing”, the practice of using a Caller ID number that appears to be from a number local to the call recipient.⁷⁰

Finally, new technologies allow robocallers to operate outside of jurisdictions where they are most likely to face prosecution.⁷¹ Indeed, the entities involved in the path of a robocall can be located in different countries, making investigations even more challenging.

⁶¹ Schulzrinne, Tr. at 20–21; Maxson, Tr. at 95–98.

⁶² Schulzrinne, Tr. at 21; Bellovin, Tr. at 16–17.

⁶³ Panagia, Tr. at 130–32; Bellovin, Tr. at 17.

⁶⁴ Schulzrinne, Tr. at 24–25; Maxson, Tr. at 100; Bash, Tr. at 104. Recently, USTelecom’s Industry Traceback Group has been able to assist law enforcement to traceback a call more quickly through the network.

⁶⁵ Panagia, Tr. at 160–61; *see also id.* at 132–133; Schulzrinne, Tr. at 21.

⁶⁶ Schulzrinne, Tr. at 24–26.

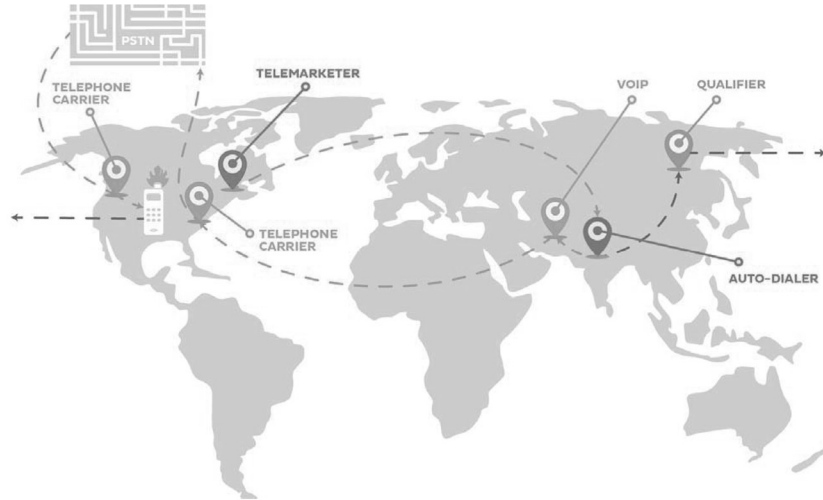
⁶⁷ *See, e.g.,* Panagia, Tr. at 129 (AT&T allows the third party that performs AT&T’s customer service to “spoof” AT&T’s customer service line).

⁶⁸ Schulzrinne, Tr. at 21–22.

⁶⁹ *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 Tele-marketing 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.).

⁷⁰ *See* FTC Consumer Information Blog, That’s Not Your Neighbor Calling <https://www.consumer.ftc.gov/blog/2018/01/thats-not-your-neighbor-calling>.

⁷¹ Schulzrinne, Tr. at 21; Bellovin, Tr. at 16–17.



The path of a robocall can span the entire globe.

B. Efforts to Stimulate Technological Solutions

1. Robocall Contests

Recognizing the need to spur the marketplace into developing technical solutions that protect American consumers from illegal robocalls, the FTC led four public challenges to help tackle the unlawful robocalls that plague consumers. In 2012–2013, the FTC conducted its first Robocall Challenge,⁷² 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. To date, “NomoRobo,” which reports blocking over 600 million calls, is being offered directly to consumers by a number of telecommunications providers and is now available as an app on iPhones.⁷³

The following year, the FTC launched its second challenge—Zapping Rachel⁷⁴—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, DetectaRobo,⁷⁵ 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.⁷⁶ Contestants built and submitted robocall solutions to the judges and finalists, then competed to “seed” their solutions and collect the highest number of robocalls. One of the winners of the Humanity

⁷² 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>.

⁷³ See <https://www.nomorobo.com/> (last visited April 4, 2018) 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.

⁷⁴ 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>.

⁷⁵ For more information on the DetectaRobo challenge see <https://www.ftc.gov/news-events/contests/detectarobo>.

⁷⁶ For more information on the Robocalls: Humanity Strikes Back challenge, see <https://www.ftc.gov/news-events/contests/robocalls-humanity-strikes-back>.

Strikes Back challenge developed Robokiller, a call-blocking app available for iOS phones.⁷⁷

Each of the four challenges provided the Commission with an opportunity to promote industry dialogue and innovation in combatting illegal robocalls, develop industry partnerships, 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.⁷⁸ 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.⁷⁹

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.⁸⁰ 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. The Strike Force expanded this effort and it contributed to a drop in IRS scam calls at the end of 2016.⁸¹

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.”⁸² In response, in March 2017, the FCC issued a Notice of Proposed Rule Making and Notice of Inquiry that sought to expand the categories of calls that voice service providers are authorized to block and invited comment on what types of standards should govern providers engaged in call blocking.⁸³ 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.⁸⁴ In November 2017, the FCC issued

⁷⁷ See <https://www.robokiller.com/> (last visited April 4, 2018).

⁷⁸ 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 April 4, 2018). 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/> (last visited April 4, 2018). 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 April 4, 2018).

⁷⁹ The Cellular Telecommunications Industry Association (CTIA) maintains a list of hundreds of available call blocking apps (including a list of the top 15 apps as determined by CTIA), 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 April 4, 2018).

⁸⁰ 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>.

⁸¹ See Robocall Strike Force, Robocall Strike Force Report at 32-33 (2016), <https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf>.

⁸² See *id.* at 40.

⁸³ 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).

⁸⁴ 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 In-

a Report and Order that enabled voice service providers to block certain categories of calls before they reach consumers' phones as proposed by the Notice of Proposed Rulemaking.⁸⁵

Increased call-blocking and call-labeling tools for consumers has presented new challenges for call originators, some of which contend that their calls are being erroneously blocked or labeled. The FTC participates in several forums that seek to improve the communication between call originators and service providers. The FCC also recently sought input on how best to address the question of potential errors in call blocking and call labeling.⁸⁶

In response, the FTC filed a comment encouraging providers of call-blocking services to consider engaging in practices that could reduce the potential for inadvertently blocking wanted calls, such as communicating clearly to subscribers the types of calls that are being blocked, using plain and specific terms to label calls, and providing designated points of contact to handle questions about calls blocked in error.⁸⁷

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 e-mail spam.⁸⁸ 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.⁸⁹

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.⁹⁰ 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.⁹¹

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.

Next, in Fiscal Year 2017, the FTC redesigned its annual National Do Not Call Registry Data Book.⁹² The Data Book now provides more information on robocall complaints, new information about the types of calls consumers reported to the FTC, and includes a complete state-by-state analysis.⁹³ In addition, this year the FTC has

quiry, 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 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.

⁸⁵ See Advanced Methods to Target and Eliminate Unlawful Robocalls, Report and Order and Further Notice of Proposed Rulemaking, CG Docket No. 17–59, FCC 17–151 (released Nov. 17, 2017).

⁸⁶ See *id.*

⁸⁷ See Comment of the FTC to the Federal Communications Commission, Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17–59, FCC 17–151 (Jan 23, 2018), available at <https://www.ftc.gov/policy/advocacy/advocacy-filings/2018/01/ftc-staff-comment-federal-communications-commission>.

⁸⁸ See M³AAWG, Activities, <https://www.m3aawg.org/> (last visited April 5, 2018).

⁸⁹ See M³AAWG, Voice and Telephony Abuse Special Interest Group, <https://www.m3aawg.org/voice-and-telephony-abuse-sig> (last visited April 5, 2018).

⁹⁰ See Internet Eng'g Task Force, Secure Telephone Identity Revisited (STIR), <https://datatracker.ietf.org/wg/stir/charter/> (last visited April 5, 2018).

⁹¹ See <https://www.ucenet.org/> (last visited April 5, 2018).

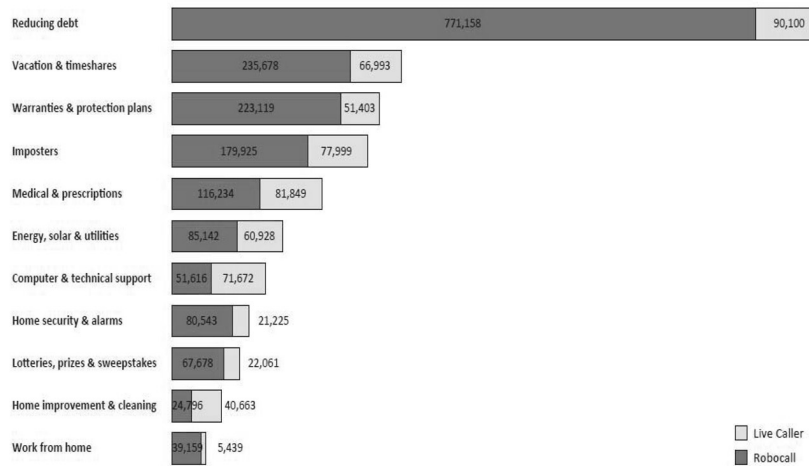
⁹² Press Release, FTC Releases FY 2017 National Do Not Call Registry Data Book and DNC Mini Site (Dec. 18, 2017) available at <https://www.ftc.gov/news-events/press-releases/2017/12/ftc-releases-fy-2017-national-do-not-call-registry-data-book-dnc>. Excerpts from the Data Book are attached at Exhibit A.

⁹³ *Id.*

developed a “mini site” on its website to make the information in the FY 2017 Data Book more accessible for the public, such as providing a webpage for each state.⁹⁴ For the first time, the data behind the report is also available in data files on the new website.⁹⁵

One of the features of the new Data Book is a breakdown of the topics of calls reported to the FTC that it gathered from the FTC’s revised online complaint form:

FY 2017 COMPLAINTS BY TOPIC⁹⁶



The state-by-state analysis also includes the top 10 topics of consumer complaints per state.⁹⁷

In addition to refining our complaint intake process and upgrading our Data Book, the FTC recently began a new initiative to help improve industry call-blocking solutions by increasing the amount and frequency of consumer complaint data that we make publicly available.⁹⁸ Beginning in August 2017, 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 whether the call was a robocall.⁹⁹ By making our available data more up-to-date and more robust, the FTC seeks to improve the functionality of 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.

⁹⁴ *Id.*

⁹⁵ *Id.*

⁹⁶ See Do Not Call Registry Data Book 2017: Complaint Figures for FY 2017 available at <https://www.ftc.gov/reports/national-do-not-call-registry-data-book-fiscal-year-2017>. Not everyone who files a complaint reports a topic.

⁹⁷ See, e.g., Do Not Call Registry Data Book 2017: Alabama available at <https://www.ftc.gov/reports/national-do-not-call-registry-data-book-fiscal-year-2017/alabama>.

⁹⁸ 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>.

⁹⁹ 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.

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,¹⁰⁰ available call blocking solutions,¹⁰¹ and how to identify common scams.¹⁰² The FTC disseminates these tips through articles,¹⁰³ blog posts,¹⁰⁴ social media,¹⁰⁵ infographics,¹⁰⁶ videos,¹⁰⁷ audio,¹⁰⁸ 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.¹⁰⁹

The FTC is taking additional steps to communicate information to consumers about the available call-blocking solutions that might reduce the amount of unwanted calls they receive. On April 23, 2018, the FTC is co-hosting with the FCC a “Stop Illegal Robocalls Expo.”¹¹⁰ The Expo will feature innovative technologies, devices, and applications to minimize or eliminate the number of illegal robocalls consumers receive.¹¹¹ The Expo is free and open to the public.¹¹² In late March, the FTC also put out additional information on its websites regarding how to stop unwanted calls for different types of phone services: mobile, landline or VOIP.¹¹³

IV. NEXT STEPS AND CONCLUSION

The Do Not Call Registry continues to help protect consumers against unsolicited calls from legitimate telemarketers. However, 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.
 - 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

¹⁰⁰ See, e.g., National Do Not Call Registry, <http://www.consumer.ftc.gov/articles/0108-national-do-not-call-registry>.

¹⁰¹ See, e.g., FTC Consumer Information Blocking Unwanted Calls <https://www.consumer.ftc.gov/articles/0548-blocking-unwanted-calls>.

¹⁰² See, e.g., FTC Consumer Information Scam Alerts, <https://www.consumer.ftc.gov/scam-alerts>.

¹⁰³ See, e.g., FTC Robocall Microsite, <http://www.consumer.ftc.gov/features/feature-0025-robocalls>.

¹⁰⁴ See, e.g., FTC Consumer Information Blog, Looking to Block Unwanted Calls? <https://www.consumer.ftc.gov/blog/looking-block-unwanted-calls>; FTC Consumer Information Blog, That’s Not Your Neighbor Calling <https://www.consumer.ftc.gov/blog/2018/01/thats-not-your-neighbor-calling>; FTC Consumer Information Blog, Apps to Stop Robocalls <https://www.consumer.ftc.gov/blog/2017/10/apps-stop-robocalls>.

¹⁰⁵ 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>.

¹⁰⁶ 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.

¹⁰⁷ See, e.g., FTC Video and Media, <http://www.consumer.ftc.gov/media>.

¹⁰⁸ See, e.g., FTC Consumer Information Audio, “Hang Up on Robocalls,” <http://www.consumer.ftc.gov/media/audio-0045-hang-robocalls>.

¹⁰⁹ See Pass It On, <http://www.consumer.ftc.gov/features/feature-0030-pass-it-on#identity-theft>.

¹¹⁰ See Press Release, FTC and FCC Seek Exhibitors for an Expo Featuring Technologies to Block Illegal Robocalls (Mar. 7, 2018) available at <https://www.ftc.gov/news-events/press-releases/2018/03/ftc-fcc-seek-exhibitors-expo-featuring-technologies-block-illegal>.

¹¹¹ *Id.*

¹¹² *Id.*

¹¹³ See FTC Consumer Information How to Stop Unwanted Calls available at <https://www.consumer.ftc.gov/features/how-stop-unwanted-calls>. A copy of this guidance is attached at Exhibit B.

- 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.

National Do Not Call Registry

Data Book FY 2017

Federal Trade Commission
December 2017



The Data Book

The *National Do Not Call Registry Data Book* contains statistical data about phone numbers on the Registry, telemarketers and sellers accessing phone numbers on the Registry, and complaints consumers submit to the FTC about telemarketers allegedly violating the Do Not Call rules. Statistical data on Do Not Call (DNC) complaints is based on unverified complaints reported by consumers, not on a consumer survey.

New in FY 2017

- When reporting the total number of DNC complaints, the Data Book now breaks the number down to show how many complaints were about robocalls and how many were from live callers. With a few exceptions, telemarketing robocalls are illegal, whether or not a number is on the Do Not Call Registry. As always, when it's a live caller, we verify that the consumer's telephone number was on the Do Not Call Registry before we take the complaint.
- The online complaint form now asks for the topic of the call, so this new information is included in the Data Book.
 - Consumers can choose to report specific topics, such as reducing debt, vacation & timeshares, and several other categories. Not everyone who files a complaint reports a topic.
 - The Data Book does not include statistics where a consumer chose "Other," or topics less likely to violate the Do Not Call Rules, such as debt collection, political, or charitable calls.
- The Data Book now includes a state-by-state analysis of DNC complaints, and it has a new, more accurate way of reporting a consumer's state:
 - If consumers report their state, the Data Book always uses the state they report.
 - If consumers do not report their state, the Data Book uses their area code.
 - The state-by-state analysis also includes the top 10 topics of consumer complaints.
- The underlying data in the report is available on our open government site at: www.ftc.gov/donotcall-databook2017.

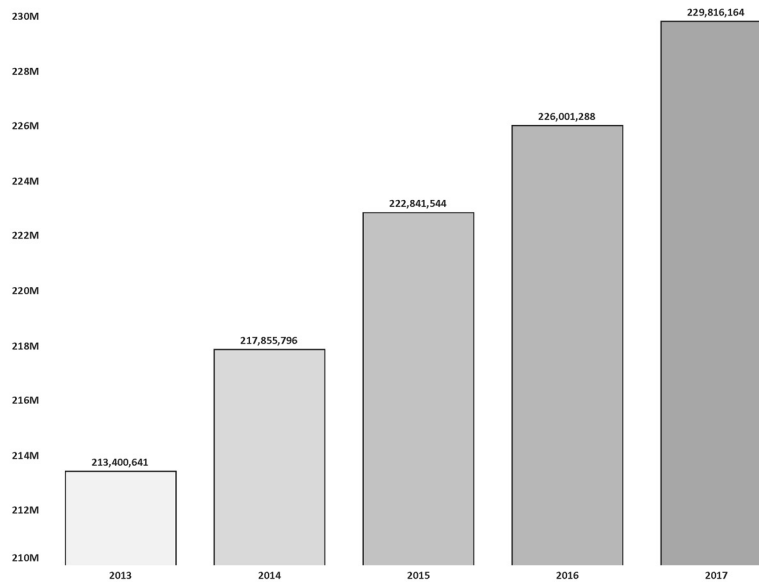
Inside the numbers

- States are ranked based on the number of registrations or complaints per 100,000 population. Complaint figures include the total number of FY 2017 complaints submitted to the FTC. Population estimates are based on 2016 U.S. Census population estimates (Table NST-EST2016-01 – Annual Estimates of the Population for the United States, Regions, States, and Puerto Rico: April 1, 2010 to July 1, 2016).
- For the purposes of this report, "active registrations" are those registrations consumers have placed on the Registry that have not been subsequently deleted by the consumer or removed by the FTC. The FTC removes numbers that have been disconnected and reassigned.



FY 2017
National Do Not Call Registry
Who is using the Do Not Call Registry

Active Registrations by Fiscal Year



"Active Registrations" reflect the total number of phone numbers registered on the National Do Not Call Registry for each fiscal year as of September 30, 2017.

Organizations Accessing the Registry by Fiscal Year

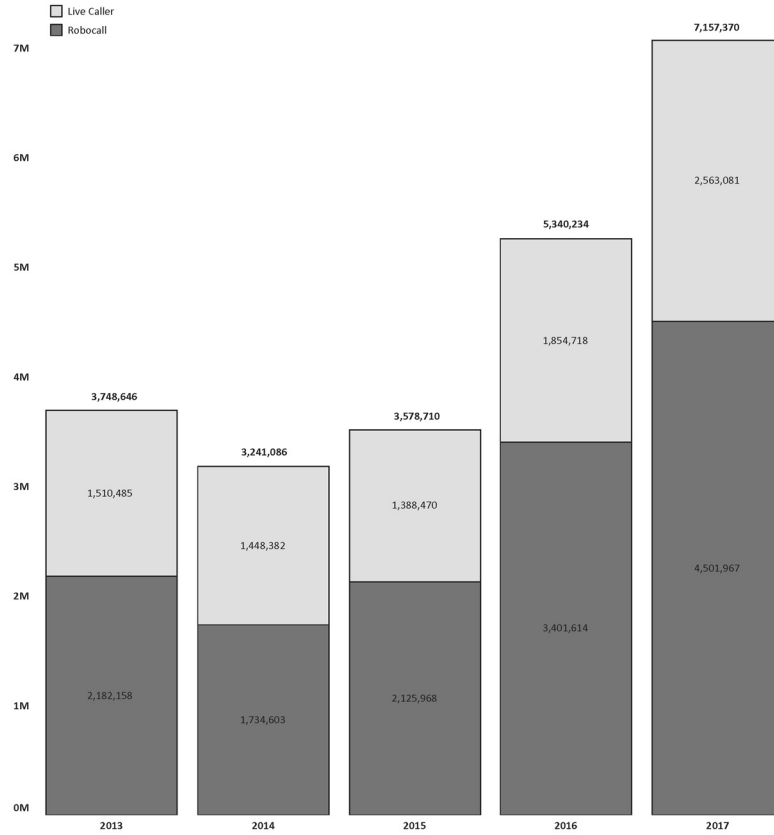
	2013	2014	2015	2016	2017
5 or Fewer Area Codes	24,182	23,049	20,075	17,634	15,536
Organizations Who Paid	2,877	2,582	2,502	2,353	2,259
Exempt Organizations	598	585	521	503	543
Total	27,657	26,216	23,098	20,490	18,338

Telemarketers and sellers can access up to five area codes on the Registry for free. To access more than five area codes, they must pay a fee. Organizations that are not selling goods or services are "exempt" and can access numbers on the Registry for free. This includes organizations asking for charitable contributions, raising money for political purposes, or conducting surveys. It also includes organizations calling **only** people they have an established business relationship with or who have given the organization written permission to call.



FY 2017
National Do Not Call Registry
Complaint Figures by Year

Complaints by Call Type and Fiscal Year

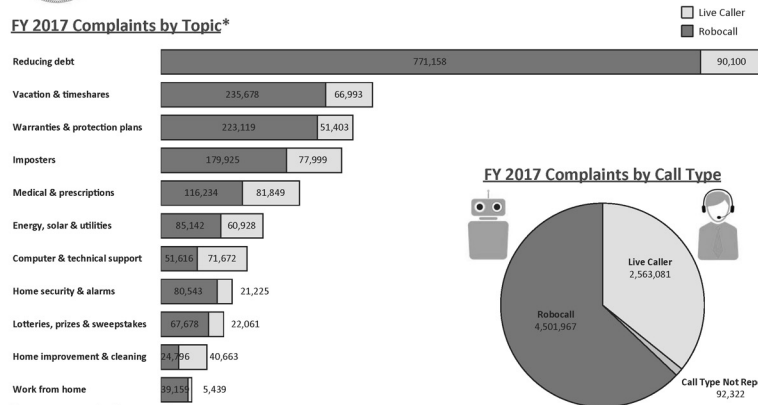


The total includes complaints about robocalls, complaints about live callers, and complaints where the call type was not reported. The number of calls where a call type was not reported is relatively small every year. The data is available at www.ftc.gov/donotcall-databook2017.



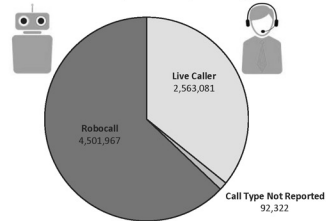
FY 2017 National Do Not Call Registry Complaint Figures for the Year

FY 2017 Complaints by Topic*

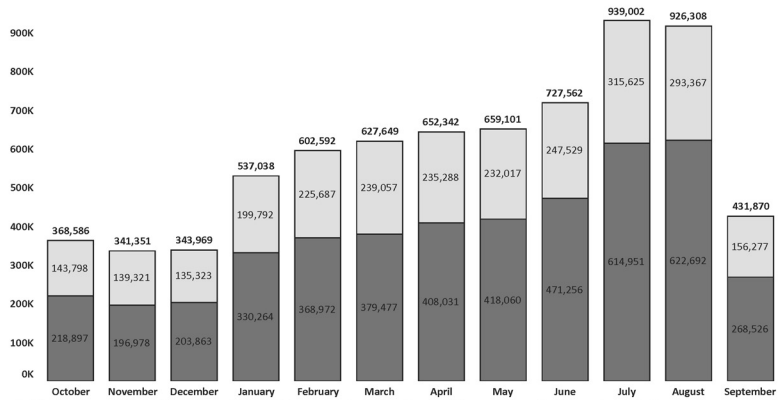


*Not everyone who files a complaint reports a topic.

FY 2017 Complaints by Call Type



FY 2017 Complaints by Month



The total includes complaints about robocalls, complaints about live callers, and complaints where the call type was not reported. The number of calls where a call type was not reported is relatively small every month. The full data, as well as complaints reporting that the consumer asked the entity to stop calling, is available at www.ftc.gov/donotcall-database2017. The FTC identified a technical problem with complaint submissions that resulted in artificially high complaint counts in July and August. The FTC addressed the issue, and September's figures reflect the adjustment.

State Rankings for National Do Not Call Registry Registrations per 100K Population



Rank	Consumer State	Active Registrations	Active Registrations per 100K Population	Rank	Consumer State	Active Registrations	Active Registrations per 100K Population
1	New Hampshire	1,222,035	91,552	27	New York	14,052,247	71,168
2	Connecticut	3,183,068	89,001	28	Washington	5,160,189	70,886
3	Massachusetts	5,794,055	89,001	29	Florida	14,607,866	70,859
4	Maine	1,092,143	82,025	30	Tennessee	3,891,688	70,724
5	New Jersey	7,306,538	83,618	31	Alabama	3,393,619	69,780
6	Kansas	2,359,523	81,159	32	Idaho	1,171,358	69,594
7	Colorado	4,444,187	80,912	33	North Dakota	524,414	69,188
8	Vermont	500,495	80,131	34	Georgia	7,095,199	68,816
9	Michigan	7,942,407	79,278	35	Oklahoma	2,667,174	68,182
10	Wisconsin	4,621,662	79,977	36	Arkansas	2,031,921	67,997
11	Pennsylvania	10,209,190	79,858	37	West Virginia	1,240,873	67,766
12	Iowa	2,436,336	79,444	38	North Carolina	6,810,043	67,115
13	Nebraska	1,496,889	78,490	39	Nevada	1,955,039	66,997
14	Delaware	746,072	76,944	40	Arizona	4,596,446	66,317
15	Ohio	9,085,945	78,230	41	Missouri	4,040,559	66,315
16	Wyoming	457,902	78,207	42	California	25,926,903	66,056
17	Minnesota	4,314,316	78,316	43	Utah	1,938,175	63,521
18	Illinois	9,960,608	77,961	44	Indiana	4,169,999	62,867
19	Maryland	4,654,044	77,363	45	South Carolina	3,160,994	61,760
20	Rhode Island	813,061	76,963	46	Louisiana	2,824,750	60,336
21	Montana	794,053	76,167	47	Texas	15,469,941	55,522
22	Kentucky	3,329,393	75,037	48	Mississippi	1,636,395	54,752
23	New Mexico	1,548,728	74,422	49	Hawaii	781,815	54,728
24	Virginia	6,189,394	73,540	50	Alaska	366,337	50,166
25	South Dakota	634,341	73,296		District of Columbia	620,154	91,042
26	Oregon	2,971,402	72,899		Puerto Rico	399,156	11,701

The District of Columbia and Puerto Rico are included in the table but are not ranked. States are ranked based on the number of active registrations per 100,000 population. Active registrations include all phone numbers on the National Do Not Call Registry as of September 30, 2017. Population estimates are based on 2016 U.S. Census population estimates.



**FY 2017
National Do Not Call Registry
Complaints by State**

State Rankings for National Do Not Call Registry Complaints per 100K Population



Rank	Consumer State	Complaints	Complaints per 100K Population	Rank	Consumer State	Complaints	Complaints per 100K Population
1	New Jersey	321,393	3,593	27	Arkansas	61,697	2,065
2	Delaware	27,691	2,909	28	Montana	21,211	2,035
3	Florida	588,021	2,853	29	Iowa	63,502	2,026
4	Virginia	232,818	2,768	30	Wyoming	11,808	2,017
5	New Hampshire	36,401	2,727	31	Texas	559,563	2,008
6	Michigan	265,465	2,674	32	South Carolina	99,620	2,008
7	Connecticut	94,440	2,641	33	Idaho	33,157	1,970
8	Rhode Island	26,590	2,517	34	North Carolina	199,407	1,965
9	Maryland	150,346	2,499	35	Kansas	55,207	1,899
10	Arizona	169,702	2,448	36	Louisiana	86,267	1,843
11	Tennessee	158,896	2,389	37	New Mexico	37,653	1,809
12	Vermont	14,896	2,385	38	Washington	125,689	1,725
13	Ohio	276,667	2,382	39	Indiana	114,241	1,722
14	Nevada	69,639	2,369	40	Wisconsin	98,352	1,702
15	Georgia	242,242	2,349	41	Minnesota	91,166	1,652
16	Colorado	129,609	2,339	42	Kentucky	72,110	1,625
17	Illinois	295,218	2,306	43	Oklahoma	61,962	1,579
18	New York	454,100	2,300	44	West Virginia	28,738	1,569
19	Massachusetts	156,006	2,290	45	South Dakota	13,316	1,539
20	Oregon	93,121	2,275	46	Mississippi	39,969	1,337
21	Nebraska	43,255	2,268	47	North Dakota	9,881	1,304
22	Alabama	108,003	2,221	48	Missouri	74,102	1,216
23	Maine	29,495	2,215	49	Hawaii	16,055	1,124
24	Utah	66,229	2,171	50	Alaska	3,041	410
25	Pennsylvania	271,832	2,126		District of Columbia	24,303	3,568
26	California	824,692	2,101		Puerto Rico	1,638	48

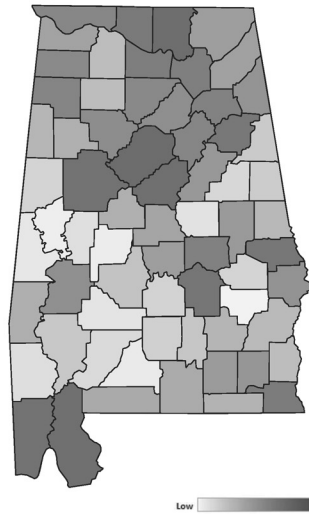
The District of Columbia and Puerto Rico are included in the table but are not ranked. States are ranked based on the number of complaints per 100,000 population. Complaints include the total number of FY 2017 complaints submitted to the FTC. Population estimates are based on 2016 U.S. Census population estimates.



FY 2017
National Do Not Call Registry
Registration and Complaint Figures by State

Alabama

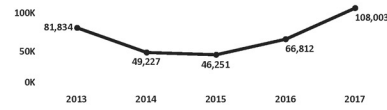
Complaints by County



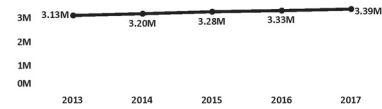
State Totals

Complaints: 108,003 (#22 nationally, per 100K population)
 Active Registrations: 3,393,619 (#31 nationally, per 100K population)

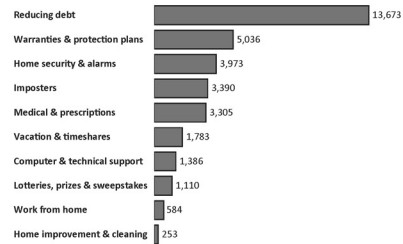
Complaints by Fiscal Year



Active Registrations by Fiscal Year

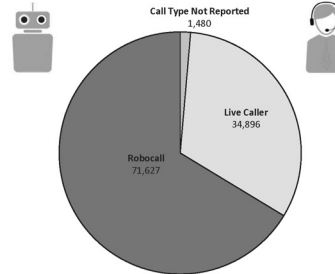


Complaints by Topics*




*Not everyone who files a complaint reports a topic.


Complaints by Call Type




How to stop unwanted calls **ON A MOBILE PHONE**



See what **built-in features** your phone has.




See what services your **carrier** offers.



Download a **call-blocking app**.


- Some apps are **free**, but others charge a monthly **fee**.
- Some apps will **access your contacts**.
- Calls might be **stopped, ring silently**, or go straight to **voicemail**.




Report unwanted calls at
ftc.gov/complaint

FEDERAL TRADE COMMISSION • ftc.gov/calls


How to stop unwanted calls
IF YOU USE VOIP




Look into
internet-based services. Your **carrier** might be able to help.




Not sure if your home phone uses the **internet** (VOIP)?
Check with your **carrier**.



With blocking services, calls might be **stopped, ring silently**, or go straight to **voicemail**.

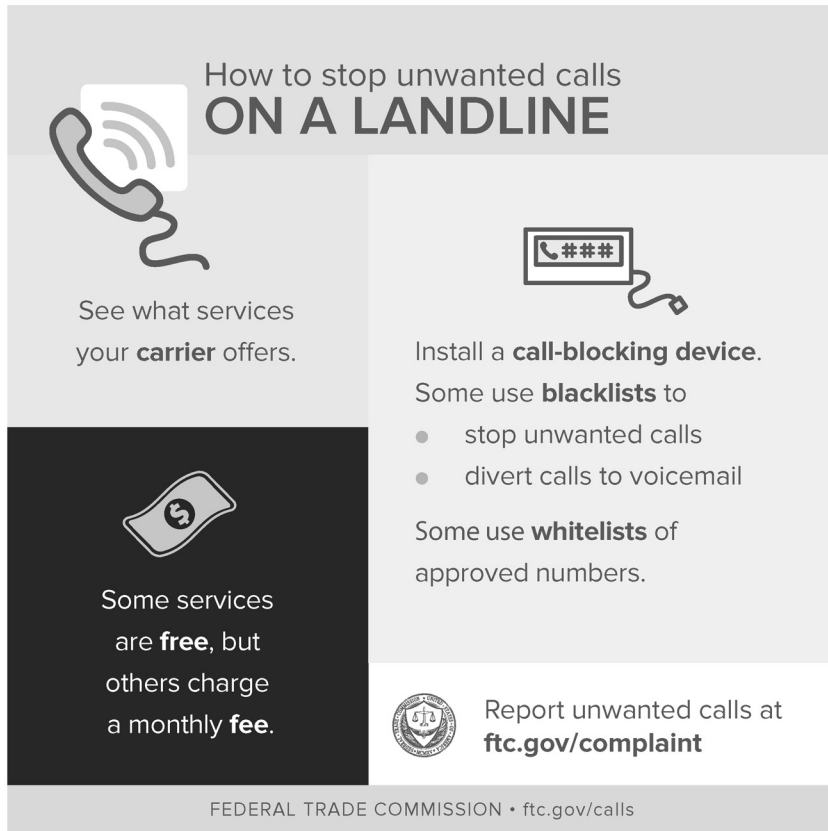


Some services are **free**, but others charge a monthly **fee**.



Report unwanted calls at
ftc.gov/complaint

FEDERAL TRADE COMMISSION • ftc.gov/calls



How to stop unwanted calls
ON A LANDLINE

See what services your **carrier** offers.

Install a **call-blocking device**.
Some use **blacklists** to

- stop unwanted calls
- divert calls to voicemail

Some use **whitelists** of approved numbers.

Some services are **free**, but others charge a monthly **fee**.

Report unwanted calls at **ftc.gov/complaint**

FEDERAL TRADE COMMISSION • ftc.gov/calls

The CHAIRMAN. Thank you, Ms. Greisman.
Mr. Rupy.

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

Mr. RUPY. Chairman Thune, 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 concerns about the problems associated with phone-based imposter scams targeting consumers.

In this ongoing battle against criminal robocallers, there have been four significant developments over the last year.

First, the industry-led, ecosystem-wide Robocall Strike Force issued a series of reports to the FCC in October 2016 and April 2017. These reports hold a significant amount of good news for consumers. For example, the reports note that the SHAKEN/STIR standards development for the next generation of robocall mitigation tools were accelerated by 6 months. Some of the initial testing of the SHAKEN standard is expected to complete later this year with potential deployments anticipated later this year and in 2019.

These reports also 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 from just three carriers in July 2016 to 22 providers 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.

Second, the reports show that USTelecom member companies, independent application developers, and a growing number of diverse companies offer services today that can help consumers 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 block suspected fraudulent calls. AT&T also offers AT&T Digital Call Protect for IP wireline phones.

Verizon's new Spam Alerts service provides its wireline customers who have caller ID, whether they are on copper or fiber, with enhanced warnings about calls that meet Verizon's spam criteria by showing the term "Spam?" with a question mark, before a caller's name on the caller ID display.

On the wireless side, Verizon has deployed and continues to expand robocall mitigation features as part of its Caller Name ID service, including a filter that automatically forwards to voice-mail any calls corresponding to the spam risk level selected by the customer.

The significant growth in consumers' tools was highlighted just a few weeks ago at a joint FCC-FTC robocall workshop where it was noted that since 2016, there has been a 495 percent increase in smartphone applications for addressing robocalls.

Third, the FCC recently adopted rules allowing voice providers to block certain types of calls. USTelecom supported adoption of these rules and participated fully in the proceeding. One issue the FCC raised is what protections legitimate callers should have if their calls are blocked, both for situations where voice providers block numbers directly, and for blocking services that consumers may opt into.

This fall, USTelecom hosted a workshop aimed at helping develop best practices for the scoring and labeling of calls, and a follow up workshop is scheduled next month.

Finally, we applaud our Federal Government partners at the FCC and FTC, who have engaged in a series of enforcement actions against illegal robocallers. Both agencies' civil enforcement actions send a strong and powerful message to illegal robocallers that they will be located and brought to justice. While these civil enforcement efforts are laudatory, we believe there is an acute need for coordinated, targeted, and aggressive criminal enforcement of illegal robocallers at the Federal level. Given the felonious nature of their activities, criminal syndicates engaged in illegal robocalling should be identified, targeted, and brought to justice through criminal enforcement efforts.

While consumer-centric tools may stop a series of calls from reaching certain consumers, root-cause removal through criminal enforcement stops millions of calls from ever being originated.

Let me again thank the Committee for holding this timely hearing. And I look forward to our continued work together to address this constantly evolving challenge.

[The prepared statement of Mr. Rupy follows:]

PREPARED STATEMENT OF KEVIN RUPY, VICE PRESIDENT, LAW AND POLICY,
USTELECOM

Chairman Thune, Ranking Member Nelson, 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 targeting consumers. Scammers can use Caller ID spoofing 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 four 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 last year on April 28, 2017. These reports, taken together, catalogue industry's substantial efforts to advance the battle against illegal robocalls. These reports hold a significant amount of good news for consumers. 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, were accelerated by six months. These standards, which incorporate caller-ID authentication capabilities into the network and consumer devices, have entered the industry testing phase. In addition, the North American Numbering Council (NANC)—a Federal Advisory Committee that counsels the FCC on numbering issues—is nearing completion of its recommendation to the FCC on the SHAKEN governance framework. Some of the initial testing of the SHAKEN standard is expected to complete later this year, with potential deployments anticipated later this year and in 2019.

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.

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. AT&T also offers AT&T Digital Call Protect for IP wireline phones. Verizon's new Spam Alerts service provides its wireline customers who have Caller

ID—whether they are on copper or fiber—with enhanced warnings about calls that meet Verizon’s spam criteria by showing the term “SPAM” before a caller’s name on the Caller ID display. And on the wireless side, Verizon has deployed and continues to expand robocall mitigation features as part of its Caller Name ID service, including a spam filter that automatically forwards to voice-mail any calls corresponding to the spam risk level selected by the customer.

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. In fact, at a recent joint FCC and FTC robocall workshop, it was noted that since 2016, there has been a 495 percent increase in smartphone applications alone for addressing robocalls.

Third, the FCC recently adopted rules allowing voice providers to block certain types of calls. USTelecom supported adoption of the rules and participated fully in the proceeding. One issue the FCC raised 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 hosted a workshop aimed at helping develop “best practices” for the scoring and labelling of calls. A follow-up workshop is scheduled next month.

Finally, we applaud our Federal government partners in the robocall fight, who have engaged in a series of enforcement actions against bad actors that have reinvigorated efforts to curb this illegal activity. For example, the FCC last year initiated enforcement actions against three entities that have resulted in more than \$200 million in proposed fines targeting perpetrators of illegal robocalling. The FTC also continues to engage in a series of complementary enforcement actions that target the worst of the worst bad actors in this space. These civil enforcement actions brought by both agencies send a strong and powerful message to illegal robocallers that they will be located and brought to justice. USTelecom and its industry partners stand ready to further assist in these efforts to bring this bad actors to justice. Indeed, the ultimate goal of USTelecom’s Industry Traceback Group is to identify the source of the worst of these illegal calls, and further enable further enforcement actions by Federal agencies.

While current Federal enforcement efforts are laudatory, they are mostly limited to civil enforcement. We believe there is an acute need for coordinated, targeted and aggressive *criminal* enforcement of illegal robocallers at the Federal level. As a result, bad actors currently engaged in criminal robocall activities are—at most—subject only to civil forfeitures. Given the felonious nature of their activities, criminal syndicates engaged in illegal robocalling activity should be identified, targeted and brought to justice through criminal enforcement efforts. We believe, in particular, that U.S. Attorneys’ offices across the country should prioritize enforcement where Federal statutes, such as the Truth in Caller ID Act, are implicated, and should work closely with the FCC and FTC and international partners in enforcement cases, particularly when the calls originate outside of the United States. While a holistic approach is essential to broadly address the issue of robocalls, robust enforcement efforts targeting illegal robocallers are most effective since they address the activity at the source. For example, consumer-centric tools may stop a series of calls from reaching tens of thousands consumers, whereas root-cause removal stops millions of calls from ever being sent.

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 last year. The collaborative efforts outlined in the re-

port 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.

The CHAIRMAN. Thank you, Mr. Rupy.
Mr. Delacourt.

STATEMENT OF SCOTT DELACOURT, PARTNER, WILEY REIN LLP, ON BEHALF OF THE U.S. CHAMBER INSTITUTE FOR LEGAL REFORM

Mr. DELACOURT. Chairman Thune, Ranking Member Nelson, and members of the Committee, my name is Scott Delacourt, and I am a partner in the telecommunications, media, and technology practice at Wiley Rein LLP. I am here today on behalf of the U.S. Chamber Institute for Legal Reform, or ILR.

The U.S. Chamber is the world's largest business federation, representing the interests of more than 3 million businesses of all sizes and sectors. ILR is an affiliate of the U.S. Chamber that promotes civil justice reform. Thank you for the opportunity to testify today about abusive robocalls and why legitimate businesses trying to communicate with their customers who do not make these types of calls need Telephone Consumer Protection Act reform.

I would like to make three points today.

First, TCPA class-action litigation has harmed consumers and legitimate businesses while doing little to reduce illegal and abusive robocalling.

Second, the D.C. Circuit's recent decision vacating portions of the FCC's 2015 Omnibus TCPA Order presents a sensible roadmap for interpreting the TCPA in a way that provides clear guidance to consumers and businesses.

Third, the FCC should follow the court's guidance, clarify the TCPA's requirements, and focus on bad actors.

Illegal and abusive robocalls continue to be a menace and a top complaint of consumers across the U.S. These calls originate with bad actors, and ILR does not condone the conduct. Customers are the lifeblood of commerce, and successful businesses avoid practices that customers revile. U.S. businesses have no interest in engaging in abusive practices. Indeed, businesses fear the brand and customer relationship damage of being cast as an illegal and abusive robocaller.

On the other hand, ILR is concerned about businesses being able to communicate with their customers through the use of modern technology in an efficient and cost-effective manner. Consumers expect timely contemporary communications from the companies with whom they choose to do business. Unfortunately, the TCPA has become an obstacle, preventing legitimate and lawful communications between businesses and their customers. Businesses are in the crosshairs of potential litigation each time they pick up the phone or send a text message.

The TCPA prohibits making calls to wireless telephone numbers using any automatic telephone dialing system, or ATDS, without the prior express consent of the called party. The act focused on

technology, not bad conduct, such as harassment or fraud. Ambiguity over what constitutes an ATDS has become a source of unnecessary class-action litigation while doing little to stop truly abusive robocalls. Indeed, the number of TCPA case filings exploded to 4,860 in 2016, and TCPA litigation grew 31.8 percent between 2015 and 2016.

Much of the litigation targets legitimate companies, many of which are well-known brands, that have committed marginal or unavoidable violations instead of the true bad actors, scam telemarketers, offshore operations, and fraudsters who operate through thinly capitalized and disappearing shell companies. These latter activities are of little interest to class-action lawyers.

Abusive litigation targeting legitimate companies has devastating effects, as the TCPA's uncapped statutory damages can lead to multimillion-dollar judgments. Often consumers do not even collect from the judgment funds established to remediate harm, making class-action lawyers the only winners. Ironically, such litigation ultimately hurts the consumers it is intended to protect, as the costs are passed on in the form of increased costs of goods and services.

The Federal Communications Commission's implementation of the TCPA to some degree has contributed to the problem. In its 2015 omnibus order, the FCC expanded the types of devices that are considered ATDS to include equipment with computing capability or to which computing capability might be added, and expansive reading that potentially sweeps in everyday devices like smartphones and tablets, creating major uncertainty for businesses. Indeed, the FCC's order contributed to a 46 percent increase in TCPA litigation.

The D.C. Circuit's decision last month in *ACA International v. FCC*, in which the U.S. Chamber was a petitioner, overturned key provisions of the FCC's order, including the agency's definition of an ATDS, which the court described as utterly unreasonable. The decision includes a sensible roadmap for how the FCC might interpret the TCPA in a manner that is clear and understandable, significantly reducing frivolous class-action litigation. This decision provides an opportunity for the FCC to revisit and clarify its approach to the TCPA. Following the D.C. Circuit's approach would provide guidance and clarity to businesses, and allow regulators, law enforcement, and courts to focus on the bad actors who are the source of the robocalling problem.

Thank you for the opportunity to testify today. And I look forward to your questions.

[The prepared statement of Mr. Delacourt follows:]

PREPARED STATEMENT OF SCOTT DELACOURT, PARTNER, WILEY REIN LLP,
ON BEHALF OF THE U.S. CHAMBER INSTITUTE FOR LEGAL REFORM

I. Introduction

Chairman Thune, Ranking Member Nelson, and members of the Committee. My name is Scott Delacourt. I am a Partner in the Telecommunications, Media, and Technology Practice at Wiley Rein LLP, and I am here on behalf of the U.S. Chamber Institute for Legal Reform ("ILR"). The U.S. Chamber is the world's largest business federation, representing the interests of more than three million businesses of all sizes and sectors, as well as state and local chambers and industry associations. ILR is an affiliate of the U.S. Chamber that promotes civil justice reform through

regulatory, legislative, judicial, and educational activities at the global, national, state, and local levels. Thank you for the opportunity to testify today about abusive robocalls, and why legitimate businesses trying to communicate with their customers, who are not making these types of calls, desperately need the Telephone Consumer Protection Act (“TCPA”) reformed.

I would like to make three points today:

- First, TCPA class-action litigation has harmed consumers and legitimate businesses while doing little to reduce illegal and abusive robocalling.
- Second, the D.C. Circuit’s recent decision vacating portions of the FCC’s 2015 *Omnibus TCPA Order* presents a sensible roadmap for interpreting the TCPA in a way that provides clear guidance to consumers and businesses.
- Third, the FCC should follow the court’s guidance, clarify the TCPA’s requirements, and focus on bad actors.

Illegal and abusive robocalls continue to be a menace and a top complaint of consumers across the U.S. These calls originate with bad actors, and ILR does not condone the conduct. The ILR’s members—a broad cross-section of American business—share consumers’ concern. Customers are the life-blood of commerce, and successful businesses avoid practices that customers revile. U.S. businesses have no interest in engaging in abusive practices. Indeed, businesses fear the brand and customer relationship damage of being cast as an illegal and abusive robocaller.

On the other hand, ILR is concerned about businesses being able to communicate with their customers through the use of modern technology, in an efficient and cost-effective manner, while consumers desire and expect timely, contemporary communications from the companies with whom they choose to do business. Unfortunately, the TCPA has become an obstacle, preventing legitimate and lawful communications between businesses—large and small—and their customers and has placed businesses in the crosshairs of potential litigation each time they pick up the phone or send a text message.

The TCPA prohibits making phone calls to wireless telephone numbers “using any automatic telephone dialing system” (“ATDS”) without the prior express consent of the called party. The Act focuses on technology, not bad conduct such as harassment or fraud. Ambiguity over the technology used or what constitutes an ATDS has become a source of unnecessary and sometimes abusive class-action litigation, burdening how businesses reach their customers, while doing little to stop truly abusive robocalls. Indeed, the number of TCPA case filings exploded to 4,860 in 2016, and TCPA litigation grew 31.8 percent between 2015 and 2016. Much of this litigation targets legitimate companies—many of which are well-known brands—that have committed marginal or unavoidable violations, instead of the true bad actors: scam telemarketers, offshore operations, and fraudsters who operate through thinly-capitalized and disappearing shell companies. These latter activities are of little interest to class-action lawyers.

Abusive litigation targeting legitimate companies has devastating effects, as the TCPA’s uncapped statutory damages can lead to multi-million-dollar judgments. Often consumers do not even collect from the judgment funds established to remediate harm, making class-action lawyers the only winners.¹ Ironically, such litigation ultimately hurts the consumers it is intended to protect as the costs are passed along in the form of increased prices for goods and services.

The Federal Communications Commission’s (“FCC”) implementation of the TCPA, to some degree, has contributed to this problem. In its 2015 *Omnibus Order*, the FCC expanded the types of devices that are considered ATDS to include equipment with computing capability or to which computing capability might be added—an expansive reading that potentially sweeps in everyday devices like smart phones and tablets, creating major uncertainty for businesses. Indeed, the FCC’s *Omnibus Order* contributed to a 46 percent increase in TCPA litigation.

The D.C. Circuit’s decision last month in *ACA Int’l v. FCC*, in which the U.S. Chamber was a petitioner, overturned certain key provisions of the FCC’s *Omnibus Order*, including the agency’s definition of an automated telephone dialing system

¹ For example, one survey of Federal TCPA settlements found that in 2014, the average attorneys’ fees awarded in TCPA class action settlements was \$2.4 million, while the average class member’s award in these same actions was \$4.12. Wells Fargo Ex Parte Notice, filed January 16, 2015, in CG Docket No. 02–278, p. 19, available at <http://apps.fcc.gov/ecfs/document/view?id=60001016697>. One of the most recent examples of the lucrative success that plaintiffs’ attorneys continue to achieve in TCPA class actions includes an award of \$15.26 million in fees. Plaintiffs’ counsel originally petition for an award in amount equal to one-third of the final common fund total. *Aranda et al., v. Caribbean Cruise Line, Inc. et al.*, No. 12–04069, 2017 U.S. Dist. LEXIS 52645 (N.D. Ill., April 6, 2017),

(“ATDS”), which the court described as “utterly unreasonable.”² The decision includes a sensible roadmap for how the FCC might interpret the TCPA in a manner that is clear and understandable, significantly reducing frivolous class-action litigation. This decision provides an opportunity for the FCC to revisit and clarify its approach to the TCPA. Following the D.C. Circuit’s approach would provide guidance and clarity to businesses, and allow regulators, law enforcement, and courts to focus on the bad actors who are the source of the robocalling problem.

II. Uncertainty Regarding the Requirements of the TCPA Has Led to Unnecessary Litigation that Does Little to Deter Robocalls

Congress enacted the TCPA in 1991 to stop abusive cold-call telemarketing and fax-blast spamming.³ In promulgating its initial rules implementing the Act, the Commission acknowledged the TCPA’s goal of “restrict[ing] the most abusive telemarketing practices.”⁴ The Supreme Court recognized that “Congress determined that Federal legislation was needed because *telemarketers*, by operating interstate, were escaping state-law prohibitions on *intrusive nuisance calls*.”⁵ Unfortunately, the Commission’s implementation of the Act over many years has fostered a whirlwind of litigation. Interpretations by courts and the FCC have strayed far from the statute’s text, Congressional intent, and common sense, turning the TCPA into a breeding ground for frivolous lawsuits brought by serial plaintiffs and their lawyers, who have made lucrative businesses out of targeting U.S. companies.⁶ The number of TCPA case filings exploded to 4,860 in 2016, and TCPA litigation grew 31.8 percent between 2015 and 2016.⁷ The focus of these lawsuits is often legitimate companies and well-known brands who have committed accidental or unavoidable violations. As then-Commissioner Ajit Pai highlighted, the Los Angeles Lakers were hit with a class-action lawsuit from fans who received text messages confirming receipt

² *ACA Int’l v. FCC*, No. 15–1211, slip op. at 15 (D.C. Cir., Mar. 16, 2018).

³ See S. Rep. 102–178 at 1–2 (1991) (stating that the purpose of the TCPA is to “plac[e] restrictions on unsolicited, automated telephone calls to the home” and noting complaints regarding telemarketing calls); H.R. Rep. No. 102–317 at 6–7 (1991) (citing telemarketing abuse as the primary motivator for legislative action leading to the TCPA). See also Comments of the U.S. Chamber and ILR, *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02–278, at 2–3 (filed Mar. 10, 2017).

⁴ See *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order, 7 FCC Rcd 8752, n.24 (Oct. 16, 1992) (“1992 Report and Order”).

⁵ *Mims v. Arrow Financial Services, LLC*, 565 U.S. 368, 370 (2012) (also citing the Preamble of the TCPA) (emphasis added); see also *Emanuel v. Los Angeles Lakers, Inc.*, 2013 WL 1719035, at *3 (“Courts ‘broadly recognize that not every text message or call constitutes an actionable offense; rather, the TCPA targets and seeks to prevent the proliferation of intrusive, nuisance calls.’”) (internal quotations omitted).

⁶ See Letter from ACA International et al to the Members of the U.S. House of Representatives, (Mar. 8, 2017), http://www.instituteforlegalreform.com/uploads/sites/1/TCPA_Coalition_Letter_FICALA_to_House.pdf. For examples, Craig Cunningham of Nashville, according to news reports, has filed approximately 83 TCPA lawsuits since 2014—including 19 in 2017. He has three cell phones he uses to compile TCPA claims. John O’Brien, *Phony Lawsuits: Man Has Filed 80 Lawsuits And Uses Sleuthing Skills To Track Down Defendants*, *Forbes*, Nov. 1, 2017, <https://www.forbes.com/sites/legalnewsline/2017/11/01/phony-lawsuits-man-has-filed-80-lawsuits-and-uses-sleuthing-skills-to-track-down-defendants/#456cd2a76be7>; A U.S. Magistrate judge found Jan Konopca, a serial plaintiff who has filed 31 lawsuits in New Jersey Federal court, was actively seeking the calls. Mr. Konopca earned approximately \$800,000 for his endeavors and has even claimed that he is no longer eligible for Social Security Disability benefits because of his TCPA litigation. John O’Brien, *Phony Lawsuits: Comcast Fighting For Access to ‘Professional’ Plaintiffs Prior Testimony*, *Forbes*, May 31, 2017, <https://www.forbes.com/sites/legalnewsline/2017/05/31/phony-lawsuits-comcast-fighting-for-access-to-professional-plaintiffs-prior-testimony/#18a02fba727c>; see also John O’Brien, *Phony Lawsuits: How a Polish immigrant apparently sued his way to \$800K*, *Forbes*, Mar. 15, 2017, <https://legalnewsline.com/stories/511092959-phony-lawsuits-how-a-polish-immigrant-apparently-sued-his-way-to-800k>; Melody Stoops began her TCPA “business” by collecting at least 35 cellphones that she stored in a shoebox. Though she lived in a small town in Central Pennsylvania, she used Florida area codes when she registered for a new phone number for each. By admitting her scheme, Stoops lost her standing to sue, a Pennsylvania judge ruled in 2015. If the calls were the goal, then she experienced no harm when she received them, it was determined. John O’Brien, *Phony Lawsuits: A Federal Law is Giving Litigious People A New Income Stream*, *Forbes*, Mar. 14, 2017, <https://www.forbes.com/sites/legalnewsline/2017/03/14/phony-lawsuits-a-federal-law-is-giving-litigious-people-a-new-income-stream/#6312998a68ee>; see also John O’Brien, *Phony Lawsuits: A ‘Most Profitable’ Scheme Has TCPA Plaintiff On Track For One Last Payday*, *Forbes*, Nov. 27, 2017, <https://www.forbes.com/sites/legalnewsline/2017/11/27/phony-lawsuits-a-most-profitable-scheme-has-tcpa-plaintiff-on-track-for-one-last-payday/#7787c5823ba1>.

⁷ See 2016 Year in Review: FDCA Down, FCRA & TCPA Up, WebRecon LLC (2018), <https://webrecon.com/2016-year-in-review/fdca-down-fcra-tcpa-up/>.

of fan-originated texts.⁸ Similarly, a ride-sharing service was sued for texts confirming receipt of ride requests.⁹ And Mammoth Mountain Ski Area was sued for calling a group of litigants who had previously provided consent.¹⁰

TCPA litigation has even gone so far as to subject nonprofit organizations to frivolous lawsuits. A blood bank, a state chapter of the Special Olympics, and the Breast Cancer Society have all faced TCPA suits.¹¹ Recently, the American Heart Association was handed a “victory” when a court in Louisiana found the plaintiff consented to the text messages she received and that the content of the messages was informational, not promotional.¹² As a result, the TCPA is forcing such organizations to utilize and waste precious staff and monetary resources to handle needless litigation rather than devoting those resources to life-saving research.

Because the TCPA provides for uncapped statutory damages, defendants in these lawsuits face multi-million-dollar judgments.¹³ Earlier this month, Outcome Health agreed to a \$2.9 million settlement to end a class-action lawsuit over daily automated nutrition tips it texted to recipients who had signed up to receive such information. In another case, Lake City Industrial Products, Inc., a small, family-owned company from Michigan, faced over \$5 million in statutory damages for faxes it sent believing they were legal.¹⁴ Other well-known companies, like Capital One Bank, AT&T, MetLife, Papa John’s Pizza and Walgreen’s Pharmacy, have faced settlements of over ten million dollars, the largest of which was \$75 million.¹⁵ TCPA lawsuits filed in the 17-month period after the 2015 FCC Omnibus Declaratory Ruling reached approximately 40 different industries.¹⁶

Compliance with the TCPA has been frustrated by uncertain and shifting standards as the FCC’s interpretations have evolved over decades, leaving a tangled web of obligations. Businesses making good-faith efforts to comply may nevertheless be subject to crippling litigation. Regulatory uncertainty and enormous settlements enriching class-action lawyers benefit neither consumers nor the economy. As FCC Commissioner Michael O’Rielly has observed, needless “enforcement actions or lawsuits” chill efforts by “good actors and innovators” to develop “new consumer-friendly communications services.”¹⁷

The FCC’s *Omnibus Order* added to the uncertainty. The TCPA prohibits making a call “using any automatic telephone dialing system” without the prior express consent of the called party.¹⁸ The Act defines “automatic telephone dialing system” as “equipment which has the capacity to store or produce telephone numbers to be called, using a random or sequential number generator; and to dial such numbers.”¹⁹ Uncertainty over the meaning of “capacity” led the FCC to adopt an order construing the term. Rather than providing clarity, however, the FCC adopted a sweeping interpretation including devices that have both the present and *potential* capacity to store or produce telephone numbers to be called, while also including devices that can generate random or sequential numbers and those that cannot.²⁰ This baffling interpretation raised the prospect that everyday devices like smart phones

⁸ *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991* Declaratory Ruling and Order, 30 FCC Rcd 7961, 8073 (2015) (“*Omnibus Order*”) (dissenting statement of Commissioner Ajit Pai).

⁹ *Id.*

¹⁰ *Scaling the ‘Mountain’ of TCPA Lawsuit Abuse*, U.S. Chamber Institute for Legal Reform (Apr. 8, 2015), <http://www.instituteforlegalreform.com/resource/scaling-the-mountain-of-tcpa-lawsuit-abuse> (explaining that the plaintiffs provided consent before a new FCC rule clarifying the prior express consent requirement took effect).

¹¹ See *Murphy v. DCI Biologicals Orlando, LLC, et. al.*, 797 F.3d 1302, 1308 (11th Cir. 2015); see also *Wengel v. DialAmerica Marketing, Inc.*, 132 F.Supp.3d 910 (E.D. Mich. Sep. 22, 2015); see also *Spiegel v. Reynolds et al.*, No. 17–3344 (7th Cir. Nov. 14, 2017).

¹² *Reese v. Anthem Inc., et al.*, No. 2:17-cv-07940 (E.D. La Mar. 12, 2018).

¹³ See *The Juggernaut of TCPA Litigation: The Problems with Uncapped Statutory Damages*, U.S. Chamber Institute for Legal Reform at 12 (October 2013), http://www.instituteforlegalreform.com/uploads/sites/1/TheJuggernautofTCPALit_WEB.PDF (“What is clear is that the TCPA’s uncapped statutory damages pose a real threat to large and small well-intentioned American companies who have potentially millions of customers and who often need to communicate with those consumers.”).

¹⁴ *Id.* at 10.

¹⁵ *TCPA Litigation Sprawl: A Study of the Sources and Targets of Recent TCPA Lawsuits*, U.S. Chamber Institute for Legal Reform at 10 (Aug. 2017), http://www.instituteforlegalreform.com/uploads/sites/1/TCPA_Paper_Final.pdf.

¹⁶ *Id.* at 3. In total 3,121 cases were examined. Over 1,000 of those cases—more than one-third of the total lawsuits reviewed—were brought as nationwide class actions. *Id.*

¹⁷ Commissioner O’Rielly, *TCPA: It is Time to Provide Clarity*, FCC Blog (Mar. 25, 2014, 2:10 PM), <https://www.fcc.gov/news-events/blog/2014/03/25/tcpa-it-time-provide-clarity>

¹⁸ 47 U.S.C. § 227(b)(1)(A).

¹⁹ *Id.* § 227(a)(1)(A)-(B).

²⁰ *Omnibus Order*, ¶¶ 10–15.

and tablets could be ATDS subject to the TCPA's prohibitions because of their potential capacity to store or produce telephone numbers to be called. This construction conflicted with the text, history, and purpose of the TCPA, and contributed to a 46 percent increase in TCPA litigation, with class actions comprising approximately one-third of those filings.²¹

III. The D.C. Circuit Vacated the FCC's Omnibus Order and Provided a Sensible Roadmap for Moving Forward

Numerous petitioners, including the U.S. Chamber of Commerce, sought judicial review of the *Omnibus Order's* unjustifiable expansion of the TCPA, arguing that the regime was unreasonable, impractical, and inconsistent with the statute's text. The D.C. Circuit largely agreed and vacated portions of the *Omnibus Order* in *ACA Int'l v. FCC*. Significantly, the court unanimously set aside the Commission's interpretation of ATDS, holding that the interpretation of capacity was "utterly unreasonable,"²² "incompatible with" the statute's goals, and "impermissibly" expansive.²³ The interpretation was so unreasonable, it was "considerably beyond the agency's zone of delegated authority."²⁴ The court also found unanimously that the Commission had offered an inconsistent and "inadequa[te]" explanation of what features constitute an [ATDS],²⁵ "fall[ing] short of reasoned decision making."²⁶

The opinion also provided a roadmap for how the FCC should proceed. The court pointed to the interpretation of "make any call . . . using" offered by Commissioner Michael O'Rielly in his *Omnibus Order* dissent, which would require that dialing equipment "*be used as an [ATDS]* to make the calls."²⁷ In other words, the calling equipment must actually use ATDS capabilities to make the call. Although the court did not explicitly endorse this approach, as the issue was not raised in the appeal, it noted that this construction would "substantially diminish the practical significance of the Commission's expansive understanding of 'capacity' in the [ATDS] definition."²⁸ This is a significant signal to the FCC and the courts about the best reading of the TCPA.

IV. The FCC Should Adopt a New Approach to the TCPA that Protects Legitimate Business Calls and Focuses on Bad Actors

The D.C. Circuit's decision provides an opportunity for the FCC to rethink its approach to the TCPA. Confusing regulations and interpretations of the statutory text have contributed to a rise in TCPA litigation while doing little to reduce illegal and abusive robocalling. At the same time, increased liability exposure and compliance costs have deterred businesses from reaching out to their customers. A renewed focus on the TCPA's statutory text offers a path forward to better protect consumers and businesses that operate in good faith.

Adopting the D.C. Circuit's suggested approach on what constitutes an ATDS would realign the interpretation of the TCPA to its text and purpose. This straightforward reading will ensure that liability attaches only when ATDS capabilities are used to make a call, rather than sweeping in calls made using smartphones, tablets, and other devices that conceivably *could* be modified to support autodialing at some point in the future. Significantly, it would provide businesses with clear guidance on the type of equipment they can use to contact their customers. A device's theoretical or potential capabilities would not be relevant to determining whether it is an ATDS. Instead, the inquiry should focus only on the functions used to make the call or calls in question. This clarification will help businesses avoid unnecessary litigation over whether they used an ATDS and help consumers differentiate whether they are targets of an illegal robocall campaign or receiving a routine business communication. Reducing the amount of TCPA litigation will also free up resources to focus on the actual bad actors who are the source of abusive robocalls. With fewer complaints, enforcement resources will not be wasted on investigating legitimate business communications and can be used to find and punish illegal robocallers.

The TCPA was never intended to make all mass calling illegal. The legislative history reflects that the Act was intended to achieve a balance between the need for legitimate businesses to lawfully communicate with their customers and protecting consumers from certain abusive uses of the telephone system. There are bad actors who abuse the openness of our communications infrastructure, including through

²¹ See *TCPA Litigation Sprawl* at 2, 4.

²² Slip op. at 19.

²³ Slip op. at 23.

²⁴ Slip op. at 19.

²⁵ Slip op. at 29.

²⁶ Slip op. at 25.

²⁷ *Omnibus Order* (statement of Commissioner O'Rielly) (emphasis in original).

²⁸ Slip op. at 30.

Caller ID spoofing and other illegal activities. The TCPA sought to prevent the use of specific equipment to engage in illegal and abusive conduct—random or sequential cold calling that tied up telephone networks, including emergency lines, and harassed consumers. The construction of ATDS suggested by the D.C. Circuit and supported by this testimony would categorically prohibit those abuses. At the same time, it would provide clear guidance to businesses on how they may lawfully communicate with their customers.

The fact that the D.C. Circuit’s preferred definition of ATDS does not cover as much equipment as the definition the court struck down in no way means that consumers are unprotected, or even less protected. The TCPA contains within itself the means of protection: the Do Not Call list. Any consumer lawfully contacted by a business using equipment that is not an ATDS and who does not desire to be called may ask the caller to be placed on the caller’s company-specific Do Not Call list. Those consumers who proactively decide they do not want to receive calls—whether from an ATDS or not—may subscribe to the National Do Not Call List. Tens of millions of Americans already have.

V. Conclusion and Recommendations

As Congress and the FCC look for ways to reduce abusive robocalls, reforming the TCPA is an important step. Reducing the amount of unnecessary litigation plaguing legitimate businesses will shift the focus of enforcement to the actual bad actors who are the root cause of illegal robocalls. In this regard, ILR commends the FCC for taking action to give telephone companies the authority to use innovative solutions to block illegal robocalls. The D.C. Circuit has provided both an opportunity and a roadmap to further the FCC’s work of focusing resources at the root of the robocalling problem. Following that guidance will help businesses avoid burdensome litigation, restore the TCPA to its original purpose, and redirect resources and attention towards reducing abusive robocalls.

As previously proposed by ILR, the following updates to the TCPA should be taken under consideration.

Statute of Limitations: The TCPA contains no statute of limitations, and so has fallen into the four-year default, which makes no sense for calls/faxes that are supposedly invasions of privacy that the consumer knows about at the moment they are placed. Class actions reach staggering amounts of damages because class plaintiffs seek four years’ worth of calling data and liability. The TCPA’s time to bring suit should be reasonably limited, as is the case with the other Federal statutes providing private rights of action for statutory damages.²⁹

Capping Statutory Damages and Adding Provisions for Reasonable Attorneys’ Fees: Similar to every other Federal statute providing statutory damages and a private right of action to consumers to seek those damages, the TCPA should have a cap on the amount of individual and class action damages that can be sought.³⁰ There is no better way to curb litigation abuse, bring the TCPA in line with its sister statutes, and avoid unconstitutional and excessive fines for technical violations causing no actual harm.

Affirmative Defenses: As businesses are targeted for calls under Section 227(b), as well as for the 227(c) calls that Congress knew could be made in error by a business acting in good faith to follow the appropriate policies and procedures, the affirmative defenses available in Section 227(c) should also be imported into Section 227(b) to provide protection to businesses working in good faith to comply with the TCPA.

Capacity: The “capacity” of an ATDS should be interpreted for past calls as written in the text of the statute, meaning only those devices that have the actual ability to randomly/sequentially dial telephone calls would be actionable. And if Congress wishes to limit some other sort of calling technologies or text messages, new and more precise language should be drafted, vetted, and implemented after a notice period to companies so that they can comply with statutory requirements.

²⁹ See, e.g., Electronic Funds Transfer Act (15 U.S.C. § 1693), Section 1693(m) (statute of limitations—1 year); Fair Debt Collection Practices Act (15 U.S.C. § 1692), Section 1692(k) (statute of limitations—1 year).

³⁰ See, e.g., Electronic Funds Transfer Act (15 U.S.C. § 1693), Section 1693(m); Fair Debt Collection Practices Act (15 U.S.C. § 1692), Section 1692(k); Truth in Lending Act (15 U.S.C. § 1631 et. al.), Section 1640; Fair Credit Reporting Act (15 U.S.C. § 1681 et. al.), Section 1681(o). (Several of these statutes also permit defendants to recover costs/fees when actions are shown to have been brought in bad faith.)

Reassigned or Wrongly-Provided Number: Businesses should not be punished via TCPA lawsuits when they, in good faith, call a customer-provided phone number that now belongs to a new party unless and until the recipient informs the caller that the number is wrong and the business has a reasonable time to implement that change in its records. (If, after that notice and reasonable time the company continues to call, then lack of prior consent would be established for future calls.)

Vicarious Liability: The FCC has interpreted the TCPA to allow “on behalf of” liability for prerecorded/autodialed calls, something not specifically provided for in the statute. Among other things, the TCPA should be revised to define any such vicarious liability so that it would exist only against the appropriate entities—those persons who place the calls, or who retain a telemarketer to place calls, or who authorize an agent to place calls on their behalf.

Bad Actors: The TCPA should be reformed to focus on the actual bad actors (*i.e.*, fraudulent calls from “Rachel from Cardmember Services,” with spoofed numbers in Caller ID fields to hide the identity of caller), instead of companies trying to contact their consumers for a legitimate business purposes.

Address New Technologies, Such As Text Messaging: A text message is not the same as a call, and courts are wrong in treating them equally. Should Congress wish to set rules on text messaging within the TCPA, it should do so through the regular channels of drafting, vetting, and implementing new statutory language.

Revocation: If a consumer that has provided a telephone number to a company no longer wishes to receive communications at that number, there should be a set process (as in the Fair Debt Collection Practices Act) on how the business should be told of the revocation, and a reasonable time for the company to implement that change.

The changes discussed above—which would help to protect American companies from expensive and damaging litigation abuse—would not risk any of these repercussions. Thus, we urge this Committee to revisit the TCPA to bring this 20th Century statute in line with 21st Century challenges. Twenty-five years have passed, and it is evident that the TCPA has had a negative impact on businesses that Congress never intended when first enacting this law in 1991. We appreciate the Committee’s calling of today’s hearing and stand ready to work with you on this important issue.

Thank you for the opportunity to testify. I look forward to answering your questions.

The CHAIRMAN. Thank you, Mr. Delacourt.
Ms. Saunders.

**STATEMENT OF MARGOT FREEMAN SAUNDERS, SENIOR
COUNSEL, NATIONAL CONSUMER LAW CENTER**

Ms. SAUNDERS. Chairman Thune, Senator Blumenthal, and members of the Committee, thank you for inviting me to testify today. I am here on behalf of the National Consumer Law Center’s low-income clients as well as six other national consumer advocacy groups.

My testimony, my written testimony, begins with a story of a woman in Florida who received over 1,800 calls from Conns Appliances. She was repeatedly—she repeatedly requested that these calls stop, and she was repeatedly bombarded with continued calls. At the end of the testimony, there’s a calendar that shows that these 1,800 calls were made over a few months, including six or seven calls often daily on weekends. She—Conns—she was actually behind, but she was making her payments on the appliances.

I start with that because one of the main points that I want to make today is that robocalls that are scams are significantly a problem, but they are not by any means the only problem that consumers are dealing with.

On page 3 of my testimony, I show that the number of—one of the problems is simply that the number of robocalls is escalating tremendously. We start from less than a billion calls a month in September 2015 to now over 3 billion robocalls a month in March 2018. That's one of the primary callers—primary reasons that we have this problem.

But we also know, if you look at Table 2 on page 4 of my testimony, who the robocallers are. The top 20 robocallers include two scammers and 17 other callers, 15 of whom are debt collectors and are not covered by the Federal Fair Debt Collection Practices Act, so that the only law that protects consumers from the onslaught of these callers is the Telephone Consumer Protection Act.

But debt collection calls are not the only problem. In Table 3 of my testimony, I show what the types of calls are. About 28 percent are alerts and reminders, and as pointed out by other members of this panel, many of those calls are wanted by consumers, and the ability to consent and revoke is a very valuable tool for consumers because they want to be able to consent to reminders from their doctors and their pharmacies about health care matters.

But the rest of the calls in that list, payment reminders, which is a euphemism for debt collectors, telemarketing, and scams, are generally unwanted calls and are rejected by consumers. And consumers very much need the ability to not only consent, but also to revoke consent, and much of the robocallers' position legally these days is that consumers, once they have consented, no longer have the ability to revoke that consent, and that is a critical piece of the Telephone Consumer Protection Act that was affirmed by the D.C. Circuit and needs to be maintained by the FCC.

Later in my testimony I go through example after example of telemarketing calls that are—that were only addressed, not by public enforcement, but by private class actions. For example, *Robertson v. Navient Solutions*, Navient called Ms. Robertson 667 times, over 500 of which were after she requested they—she—they stop calling.

Telemarketers remain a real problem, and these are not scammers, these are telemarketers selling real products. On page 8, there's an example of a case brought against Mortgage Investors Corporation for 64 million illegal telemarketing calls. This was a class action that stopped the caller and resulted in payment to all of the people who were harmed. The autodialer—the mechanism here was an autodialer with a human agent on the other end.

Smith v. State Farm was another telemarketing litigation that was a class action that was only resolved by class actions. On Table 4 on page 10, I point out that while TCPA lawsuits have gone up, they've gone up in far less—a far lower proportion to the number of complaints and the number of robocalls that has escalated.

We have suggestions at the end of the testimony for how the FCC should proceed. And I'm happy to answer any questions.

Thank you.

[The prepared statement of Ms. Saunders follows:]

PREPARED STATEMENT OF MARGOT FREEMAN SAUNDERS, SENIOR COUNSEL, NATIONAL CONSUMER LAW CENTER, ON BEHALF OF THE LOW-INCOME CLIENTS OF THE NATIONAL CONSUMER LAW CENTER; AMERICANS FOR FINANCIAL REFORM, CONSUMER FEDERATION OF AMERICAN, NATIONAL ASSOCIATION OF CONSUMER ADVOCATES, PUBLIC CITIZEN, PUBLIC KNOWLEDGE AND U.S. PIRG

Chairman Thune, Senator Nelson, and Members of the Committee, I appreciate the opportunity to testify today on the importance of maintaining the integrity of the Telephone Consumer Protection Act (TCPA) for consumers. I provide my testimony here today on behalf of the low-income clients of the *National Consumer Law Center*¹ (NCLC), *Americans for Financial Reform*, *Consumer Federation of American*, *National Association of Consumer Advocates*, *Public Citizen*, *Public Knowledge* and *U.S. PIRG*.

I. The Scope of the Robocall Problem

Unwanted robocalls are an invasion of privacy. As was forcefully stated by Senator Hollings, the TCPA's sponsor, "[c]omputerized calls are the scourge of modern civilization. They wake us up in the morning; they interrupt our dinner at night; they force the sick and elderly out of bed; they hound us until we want to rip the telephone right out of the wall."² I speak today for the 4.5 million Americans who complained last year about the barrage of unwanted robocalls we all receive.

Let me tell you about just one case, which is typical of so many:

Tonya Stevens of Tampa, Florida purchased some appliances from Conns Appliances, Inc., a Texas company, in late 2014. Although she was making her payments, they were not always on time. Nevertheless, over the next *fourteen months Conns called Ms. Stevens on her cell phone 1,845 times, over one hundred times a month, often as much as eight or nine times a day.*³ These calls were made despite Ms. Stevens' repeated requests that Conns' agent stop calling. During one call, she said, "I am at my grandmother's death bed, quit calling." Conns' position is that once Ms. Stevens provided consent to be called on her cell phone she could never revoke that consent.

This case is emblematic of the problem Americans are facing with robocalls. The calls are unrelenting. The callers will not stop, despite consumers' pleas. The Federal Trade Commission's (FTC) "Biennial Report to Congress"⁴ reveals a surge in consumer complaints about robocalls in 2017, with *4.5 million complaints filed in 2017* compared to 3.4 million in 2016. This rise in complaints is consistent with an increased use of intrusive and disruptive robocall technology. But the problem is far worse than the FTC's complaint numbers show. Industry data shows that over two *billion* robocalls are made *every month*, many of which are unwanted and illegal. Over **3 billion** robocalls were made just in February 2018. Robocalls increased from 831 million in September 2015 to 3.2 billion in March 2018—a 285 percent increase in less than three years.

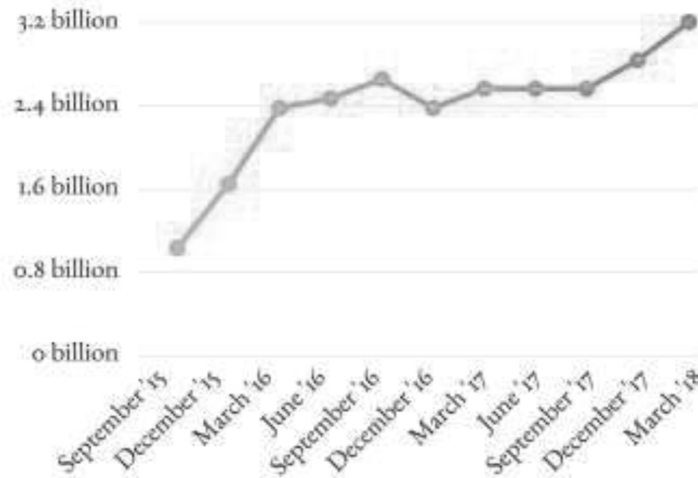
¹The *National Consumer Law Center* (NCLC) is a non-profit corporation founded in 1969 to assist legal services, consumer law attorneys, consumer advocates and public policy makers in using the powerful and complex tools of consumer law for just and fair treatment for all in the economic marketplace. NCLC has expertise in protecting low-income customer access to telecommunications, energy and water services in proceedings at state utility commissions, the FCC and FERC. We publish and annually supplement nineteen practice treatises that describe the law currently applicable to all types of consumer transactions, including *Access to Utility Service* (5th ed. 2011), covering telecommunications generally, and *Federal Deception Law* (3d ed. 2017), which includes a chapter on the Telephone Consumer Protection Act. This testimony was prepared with the substantial assistance of Carolyn Carter and Stephen Rouzer.

²137 Cong. Rec. 30,821–30,822 (1991) (also quoting Justice Brandeis, in *Olmstead v. U.S.*, 277 U.S. 438, 479, 48 S. Ct. 564, 72 L. Ed. 944 (1928), declaring "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men"). See also S. Rep. 102–178, at 5 (1991), reprinted in 1991 U.S.C.A.N. 1968, 1972–1973 ("The Committee believes that Federal legislation is necessary to protect the public from automated telephone calls. These calls can be an invasion of privacy, an impediment to interstate commerce, and a disruption to essential public safety services."); 137 Cong. Rec. S18781–02 (quoting Sen. Hollings as stating "These calls are a nuisance and an invasion of our privacy."); *Mims v. Arrow Fin. Services, L.L.C.*, 565 U.S. 368, 370 132 S. Ct. 740, 181 L. Ed. 2d 881 (2012) (noting that the TCPA "bans certain practices invasive of privacy").

³As this case is in arbitration, there is no formal complaint. However, Appendix 1 is a calendar showing the number of times these calls were made each day and each week.

⁴https://www.ftc.gov/system/files/documents/reports/biennial-report-congress-under-do-not-call-registry-fee-extension-act-2007-operation-national-do-not/biennial_do_not_call_report_fy_2016-2017_0.pdf

Table 1
Monthly Number of Robocalls



Congress passed the Telephone Consumer Protection Act⁵ (TCPA) in 1991 in direct response to “[v]oluminous consumer complaints about abuses of telephone technology—for example, computerized calls dispatched to private homes.”⁶ Yet 27 years later, the problem is only growing worse. The complaints are still pouring in. Private litigation and public enforcement have not kept pace with the problem—both the number of calls and the number of complaints by consumers increase every month. Robocalls are very inexpensive to make. Callers can discharge tens of millions of robocalls over the course of a day at only a penny per call.⁷

A. Who Is Making These Calls?

The problem of abusive, unwanted robocalls is not limited to scam calls. Scam calls—calls that are selling products or services they do not intend to provide, or that are pretexts for identity theft—are only one small part of the invasive robocall problem in the United States.

We know who is making robocalls because call-blocking technologies track the identity of callers. The Robocall Index created by one call-blocking app provider, YouMail, identifies the biggest robocallers every month.⁸ The biggest robocallers are not scammers; scammers actually account for only a small fraction of the robocalls to consumers in the United States. In March of 2018, only two scam callers (those marked in bold in Table 2, below) made the list of the top 20 sources of robocalls. Banks, credit card companies, retailers, and debt collectors, all of whom were collecting debts according to the robocall blocker, took 17 of the top 20 spots.

⁵ 47 U.S.C. § 227.

⁶ *Mims v. Arrow Fin. Servs., LLC*, 565 U.S. 368, 370–371 132 S. Ct. 740, 181 L.Ed. 2d 881 (2012).

⁷ See, e.g., Robodial.org, which costs 1 cent a call for calls up to 15 seconds, at <https://www.robodial.org/instantpricequote/> (last accessed Apr. 12, 2018); Call-Em-All Pricing, which quotes pricing from a high of 6 cents per call to \$7.50 per month “for one inclusive monthly fee. Call and text as much as you need.” <https://www.call-em-all.com/pricing> (last accessed Apr. 12, 2018).

⁸ The existence of these third-party call-blocking technologies does not fully address the problem. Unfortunately, many consumers do not use them. Moreover, many consumers, particularly traditional landline users, lack access to effective robocall-blocking tools.

Table 2—Top Twenty Robocallers in the United States March 2018⁹

1. Capital One	8. <i>Loan scam</i>	14. Barclaycard
2. <i>Portfolio Recovery Associates</i> (debt collection)	9. AT&T	15. First Premier Bank
3. Wells Fargo	10. <i>Enhanced Recovery Corporation</i> (debt collection)	16. PayPal
4. Santander	11. Fingerhut	17. Chase Bank
5. <i>A health insurance scam</i>	12. <i>Transworld Systems (debt collec- tion)</i>	18. Chase Bank (alternate num- ber)
6. Comcast	13. <i>Encore Receivables Management</i> (debt collection)	19. Kohl's
7. Job availability call (substitute teachers)		20. Citibank

By no means do I intend to minimize the problem with scam calls. They are a real problem that must be dealt with. But they are also not, by any measure, the entire problem. In the first two months of 2018, *scam calls accounted for only a quarter of all robocalls*:

Table 3—Estimated National Robocalls By Type¹⁰

Category	January	February
Alerts and Reminders	27%	28%
Payment Reminders	33%	32%
Telemarketing	15%	16%
Scams	25%	24%

This list of robocallers begs the question of which calls are objected to by consumers. We know the answer from the developers of one of the leading robocall-blocking apps: YouMail's Robocall Blocker.¹¹ All of the calls in the bottom two categories—Telemarketing and Scams—are routinely blocked by users of the call-blocking program.¹² Very few of the calls in the first category—Alerts and Reminders—are blocked. Most of the calls in the second category—Payment Reminders (which is a polite characterization for the debt collection callers)—are blocked by their recipients.¹³

B. Debt Collection Robocalls are a Huge Problem That Often Only the TCPA Can Address

As can be surmised from the huge number of debt collection robocalls made in the U.S., one third of all American consumers have accounts in collection.¹⁴ Indeed ACA International, “a trade group located in the United States representing collection agencies, creditors, debt buyers, collection attorneys and debt collection industry service providers,”¹⁵ has been a primary driver of efforts before the Federal Communications Commission (FCC) to roll back the consumer protections in the TCPA¹⁶ both prior to and after the FCC's 2015 Omnibus Order.¹⁷ This organization was also, of course, the lead petitioner in the appeal of the FCC's pro-consumer order issued in 2015, which led to the recent decision of the D.C. Circuit Court in *ACA International v. F.C.C.*¹⁸

⁹ See YouMail Robocall Index, available at <https://robocallindex.com/> (last accessed Apr. 12, 2018). To come up with the names of the callers, we simply called the numbers listed on the website to see who answered.

¹⁰ Press Release, YouMail, YouMail Releases Detailed Breakdown of U.S. Robocalls in February (Mar. 21, 2018), available at <https://www.prnewswire.com/news-releases/youmail-releases-detailed-breakdown-of-us-robocalls-in-february-300616969.html> (last accessed Apr. 12, 2018).

¹¹ See <https://www.youmail.com/home/feature/stop-robocalls> (last accessed Apr. 12, 2018).

¹² This information was provided by Alex Quilici, CEO of YouMail, on March 28, 2018.

¹³ *Id.*

¹⁴ See Urban Institute, Debt in America: An Interactive Map (last updated Apr. 5, 2018), available at <https://apps.urban.org/features/debt-interactive-map/> (last accessed Apr. 12, 2018).

¹⁵ https://en.wikipedia.org/wiki/ACA_International.

¹⁶ See e.g., ACA International, Petition for Rulemaking of ACA International (filed Feb. 11, 2014), available at <https://ecfsapi.fcc.gov/file/7521072801.pdf>.

¹⁷ *In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order, 30 FCC Rcd. 7961 (F.C.C. July 2015) [hereinafter 2015 TCPA Omnibus Order].

¹⁸ 885 F.3d 687 (D.C. Cir. 2018).

It is a common misconception that the Federal Fair Debt Collection Practices Act¹⁹ (FDCPA) provides sufficient protections for consumers against invasive and abusive debt collection calls. Unfortunately, that is the not case, for several reasons. The primary reason is that the FDCPA does not cover collection efforts made by creditors to collect their own debts; it covers only third-party debt collectors—those collecting debts originally owed to others.²⁰ So of the 20 top robocallers listed in Table 2, only four (those whose names are in italics) were even covered by the FDCPA. Debt collection calls by all of the remaining robocallers were not covered by the FDCPA because they were collecting their own debts.

This leaves the TCPA as the principal Federal law providing protections against harassing and unrelenting debt collection calls to consumers' cell phones. Below are just a few examples of the significance of the problem of debt collector robocallers. All of these cases are recent; all involve hundreds—if not thousands—of calls; and all involve multiple calls after repeated requests from the consumer to stop calling:

1. *Robertson v. Navient Solutions*.²¹ Shortly after Ms. Robertson acquired a Certified Nursing Assistant certificate, which she had funded with student loans, she experienced health problems and, also, had to care for her dying father. She was unable to work, and applied for disability. She received a forbearance on her Federal student loans, but not for the private loans. Ms. Robertson made payments when she was able. However, payments did not stop the calls. *In total, Navient called Ms. Robertson a total of 667 times, and called 522 times after she told them to stop calling.* Navient would call back the same day even when Ms. Robertson would tell the collection agent that she would not have any money to pay until the following month.
2. *Gold v. Ocwen Loan Servicing*.²² The plaintiff consented to being contacted about his mortgage debt, and answered several collection calls, but then asked for the calls to stop. However, the servicer *called his cell phone at least 1,281 times between April 2, 2011 and March 27, 2014, after the repeated requests to stop.*
3. *Montegna v. Ocwen Loan Servicing*.²³ The servicer called the plaintiff on his cell phone at least 234 times, even after he requested that the calls stop.
4. *Todd v. Citibank*.²⁴ Some time in January 2016, the bank began calling the plaintiff's cell phone. The calls, *often made twice a day, totaled 350 calls*, even after repeated requests to stop calling. "The purported injury here is Plaintiff's 'privacy, peace, and quiet' was disturbed by the numerous telephone calls."²⁵

C. Real Telemarketers Are Making Many of the Unwanted Robocalls

Telemarketing calls are also the source of millions of unwanted, and illegal, robocalls. Telemarketers with real products to sell (car insurance, home security networks, even marketing an independent film) bombard consumers' homes and cell phones with illegal robocalls. It is important to note that "real" telemarketing calls, often with a human caller at the other end of the phone, are not scammers. Their caller IDs are sometimes—although not always—truthfully displayed. So addressing scams and spoofing will not deal with these maddening and invasive—and illegal—calls.

Often a single consumer is hounded by persistent telemarketing calls from the same company.²⁶ With many telemarketing campaigns, however, the campaign will make millions of illegal calls, but only one or two to any given consumer. The only effective way to enforce the TCPA's protections against these illegal calls is through public enforcement or private class actions.

That is because the TCPA allows a consumer to recover only \$500 to \$1500 per call, and does not require the defendant to reimburse the consumer for the attorney fees incurred to prosecute the case. As a result, individual suits regarding just one or two calls are not economically feasible. (And a million individual suits for a million-robocall campaign would overwhelm the court system in any event).

¹⁹ 15 U.S.C. § 1692.

²⁰ 15 U.S.C. § 1692a(6).

²¹ *Robertson v. Navient Solutions, Inc.*, Case No.: 8:17-cv-01077-RAL-MAP (M.D. Fla. filed May 8, 2017).

²² 2017 WL 6342575 (E.D. Mich. Dec. 12, 2017).

²³ 2017 WL 4680168 (S.D. Cal. Oct. 18, 2017).

²⁴ 2017 WL 1502796 (D.N.J. Apr. 26, 2017).

²⁵ *Id.* at *8.

²⁶ *See, e.g., Jenkins v. MGage, L.L.C.*, 2016 WL 4263937 (N.D. Ga. Aug. 12, 2016) (individual action challenging 150 text messages promoting events at a nightclub despite 17 requests to stop).

One example of a particularly intrusive telemarketing campaign is the case of *Golan v. Veritas Entertainment*, decided by a Federal court in Missouri in 2017.²⁷ In its efforts to market a political film, the company made so many calls in violation of the TCPA—over 3.2 million calls—that the judge ordered the statutory damages award reduced to just \$10 per call. If he had stuck with \$500 per call, the total would have been \$1.6 billion, which he held to be so disproportionate as to violate due process. In reducing the award, the court noted:

This reflects the severity of the offense, a six-day telemarketing campaign which placed 3.2 million telephone calls, as well as respecting the purposes of the TCPA to have a *deterrent effect and to account for unquantifiable losses including the invasions of privacy, unwanted interruptions and disruptions at home, and the wasted time spent answering unwanted solicitation calls or unwanted voice messages*.²⁸

This sentiment was emphasized in another large class action case, *Krakauer v. DISH Network*,²⁹ in which the court refused to unwind the jury's award of \$400 per call, trebled by the court, for each of 51,000 telemarketing calls. The court pointed out:

It is not 'grossly excessive' to require Dish to pay treble damages for the more than 50,000 willful violations it committed, given the nature of the privacy interests repeatedly invaded and Dish's continuing disregard for those interests, the extent of the violations, and the need to advance reasonable governmental interests in deterring future violations.³⁰

The court went on to treble the damages awarded by the jury, which the court found appropriate here in light of the seller's "sustained and ingrained practice of violating the law," and the need for deterrence.³¹

Below are just a few examples of pending or resolved class action lawsuits that used the TCPA to obtain redress for consumers for *tens of millions of illegal robocalls*:

1. *Ott v. Mortgage Investors Corp.*³² In this case, which settled in 2016, there were over 64 million illegal telemarketing calls made to millions of veterans to convince them to refinance their VA loans. The consumers reported receiving dozens of unwanted calls from the defendant, who repeatedly failed to remove their telephone numbers from its call list upon demand. The defendant's telemarketing efforts were so aggressive that thousands of consumers filed complaints with the FTC and other agencies regarding the unwanted and harassing telemarketing calls. The technology used was an autodialer with a human agent.
2. *Strache v. SCI Direct, Inc.*³³ This class action involved over four million calls made by a company selling cremation services. One of the consumers kept receiving these calls, even after sending e-mails, calling back and requesting that the calls stop, and filing an FTC complaint.
3. *Smith v. State Farm Mutual Ins. Co.*³⁴ This class action was filed after a marketing company made 350 million phone calls to consumers from a list of numbers it found in the White Pages. During each call, a recording instructed recipients to "press 1 now" for a better deal on auto insurance. Recipients who pressed 1 were transferred to a live "screener," who asked questions and then transferred the call to insurance agents, including agents for State Farm Mutual Automobile Insurance Company. The calls resulted in leads to State Farm agents for at least 62,827 unique cell phone numbers. State Farm agents continued to employ the marketers' services for over six months after the lawsuit was brought.

²⁷ 2017 WL 3923162 (E.D. Mo. Sept. 7, 2017).

²⁸ *Id.* at *4 (emphasis added).

²⁹ 2017 WL 4417957 (M.D.N.C. Oct. 3, 2017).

³⁰ *Id.* at *11 (M.D.N.C. Oct. 3, 2017) (emphasis added). See also *U.S. v. DISH Network*, 256 F. Supp. 3d 810 (C.D. Ill. 2017) (similar case brought against Dish Network by the United States, as well as the states of California, Illinois, North Carolina and Ohio; the court ordered DISH to pay a civil penalty of \$168,000,000 "for Dish's violation of the TSR done with knowledge or knowledge fairly implied," plus statutory damages of \$84,000,000).

³¹ *Krakauer v. DISH Network, L.L.C.*, 2017 WL 2242952, at *12–*13 (M.D.N.C. May 22, 2017).

³² *Ott v. Mortg. Investors Corp. of Ohio*, 65 F. Supp. 3d 1046 (D. Or. 2014).

³³ Case No. 1:17-cv-04692 (N.D. Ill.); original case was *Allard v. SCI Direct, Inc.*, Case No. 3:16-cv-01033 (M.D. Tenn.).

³⁴ Case No. 1:13-cv-02018 (N.D. Ill.).

4. *Holtzman v. Turza*.³⁵ This case involved 8,430 junk faxes sent by an attorney who was advertising his law practice to CPAs. The defendant litigated the case for over ten years, until the Seventh Circuit Court of Appeals put a stop to it.³⁶

II. Class Actions are Not the Problem

Robocallers like to point to the numbers of class actions as fodder for their claim that TCPA rules are out of control. Class actions regarding TCPA violations have increased over the past several years, but they have not increased nearly as dramatically as the number of robocalls has increased. The annual number of robocalls increased from 14 billion in 2015 to 30 billion in 2017, a 115 percent increase in just three years—see Table 4. (And the steep climb in the number of robocalls per month is even more alarming, as that number has increased 285 percent from September 2015 to March 2018. Even if the monthly rate does not increase beyond March’s total of 3.2 billion, we will see 38.4 billion robocalls this year).

The number of complaints to government agencies has also increased dramatically—a 100 percent increase during the same three-year period, from 3.5 million to 7.1 million.³⁷ Yet the number of TCPA lawsuits *of all types*—both class actions and individual actions—increased only 19 percent, from 3687 in 2015 to 4392 in 2017. The key point is that robocalls are rapidly increasing, which is clearly upsetting the Americans subjected to them.

Table 4—Comparing Lawsuits to Complaints to Robocall Numbers

	TCPA Lawsuits Filed ³⁸	Complaints to FTC & FCC ³⁹	Total Number of Robocalls in U.S. ⁴⁰
2015	3687	3,578,710	14,214,000,000
2016	4860	5,340,234	29,300,000,000
2017	4392	7,157,370	30,500,000,000

Class actions serve a critical role in deterring robocallers from violating the law as well as protecting consumers from TCPA violations. Without class actions there would be little incentive for callers to comply with the TCPA. As is evident from the comparison of the number of complaints filed by consumers with the FTC and the FCC, and the number of cases actually filed, only a tiny proportion of complaints actually mature into real lawsuits. As there are no fee-shifting provisions in the TCPA, the economics of bringing litigation under the TCPA require that there be significant numbers of violations (multiples of the \$500 statutory damages) before litigation regarding even the most blatant violations is feasible. These cases are time-consuming to litigate and they require expensive expert witnesses to prove the claims. The lawyers who bring these cases benefit from them—but only if they successfully prove the elements of the claims under the TCPA. That is why private enforcement is an effective mechanism of enforcing a consumer protection statute.

When cases settle, the unnamed class members typically receive a portion of what they would have been entitled to had the case proceeded to final judgment. That is why the cases settle—so that the defendants do not have to pay as much as they might if the case was litigated through to judgment. The compensation for the attorneys who handled the case for the consumers must be approved by the court and depends on the benefit they achieved for the consumers, so they have the incentive to get the best settlement possible for the class.

Consumers who are not members of the class also benefit from class actions, whether the actions are settled or resolved only after trial. Class actions provide a

³⁵ 728 F.3d 682 (7th Cir. 2013).

³⁶ ABA Journal, *7th Circuit rejects another appeal by lawyer ordered to pay up to \$4.2M for sending junk faxes*, Nov. 16, 2017, available at http://www.abajournal.com/news/article/7th_circuit_rejects_another_appeal_by_lawyer_ordered_to_pay_up_to_4.2m_for/.

³⁷ Growth calculated through analysis of 2015 and 2017 figures. Federal Trade Commission, National Do Not Call Registry Data Book FY 2017, at 6, (Dec. 2017), available at https://www.ftc.gov/sites/default/files/filefield_paths/dnc_data_book_fy2017.pdf (last accessed Apr. 14, 2018).

³⁸ WebRecon, *Web Recon Stats for Dec 2017 & Year in Review*, available at <https://webrecon.com/webrecon-stats-for-dec-2017-year-in-review/> (last accessed Apr. 14, 2018).

³⁹ See Federal Trade Commission, National Do Not Call Registry, *supra* note 37.

⁴⁰ 2016 and 2017 numbers derived from the sum of monthly totals. YouMail Robocall Index, *supra* note 9. The 2015 number is derived from the average number of calls in the six months for which totals are provided. *See id.*

much-needed deterrent effect against violating the TCPA, which limits the number of unwanted calls and texts to cell phones for the rest of us.

In dissenting from the FCC's 2015 Omnibus Order,⁴¹ Chairman (then Commissioner) Pai and Commissioner O'Rielly cited several TCPA cases that they felt were meritless. But this is not a reason to weaken the TCPA. With the exception of just one case (the *Rubio* case, discussed below), *the courts dismissed those cases*. In other words, our justice system, while not perfect, does a reliable job of weeding out meritless or abusive cases. For example:

1. *Emmanuel v. Los Angeles Lakers, Inc.*,⁴² mentioned by Commissioner Pai in his dissent.⁴³ In this case, the plaintiff attended a Lakers game during which attendees were invited to send a text message to a specified telephone number for the opportunity to have the message appear on the scoreboard. After the plaintiff sent the Lakers a text message, he received a confirmatory text back. He then sued, alleging that this confirmatory text violated the TCPA's prohibition against sending a consumer a text message without the consumer's prior consent.

The District Court granted the Lakers' motion to dismiss with prejudice. Taking a "common sense" approach, the court held that the challenged text message was not actionable under the TCPA. By sending his original message, the plaintiff expressly agreed to receive a return confirmatory text. This confirmatory text was not the type of intrusive communication prohibited by the TCPA because it responded directly to the plaintiff's original text.

2. *Gragg v. Orange Cab Co., Inc.*,⁴⁴ mentioned by Commissioner Pai in his dissent.⁴⁵ After the plaintiff requested a taxi, the dispatcher manually inputted pertinent information, and pressed "enter" to transmit the data to TaxiMagic to reach the nearest available driver. A driver transmitted his acceptance of the request by pressing "accept" on his Mobile Data Terminal and then sent the plaintiff a message that read "Taxi # 850 dispatched @ 05:20." The plaintiff brought a class action suit alleging that the text message violated the TCPA as it was made with an autodialer without prior express consent.

*The court rejected the plaintiff's argument that the modem utilized by defendants to operate the TaxiMagic program was a "system" as envisioned by TCPA precedent: "The Court declines to adopt an interpretation of 'system' that would lead to an absurd result."*⁴⁶ The court entered summary judgment against the consumer on the TCPA claim.

3. *Kinder v. Allied Interstate, Inc.*,⁴⁷ mentioned by Commissioner Pai in his dissent.⁴⁸ Soon after acquiring a pager number (619-999-9999), the plaintiff realized that it was receiving thousands of unwanted pages that were not meant for him. He then disconnected the pager, but recorded all the calls made to it and filed many suits regarding them. The appellate court affirmed the trial court's finding that the plaintiff intentionally subjected himself to unwanted calls and that, as a matter of policy, *this conduct precluded any recovery under the TCPA*.⁴⁹

Both Commissioners Pai and O'Rielly also cited the case of Rubio's Restaurant, which was sued for repeatedly calling a reassigned number, relying on the called party's statements that it had blocked the calls.⁵⁰ Rubio's then filed a petition with the FCC requesting that a bad faith defense be allowed for TCPA claims. The FCC denied the request in the 2015 Omnibus Order, pointing out that once the caller affirmatively knew that the number was no longer assigned to the person from whom it had consent, it was incumbent on the caller to stop the calls.⁵¹

⁴¹ 2015 TCPA Omnibus Order, *supra* note 17.

⁴² Case no. 2:12-cv-09936-GW-SH (C.D. Cal. Apr. 18, 2013).

⁴³ 2015 TCPA Omnibus Order, *supra* note 17, at 8072 (Pai, Comm'r, dissenting).

⁴⁴ 995 F. Supp. 2d 1189 (W.D. Wash. 2014).

⁴⁵ 2015 TCPA Omnibus Order, *supra* note 17, at 8072 (Pai, Comm'r, dissenting).

⁴⁶ 995 F. Supp. 2d 1189, 1192 (W.D. Wash. 2014) (emphasis added).

⁴⁷ 2010 WL 2993958 (Cal. Ct. App. Aug. 2, 2010).

⁴⁸ 2015 TCPA Omnibus Order, *supra* note 17, at 8072 (Pai, Comm'r, dissenting).

⁴⁹ 2010 WL 2993958, at *8 (Cal. Ct. App. 2010). *See also Epps v. Earth Fare, Inc.*, 2017 WL 1424637 (C.D. Cal. Feb. 27, 2017) (dismissing case as "manufactured" lawsuit where plaintiff purported to revoke consent to receive commercial text messages by responding with long sentences rather than simply responding with the STOP command, as instructed in each message).

⁵⁰ Rubio's Restaurant, Inc., Petition for Expedited Declaratory Ruling, CG Docket No. 02-278 (filed Aug. 15, 2014), available at <http://apps.fcc.gov/ecfs/document/view?id=7521768526>.

⁵¹ 2015 TCPA Omnibus Order, *supra* note 17, at 8012.

Indeed, without ensuring that callers have the obligation to update records regarding reassigned numbers, there would be no meaningful enforcement of the TCPA's proscription against robodialing numbers without consent. Hopefully, the FCC's pending proposal to establish a reassigned number database⁵² will resolve most, if not all, of the challenges relating to reassigned numbers.

The potential of class action lawsuits benefits not only consumers, but also businesses that want to comply with the law. Without the threat of class action lawsuits, their competitors would violate the law with little fear of consequences, putting the law-abiding business at a competitive disadvantage. The deterrent effect of class actions protects millions of consumers from receiving unwanted—and unconsented to—calls and texts to their cell phones on a daily basis. Courts are quite capable of ferreting out meritless TCPA lawsuits.

III. The Impact of the D.C. Circuit Court's Decision in *ACA International v. FCC*⁵³

On March 16, 2018, the D.C. Circuit issued its long-awaited decision in *ACA International v. FCC*,⁵⁴ an appeal filed by debt collectors and a number of other industry players from the 2015 Omnibus Order issued by the FCC.⁵⁵ *ACA International* addresses three major issues:

- The definition of “automatic telephone dialing system” (ATDS);
- Caller liability for calls to reassigned numbers; and
- The right of consumers to revoke consent to receive robocalls.

The TCPA prohibits the use of an autodialer (the statute uses the term “automated telephone dialing system” or ATDS) to call a cell phone without the called party's consent.⁵⁶ This prohibition is critically important to consumers, as it is the primary bulwark against the tsunami of unwanted calls that would otherwise flood their phones.

The TCPA defines autodialer as equipment that has the capacity to store or produce telephone numbers to be called, using a random or sequential number generator, and to dial such numbers.⁵⁷ The FCC has interpreted this definition on several occasions.

In 2003, the FCC held that a device cannot be excluded from the definition because it dials from a given set of numbers rather than from randomly or sequentially generated numbers.⁵⁸ That ruling also holds that a predictive dialer is an autodialer, reasoning that, like earlier autodialers, the basic function of a predictive dialer is the capacity to dial numbers without human intervention. In 2008, the FCC issued another declaratory ruling reiterating that a predictive dialer is an autodialer.⁵⁹ Many decisions have held that these rulings are binding on courts.⁶⁰

⁵²*In re Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17–59, Second Further Notice of Proposed Rulemaking, 37 FCC Rcd. 56 (F.C.C. Mar. 2018), available at https://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0323/FCC-18-31A1.pdf.

⁵³NCLC has produced a comprehensive analysis of the decision in a memorandum entitled *The Effect of ACA International: What Does it Vacate, What Does it Undermine, What Rules Remain?* (Apr. 2, 2018), available at www.nclc.org.

⁵⁴885 F.3d 687 (D.C. Cir. 2018).

⁵⁵2015 TCPA Omnibus Order, *supra* note 17.

⁵⁶47 U.S.C. § 227(b)(1)(A)(iii).

⁵⁷47 U.S.C. § 227(a)(1). *See also* 47 C.F.R. § 64.1200(f)(2) (similar definition).

⁵⁸*In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02–278, Report and Order, 18 FCC Rcd. 14,014 (F.C.C. July 2003).

⁵⁹*In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02–278, Declaratory Ruling, 23 FCC Rcd. 559 (F.C.C. Jan. 2008).

⁶⁰*Zeidel v. A&M (2015) L.L.C.*, 2017 WL 1178150 (N.D. Ill. Mar. 30, 2017) (relying on FCC's 2003 order to hold that device that sends text messages *en masse* is ATDS regardless of whether it has capacity to generate numbers sequentially or randomly; device is ATDS if it stores pre-programmed numbers or receives numbers from a computer database, can dial those numbers at random in sequential order or from a database of numbers, and its basic function is the capacity to dial numbers without human intervention); *Espejo v. Santander Consumer USA, Inc.*, 2016 WL 6037625 (N.D. Ill. Oct. 14, 2016) (relying on 2003 order to hold that predictive dialer is an ATDS); *Brown v. Credit Mgmt., L.P.*, 131 F. Supp. 3d 1332 (N.D. Ga. 2015) (relying on 2003 and 2008 orders to hold predictive dialer an ATDS); *Swaney v. Regions Bank*, 2015 WL 12751706 (N.D. Ala. July 13, 2015) (text message sending system is ATDS because it has ability to dial numbers without human intervention); *Brown v. Account Control Tech., Inc.*, 2015 WL 11181947 (S.D. Fla. Jan. 16, 2015) (relying on 2003 and 2008 orders to hold that a predictive dialer is an ATDS; dismissing defendant's argument that predictive dialer is ATDS only if it has capacity to use random or sequential number generation); *Morse v. Allied Interstate, L.L.C.*, 65 F. Supp. 3d 407 (M.D. Pa. 2014) (2003 and 2008 orders are binding; predictive dialer that calls numbers without human intervention is ATDS); *Moore v. DISH Network L.L.C.*, 57 F.

Robocallers have not been happy with these rulings. They have sought to create equipment that automatically calls millions of numbers a day but that does not quite meet the statutory definition, and they have also repeatedly petitioned the FCC to issue a narrow definition of “autodialer.” In 2015, in response to the latest batch of petitions, the FCC issued another declaratory order that reiterated the conclusions of the 2003 and 2008 orders and added further interpretations.⁶¹ The 2015 order held that, whether or not a particular call was placed through random or sequential generation of telephone numbers, a system is an autodialer if it has the present or potential capacity to generate numbers in this way.⁶² The order also made it clear that “the TCPA’s use of ‘capacity’ does not exempt equipment that lacks the ‘present ability’ to dial randomly or sequentially.”⁶³ Thus hardware that can store or produce telephone numbers to be called using a random or sequential number generator is an autodialer even if software necessary to accomplish that functionality has not yet been installed.⁶⁴

The industry appealed the 2015 order,⁶⁵ and in 2018, in *ACA International v. Federal Communications Commission*,⁶⁶ the D.C. Circuit set aside the portions of the 2015 order that dealt with the definition of autodialer. The court’s main concern was that the FCC’s broad interpretation of the term “capacity” in the autodialer definition could sweep in smartphones that consumers were using for ordinary purposes. It sent this part of the order back to the FCC to redo.

While *ACA International* sets aside the portions of the FCC’s 2015 order that dealt with the definition of ATDS, it leaves in place the FCC’s 2003 and 2008 orders, which remain binding on the courts.⁶⁷ The D.C. Circuit’s decision thus rolls the clock back to 2014, before the FCC had issued the portions of its 2015 order that relate to the definition of an ATDS. Accordingly, the role of courts after *ACA International* should be to interpret the statute in light of the 2003 and 2008 FCC orders, the decisions of the Court of Appeals for their Circuit, and any decisions of other courts that have persuasive value, but without the benefit of the 2015 order on this point. In our view, discussed in length in our published analysis of the effect of *ACA International*,⁶⁸ most dialers used by robocallers still fall within the definition of autodialer.

In *ACA International*, the D.C. Circuit also addressed the question of reassigned cell phone numbers. Often callers have claimed that a barrage of calls is legal because the called party’s cell phone number was previously assigned to a consumer who had consented to the calls. Consumers have found these calls extremely difficult to stop. The FCC’s 2015 order made it clear that a caller has to have the consent of the person it actually calls, and that, when a telephone number is reassigned

Supp. 3d 639 (N.D. W. Va. 2014) (predictive dialer is ATDS even if it lacks capacity to generate random or sequential phone numbers and even though humans create the lists of numbers to be called); *Sterk v. Path, Inc.*, 46 F. Supp. 3d 813 (N.D. Ill. 2014) (relying on 2003 and 2008 orders; a predictive dialer is an ATDS; here, device that sends text messages to call list is ATDS even if it lacks capacity to generate numbers randomly or sequentially); *Davis v. Diversified Consultants, Inc.*, 36 F. Supp. 3d 217 (D. Mass. 2014) (relying on 2003 and 2008 orders to hold that predictive dialer is ATDS even if it does not have capacity for random or sequential number generation); *Lardner v. Diversified Consultants, Inc.*, 17 F. Supp. 3d 1215 (S.D. Fla. 2014) (relying on 2003 order and finding it reasonable; device is ATDS if it automatically dials numbers from a preprogrammed list); *Cabrera v. Gov’t Employees Ins. Co.*, 2014 WL 11881002 (S.D. Fla. Nov. 26, 2014) (relying on 2003 and 2008 orders to hold that any device that is able to dial numbers without human intervention, for example by calling numbers stored in a database, is an ATDS; LiveVox system is ATDS).

⁶¹*In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02–278, Report and Order, 30 FCC Rcd. 7961 ¶¶ 10, 23, 24 (F.C.C. July 10, 2015), *appeal resolved*, *ACA International v. FCC*, 885 F.3d 687 (D.C. Cir. 2018) (setting aside portions of FCC’s 2015 order dealing with ATDS definition and treatment of reassigned cell phone numbers).

⁶²*Id.* at ¶ 15.

⁶³*Id.*

⁶⁴*Id.* at ¶¶ 16, 18–20.

⁶⁵See National Consumer Law Center, Federal Deception Law § 6.2.4.3A (3d ed. 2017), *updated at* www.nclc.org/library.

⁶⁶885 F.3d 687 (D.C. Cir. 2018).

⁶⁷The D.C. Circuit’s brief references to the 2003 and 2008 FCC orders in *ACA International* do nothing to undermine the conclusion that the opinion decides only the validity of the 2015 order. Except for a brief mention of the 2003 order in an introductory section describing the FCC’s history of rulemaking and declaratory rulings, *ACA International* mentions the FCC’s 2003 and 2008 orders only in section II(A)(2). 885 F.3d at 701. That section first addresses the question whether the existence of the 2003 and 2008 orders deprives the D.C. Circuit of jurisdiction to entertain the challenge to the 2015 order. This was a necessary prerequisite for the court to address the 2015 order. For more discussion of this point, see NCLC’s memorandum on the impact of the decision, *supra* note 54, at § I.A.3.

⁶⁸See NCLC’s memorandum on the impact of the decision, *supra* note 54, at § I.A.3.

from one consumer to another, the caller must have the new consumer's consent. In addition, however, the FCC created a safe harbor for the first call to a reassigned number while imposing liability for calls after that first call. The D.C. Circuit held that, while the rationale for requiring the caller to have the consent of the person it actually called was "persuasive," the FCC had not articulated a good enough rationale for the one-call safe harbor, so it set aside the entire portion of the order dealing with liability for calls to reassigned numbers and sent it back to the FCC to redo.

The D.C. Circuit rejected the other challenges to the FCC's 2015 order. It agreed that the FCC's ruling that consumers have the right to revoke consent by any reasonable means was reasonable, and it rejected a pharmacy chain's argument that a narrow, carefully crafted exception from the consent requirement for time-sensitive health care messages should have been broader. It left all the other portions of the 2015 order undisturbed.

IV. A Plan for Dealing with Robocalls

American consumers want robocalls to stop. Callers want to continue calling, and they do not want to be sued. But most responsible callers agree that consumers should have some control over the calls they receive. The way to thread our way through this conundrum is for the FCC to develop clear rules to guide callers, to cover all truly automated calls (otherwise consumers will have no control), to ensure that consumers can clearly and easily revoke consent, and to give consumers the means to block calls they do not want.

The FCC, under Chairman Pai, has already launched some important initiatives to deal with unwanted robocalls. These include permitting phone companies to allow call blocking,⁶⁹ consideration of a comprehensive reassigned number database that will enable callers to check that they have consent from the current subscriber of the phone before calling,⁷⁰ encouraging phone companies to develop technologies that allow for reliable call authentication,⁷¹ and beginning the process of tightening regulations around caller ID spoofing.⁷²

But the first step must be to make sure that all of the invasive and unwanted calls are covered by the TCPA's consumer protections. This step involves ensuring that the TCPA's definition of an ATDS covers the automated calls being made. As explained in the previous section, we believe that if the FCC does nothing to change the existing law on the definition, then there is ample room for the courts to find that most autodialers currently being used are covered. But doing nothing to resolve the outstanding issues does not provide the clarity craved by responsible callers. And it would invite callers to continue trying to design equipment that barrages consumers with unwanted calls yet does not quite meet the definition of autodialer.

The TCPA requires consent for calls to cell phones that include either a prerecorded or artificial voice, or that are made with an autodialer (whether or not a human operator speaks to the consumer once the call is answered). As described in previous sections of this testimony, many of the worst calls about which consumers are now complaining are made with human operators and autodialers. Consumers would be substantially harmed if the FCC moved forward with a constricted definition of autodialer that excluded these calls. The definition of autodialer is central to coverage of the calls under the TCPA, not only for private enforcement, but for FCC enforcement as well.

Consider, for example, what happened in the case of *Dominguez v. Yahoo, Inc.*⁷³ In this case, Yahoo sent 27,809 *wrong number text messages* to Mr. Dominguez over 17 months. It refused to stop even after the consumer's many pleas, and even after he called a representative from the FCC, who then participated in a call (with Mr. Dominguez on the line) to Yahoo's customer service. Yahoo told Mr. Dominguez that the company could not stop the messages and that, as far as Yahoo was concerned, the number would always belong to the previous owner. Yahoo defended—and is

⁶⁹*In re Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Report and Order and Further Notice of Proposed Rulemaking, FCC 17-51 (F.C.C. Nov. 2017).

⁷⁰*In re Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Second Further Notice of Proposed Rulemaking, *supra* note 53.

⁷¹*In re Call Authentication Trust Anchor*, CG Docket No. 17-97, Notice of Inquiry, 32 FCC Rcd. 5988 (F.C.C. July 2017).

⁷²See Press Release, Federal Communications Commission, FCC Proposes \$82 Million Fine for Spoofed Robocalls (Aug. 3, 2017); Press Release, Federal Communications Commission, Robocall Scammer Faces \$120 Million Proposed Fine for Massive Caller ID Spoofing Operation (June 22, 2017).

⁷³629 Fed. Appx. 369 (3d Cir. 2015).

still defending⁷⁴—its actions by saying that that the equipment sending the messages did not fit the statutory definition for an ATDS. Without a broad definition of autodialer, companies will be able to continue to thumb their noses like this at both consumers and the FCC.

If the FCC were to adopt a limited definition, the following calls, even if made by automated equipment from a call center, would be outside the scope of the TCPA's protections for cell phones, and neither the U.S. Government nor consumers would have control over these calls.

- All texts to cell phones, since these do not use artificial voices. Consumers could try to put their cell phones on the FCC's Do Not Call list, but it applies only to residential phones, and only to telemarketing calls. The FCC has created something of a presumption that a cell phone is a residential phone, but this is not a universal rule.
- Telemarketing calls that avoid artificial or prerecorded voices, including scam telemarketing calls that use humans, such as the IRS scam calls ("Your computer has a virus," etc.). Consumers could register their cell phones on the FCC's Do Not Call list, but, as noted in the preceding bullet, all cell phones may not be protected by the Do Not Call list.
- Debt collection calls, as long as they avoid prerecorded or artificial voices.
- Unwanted autodialed calls to emergency rooms, hospitals, etc., if they do not use prerecorded or artificial voices.

Below is our proposal for the next steps that we believe the FCC should take to deal with illegal and invasive robocalls.

- 1) Cover all the calls to cell phones that are made with automated equipment.
 - This ensures that the FCC has authority over all problem calls;
 - Clarity of coverage will assist the calling industry; and
 - The statutory definition of ATDS provides ample room to do so (using either the language "store" numbers and "dial those numbers" or a broad definition of "capacity").
- 2) To prevent application of a broad definition to ordinary personal use of a smart phone, use the FCC's general authority to adopt rules implementing the TCPA to exclude equipment that *does not* routinely make *en masse* calls, possibly by:
 - More closely defining the call abandonment rate; and
 - Excluding equipment that does not have more than X abandoned calls.
- 3) Provide a safe harbor for one or more methods for consumers to revoke their consent to receive calls and text messages. This would:
 - Encourage uniform methods of stopping calls;
 - Mimic methods used by the text trade association (including in every call a simple way to stop future messages);
 - Provide clarity for callers, which would reduce litigation; and
 - Ensure protection for consumers who want to stop calls.
- 4) Require phone companies to implement call authentication, in which the caller is determined to be the person whose name appears on the caller ID, as soon as possible.
 - This will drastically reduce scams;
 - It will empower consumers to use personal blocking tools;
 - It will make caller ID much more reliable, thereby empowering consumer choice of which calls to accept; and
 - It will enable anti-spoofing rules to be more meaningful.
- 5) Promulgate more rigorous regulation of spoofing in order to:
 - Prohibit all spoofing of numbers that callers do not have a right to use; and
 - Allow caller IDs to be legitimately altered by callers, but only for legitimate purposes (*i.e.*, caller from call center in Iowa calling on behalf of Bank in Delaware can use Bank's Delaware caller ID, but not a fake number, etc.).
- 6) Institute the proposed reassigned number database that features:

⁷⁴Dominguez v. Yahoo!, Inc., 2017 WL 390267 (E.D. Pa. Jan. 27, 2017) (appeal filed 3d Cir. Feb. 2, 2017).

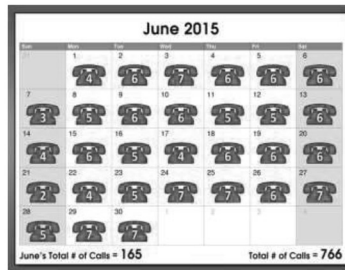
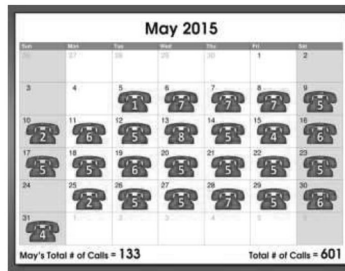
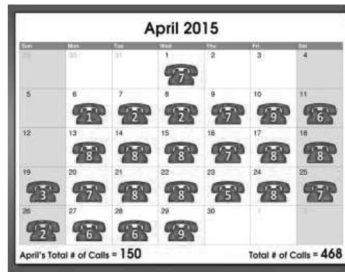
- A centralized system which is reliable, easy and inexpensive for callers to use; and
 - A safe harbor only for calls made as the result of database mistakes, and for which callers otherwise complied with the TCPA.
- 7) Require telecommunication providers to make a free robust call blocking system available to consumers. This would:
- Provide consumers with control over their incoming calls; and
 - Create a centralized appeals/whitelist system to address caller needs, yet always permit consumers to block specific numbers.
- 8) Implement congressionally-required rules limiting calls made to collect debt owed to the Federal government by limiting the number of calls that can be made.
- Thank you for the opportunity to bring our concerns and ideas to your attention. I would be happy to answer any questions.

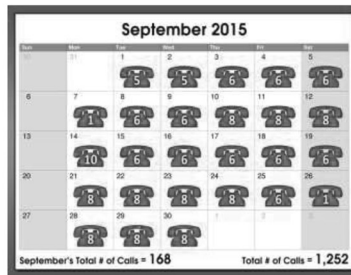
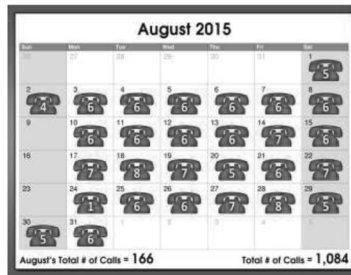
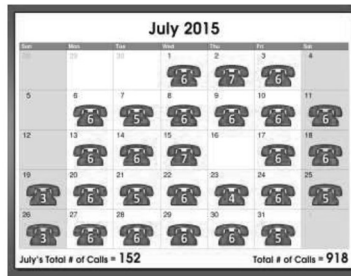
Appendix 1
Calendar Showing Daily and Monthly Calls from Conns Appliances to Ms. Stevens

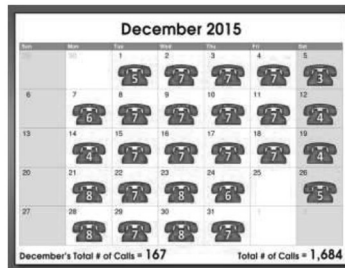
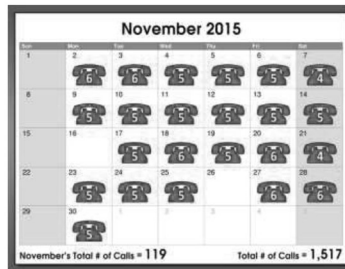
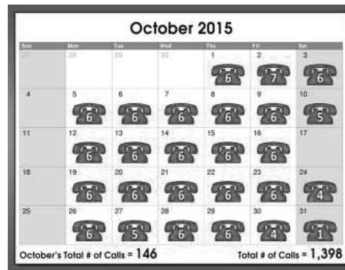
January 2015						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
January's Total # of Calls = 75				Total # of Calls = 75		

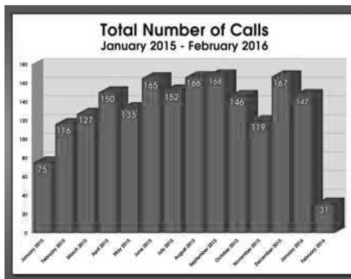
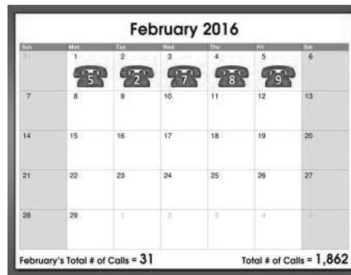
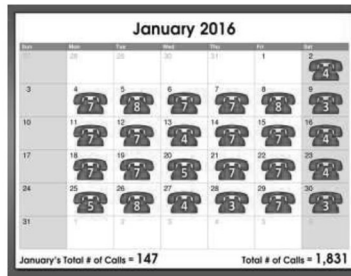
February 2015						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				
February's Total # of Calls = 116				Total # of Calls = 191		

March 2015						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				
March's Total # of Calls = 127				Total # of Calls = 318		









Ms. Stevens' Payment History

Actual Date	Effective Date	Tran Code	Description	Applied Principal	Applied Interest	Applied Other	Principal Balance
12-06-2014	11-29-2014	702-4	New loan debit	9,240.64	.00	.00	9,240.64
01-13-2015	01-13-2015	764-6	Late charge assessment	.00	.00	5.00	9,240.64
01-26-2015	01-26-2015	738-2	Collect late charge	.00	.00	1.23	9,240.64
01-26-2015	01-26-2015	725-5	Regular Payment	288.77	.00	.00	8,951.87
02-13-2015	02-13-2015	764-6	Late charge assessment	.00	.00	5.00	8,951.87
02-26-2015	02-26-2015	725-5	Regular Payment	288.77	.00	.00	8,663.10
03-13-2015	03-13-2015	764-6	Late charge assessment	.00	.00	5.00	8,663.10
04-01-2015	04-01-2015	725-5	Regular Payment	288.77	.00	.00	8,374.33
04-13-2015	04-13-2015	764-6	Late charge assessment	.00	.00	5.00	8,374.33
04-29-2015	04-29-2015	725-5	Regular Payment	288.77	.00	.00	8,085.56
05-05-2015	05-05-2015	712-4	NSF Fee NSF Batch 8752	30.00	.00	.00	8,115.56
05-05-2015	04-29-2015	718-4	Amegy NSF Pmt NSF Batch 8752	288.77	.00	.00	8,404.33
05-13-2015	05-13-2015	764-6	Late charge assessment	.00	.00	5.00	8,404.33
06-05-2015	06-05-2015	725-5	Regular Payment	288.77	.00	.00	8,115.56
06-13-2015	06-13-2015	764-6	Late charge assessment	.00	.00	5.00	8,115.56
07-13-2015	07-13-2015	764-6	Late charge assessment	.00	.00	5.00	8,115.56
07-15-2015	07-15-2015	725-5	Regular Payment	288.77	.00	.00	7,826.79
08-13-2015	08-13-2015	764-6	Late charge assessment	.00	.00	5.00	7,826.79
08-29-2015	08-29-2015	725-5	Regular Payment	288.77	.00	.00	7,538.02
09-13-2015	09-13-2015	764-6	Late charge assessment	.00	.00	5.00	7,538.02
10-13-2015	10-13-2015	764-6	Late charge assessment	.00	.00	5.00	7,538.02
10-30-2015	10-30-2015	725-5	Regular Payment	288.77	.00	.00	7,249.25

The CHAIRMAN. Thank you, Ms. Saunders. Let me just direct this, if I can, principally at least to the FTC and the FCC. But consumer complaints about illegal robocalls seem to be on the rise despite the efforts that you've all noted. The FTC, FCC, and the industry have tried to prevent them. What do you think accounts for this?

Ms. HAROLD. This is a difficult and complex problem, as everyone understands, and there is no silver bullet. A big part of the problem obviously is that technology has made it easy and relatively cheap to engage in this kind of behavior. No single entity has 100 percent of the answers, so we'll have to work together. The kind of activities that we're undertaking, targeted enforcement against some of the biggest robocallers to get attention and send a message to others, is part of it, of course. Technological developments to put into consumer hands so that they can block calls they don't want is a big part of that as well, as is consumer education, and continued cooperation among law enforcement authorities, both between the FTC and us, but also between State and Federal law enforcement authorities. I'm happy to say that that kind of exchange happens regularly.

The CHAIRMAN. Yes, that's good.

Ms. GREISMAN. Chairman? Chairman? Complaints are on the rise. We've seen that steadily over the years. On average now, we're receiving some 475,000 complaints each month. And we know they're the tip of the iceberg because we know from our law enforcement cases, we have sued individuals and companies that have placed billions of calls. So complaints are the tip of the iceberg.

This may sound odd, but complaints are actually very helpful. They're very useful for us. We mine them. We use them to identify

law enforcement targets. And as I mentioned earlier, each day we're putting some 22,000 numbers that consumers complained about, we're putting them out into the public where they can be used by others engaged in call-blocking technologies.

So complaints will continue to rise.

The CHAIRMAN. Do you all think you have the authorities that you need to meet the challenge, the legal authorities you need?

Ms. HAROLD. With respect to the FCC's enforcement actions, what we're concentrating now are on major robocallers. And fortunately, we have two good grounds to do that. Almost all such robocallers use prerecorded messages, which is part of the TCPA and was not affected by the recent court decision. They also spoof, and that's a completely different statute. Should Congress decide to give us additional authority, of course, we will pay close attention to that.

Ms. GREISMAN. Mr. Chairman, the Commission has been on record for well over a decade now calling for the repeal of the Common Carrier Exemption. It is a real impediment to our ability to provide robust law enforcement in this space. In fact, Mr. Abramovich, I believe what he was commenting on are certain carriers whose primary, if not significant, business that generates significant revenues is precisely to carry robocalls. Currently, under the law, we do not have jurisdiction over those entities to the extent they are actually engaged in the business of common carriage.

Ms. HAROLD. I would like to add one thing, Mr. Chairman. If Congress would like to enact legislation, there are two procedural things that would help us at the FCC. One would be to eliminate the citation requirement that applies to actions taken under the Consumer—the TCPA. That does not apply to the anti-spoofing law, but it does apply to the robocall law essentially. We have to give somebody a citation, which is basically a warning, that gives them maybe a free “Get Out of Jail” card free because they get a warning before we can take any serious action against them. They can change the way they do business, and we have to go hunting them down again. If we could get rid of the citation requirement for the TCPA, that would be very helpful.

The other thing that would be helpful would be to harmonize the statute of limitations for both statutes. Right now, under the anti-robocalling law, we have 2 years to get to the point where we charge someone. Under the TCPA, we only have one. It makes it a little difficult back in the office when we're actually working on the investigations to figure out which deadline applies to which part of an investigation that often covers both types of problems.

The CHAIRMAN. We're coming up on the 15th anniversary of the creation of the National Do Not Call Registry. And so I want to ask you a yes-or-no question, and then if anyone wants to elaborate on it, you can. But is the Do Not Call list broken?

Ms. GREISMAN. No. Do Not Call set out to prevent live calls from legitimate telemarketers. That's what the system was designed to do. It was not designed to prevent or halt fraudulent calls. The bad guys never were going to subscribe to the list and abide by the law. So the goal of and the purpose of the Do Not Call Registry was to prevent legitimate live calls, and I do believe it has been and remains successful in that regard.

The CHAIRMAN. All right. Yes? No?

Ms. HAROLD. I agree with what Ms. Greisman said. For the limited purpose it was designed to serve, it seems to be serving that purpose, but the bad guys don't pay attention to it.

The CHAIRMAN. Right.

Mr. RUPY. Mr. Chairman, I would agree with both Ms. Harold and Ms. Greisman on that point.

The CHAIRMAN. OK.

Mr. DELACOURT. I agree as well. The Do Not Call list is well understood by consumers who have subscribed in large numbers. It's oriented to people who are going to comply with the law, companies that are going to comply with the law. It's not going to address those scofflaws who aren't going to comply regardless of what the law requires.

Ms. SAUNDERS. I agree.

The CHAIRMAN. OK. Senator Blumenthal.

Senator BLUMENTHAL. Thanks, Mr. Chairman.

Let me ask the same question, but in a different way. If the Do Not Call Registry is working, why do I receive hundreds, maybe thousands of calls, from my constituents saying, "I'm on the Do Not Call list, but I'm continuing to receive calls"? And when I ask them, it's not fraudulent calls, it's not calls from charitable organizations or politicians who are perhaps within an exemption, they are regular calls that should be covered by the Do Not Call list. Is it that the law is working, but the companies are ignoring it?

Ms. GREISMAN. It's a little bit of both. We distinguish between abusive calls and fraudulent calls. To focus on abusive calls, yes, there are companies that—one was named, one recognized, Dish, for example, that, as challenged in the lawsuit and as reflected in a \$280 million judgment, civil penalty judgment, violated Do Not Call provisions of the Telemarketing Sales Rule and the TCPA. So there are entities out there that take a view that the way their product is marketed by others, it does not result in liability for them.

Senator BLUMENTHAL. Let me ask every one of the members of the panel, would you all agree that consumers need and deserve more effective means to block robocalls, better tools?

Ms. HAROLD. Yes. And I think that technology is probably the leading pipeline for us to be able to help people. The FCC certainly will encourage that and has been working with industry to develop things like Call Authentication, a system that will allow for a technological block, and educating consumers about the availability of these tools is an important part of the picture.

Ms. GREISMAN. Absolutely. That's why back in 2012 in the first robocall contest, the FTC put forth a stimulation to the public, to industry, to develop call-blocking tools.

Mr. RUPY. Senator, I would agree with Ms. Greisman's point in her testimony, and I think it is certainly crucial that we deploy and get tools into the hands of consumers. And think, you know, one of the points that was raised, it was raised in my testimony, you are seeing more and more tools that are out there today—

Senator BLUMENTHAL. I take it the three of you would support the ROBOCOP bill that I've introduced that would require phone companies to provide more effective tools.

Mr. RUPY. Senator, I think a couple things on that and on the tool issue. Number one, I think when you look at just the last couple years alone, the marketplace is responding in terms—

Senator BLUMENTHAL. Well, why would you not support the ROBOCOP?

Mr. RUPY. Because I think a couple things, Senator. First, the marketplace is deploying tools. In smartphone apps alone—

Senator BLUMENTHAL. They're not moving fast enough.

Mr. RUPY. There are a growing number of tools in terms of the apps. And you're also seeing voice providers partnering with a lot of these services.

The other—the other issue that I would state on that, Senator, is that it's important that we take a holistic approach to this. When you look at blocking in and of itself, AT&T has blocked 3.3 billion calls. And my sense is that we are not going to block our way out of this problem. I think we need to take a very holistic approach in terms of getting tools out there, which is happening, educating consumers, and civil and criminal enforcement.

Senator BLUMENTHAL. Mr. Delacourt?

Mr. DELACOURT. Yes. I agree that technology is going to be a big part of the solution for robocalls, particularly with respect to scoff-laws and people who won't be bound by law.

Senator BLUMENTHAL. But would you support the ROBOCOP bill?

Mr. DELACOURT. I'm not familiar with the particular ins and outs of that piece of—

Senator BLUMENTHAL. We'll get you a copy of it.

Mr. DELACOURT. I appreciate that. And I'll review it.

Senator BLUMENTHAL. I'm pressed for time, so I'm interrupting you. I apologize.

But let me ask Ms. Saunders.

Ms. SAUNDERS. Senator, I worked with your staff on your good bill, and I certainly—we certainly support it.

Senator BLUMENTHAL. I'm not going to ask the FCC and the FTC representatives because I know you will have to go back to your agencies and go through the, for lack of a better term, bureaucratic process, but I hope that you will review it carefully and support it. Thank you.

Thanks, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Blumenthal.

Senator Tester.

Senator TESTER. Thank you, Mr. Chairman.

I just want you to know, Senator Blumenthal, they were both nodding their heads. I don't know if that's in support of the bill or not, but, you know.

[Laughter.]

Senator BLUMENTHAL. Thank you, Senator Tester.

Senator TESTER. That's good.

So, Mr. Delacourt, you talked about business, and I think it is affecting business. And I think many parts of the country get work done by e-mails or texts or video chat. In Montana, I speak for myself, but also for my neighbors, we pick up the phone, and so the phone is really critical for jobs and for health care and many of the essential services we have. If I want to buy something, as I pointed

out to the previous guy, I pick up the phone and call, I don't expect them to call me.

But nonetheless, when I start getting a bunch of robocalls, I start losing faith. And I'll just be honest with you, because of robocalls, if I don't recognize the number, even if it's in my area code, even if it's in my three digit, I don't pick up the phone because I don't want to waste my time. And so from that standpoint, it's bad for business, wouldn't you say?

Mr. DELACOURT. Oh, yes.

Senator TESTER. Yes.

Mr. DELACOURT. In the sense that businesses want to lawfully communicate with their customers, they want to be credible, they want consumers to have the faith to answer the phone. Absolutely.

Senator TESTER. Yes. So it's cutting those folks out of the business because I screen my calls now, and I never used to do it. I think it's an important priority. And I don't want to put you on the spot in this question, it isn't meant to put you on the spot, but has the Chamber thought about ways we could solve this problem? Because it truly is a problem and it's a problem for business.

Mr. DELACOURT. Sure. The Chamber has thought about it, and our thinking is that the approach, not unlike what others have said here today, is to really focus on two things, law enforcement and technology. I would distinguish between and I think this hearing today has drawn a useful distinction between abusive robocalls, sort of what was discussed on the first panel, and legitimate businesses.

Senator TESTER. Right.

Mr. DELACOURT. The first—the activity of the first panel is not something that could really be addressed through law, it has to be addressed through—through changes in the law, requiring regulation. It can be addressed through law enforcement and it can be addressed through technology.

Senator TESTER. Yes. So let me move over on that question to either the FTC or the FCC, whichever is most appropriate to answer this question. As far as the Do Not Call list goes, are there any penalties if people don't follow the rules?

Ms. GREISMAN. Absolutely. Civil penalties are upwards of I think it said \$44,000.

Senator TESTER. Upwards of \$4,000?

Ms. GREISMAN. \$44,000 per violation.

Senator TESTER. 44,000? Does the person who receives the calls have any recourse within the courts?

Ms. GREISMAN. Under the Telemarketing Sales Rule, there is a private cause of action, but it is more—far more circumscribed than that which exists under the TCPA.

Senator TESTER. OK. And so do you think that would be helpful? I mean, I've got to tell you, when I do happen to pick up the phone because I don't have my glasses on, and I think it's somebody that it isn't, you know, I always tell them, "I'm going to go get recourse in the courts, and when I get done, you're not going to be able to breathe." I don't know that I can do that. But you think I can.

Ms. GREISMAN. Under the TCPA, as we've heard on this panel, there is quite robust and extensive litigation, plaintiffs exercising the private cause of right that exists under it.

Senator TESTER. OK, good. When was the last time the Do Not Call rule was updated? Do you know? Or has it been in the last 15—

Ms. GREISMAN. The amendments in the Commission, approved amendments in 2008, which became effective in 2009. Those are the robocall prohibitions.

Senator TESTER. OK. Ms. Harold, I understand that a lot of the bad actors are from other countries. Does the FCC have an idea who these countries are?

Ms. HAROLD. Senator, we have some notion that a good number of the calls come from the west—west of our western border or south of our southern border, but beyond being able—I can't pinpoint for you a particular country—

Senator TESTER. For specific countries, you don't know.

Ms. HAROLD. I don't have that information at the tip of my fingers, but if you would like me to get it for you, I'll deliver it to you after the hearing.

Senator TESTER. But you have it. You have it.

Ms. HAROLD. We have some information.

Senator TESTER. OK. So are you able to talk to your counterparts in those countries to hold those folks—

Ms. HAROLD. We do. And I think that the—

Senator TESTER. And how successful has that been?

Ms. HAROLD. I think that the omnibus legislation that Congress just enacted that gives us clear authority to go after callers in other countries will be a helpful starting point.

Senator TESTER. Yes. OK. Good enough.

Just one other question, and I know I'm past time, but it's really quick. You guys talked about technology that's out there, blocking tools that are available. Are they available to me? And are they expensive? And do they work?

Mr. RUPY. So there are a variety of tools that are out there, Senator. Many of these tools are free. Some of these may have a charge. There are native apps that are out there, so these are independent—

Senator TESTER. I would love to have it work like my spam box does.

Mr. RUPY. Absolutely, Senator.

Senator TESTER. If I get a robocall, I just hit the spam button and it just goes to a different file.

Mr. RUPY. And that's something that you're seeing in the marketplace.

Senator TESTER. OK.

Thank you, Mr. Chairman. I appreciate the flexibility.

The CHAIRMAN. Thank you, Senator Tester.

Senator Cortez Masto.

**STATEMENT OF HON. CATHERINE CORTEZ MASTO,
U.S. SENATOR FROM NEVADA**

Senator CORTEZ MASTO. Thank you, Mr. Chair.

So this is for the panel. Let me just start with maybe Ms. Harold, Ms. Greisman, and Mr. Rupy.

So there was an article in the *Washington Post* in January about an FTC action against a robocaller from California who had made

billions of illegal robocalls, and he was living in a wealthy neighborhood, paying \$25,000 a month for his house, had a personal chef, and drove two Mercedes. The FTC brought him in for questioning and he basically admitted he did it without remorse, and he was fined \$2.7 million and banned from telemarketing.

Now, while it's clear that in the digital age your agencies need more resources to police this behavior, and we've talked a little bit about the technology, but it's also evident from the article that even when cases are brought, there is this thought that robocallers believe they have clearly concluded that the financial benefits outweigh any cost of their behavior, it's a cost of doing business. Any fine that is assessed against them is a cost of doing business, and so they'll continue and engage in that.

For this reason, I'm looking at—excuse me—to introduce legislation to include criminal penalties or criminal enforcement.

And so, Mr. Rupy, you've talked about this, the need for criminal enforcement.

I also noted, both Ms. Greisman and Ms. Harold, certain things. One of them was the elimination of citations laws for the TCPA and to harmonize the statute of limitations. But if we're looking at enforcement and new criminal enforcement tools, do you have an idea what that should look like?

Mr. RUPY. That's a great question, Senator. And I think a couple things. And the first point I want to emphasize is that the civil enforcement authority that the FCC and FTC have is effective and it's important. And when they initiate those actions and take those actions, those actions send a very strong message to bad actors. So we applaud those types of actions targeted at these illegal robocallers. With that being said, you know, we certainly believe that given the financial harm that these activities cause, the emotional harm that these activities cause, both of which are significant, criminal law enforcement is warranted.

Now, I am not an expert, if you will, on criminal law enforcement, but my sense is that there are sufficient or existing statutes on the books, whether it's bank fraud, wire fraud, RICO statutes, whereby a criminal—a Federal criminal enforcement agency can target these actors. And if I'm not mistaken, I think the FCC's citation against Mr. Abramovich cites the Wire Fraud Act, which is a Federal criminal statute.

So, you know, my sense is we have tools in the toolbox to go after these bad actors from a criminal perspective.

Senator CORTEZ MASTO. And so, Ms. Greisman and Ms. Harold, do you think—would you agree there's maybe tools out there that we could look to, to mirror?

Ms. GREISMAN. I'm very familiar with the case that you referred to and with the set of facts you described. There are limitations to civil law enforcement; we're well aware of that. We work closely with our counterparts at the Department of Justice. There have been a significant number of criminal cases brought against telemarketers engaged in hard-core fraud, wire fraud, mail fraud, as well as some that were involved in Do Not Call violations and robocall violations. And we're committed to working with our criminal colleagues to get greater deterrent effect.

Senator CORTEZ MASTO. OK. Thank you.

Ms. HAROLD. The same.

Senator CORTEZ MASTO. Thank you.

Let me ask you, Mr. Delacourt. In May of last year, the Chamber submitted a comment to the FCC on a petition from a group called All About the Message, which hoped to remove automated voice-mail from the authority of the TCPA. The comment in support of All About the Message argued that a central problem with the unchecked expansion of the TCPA's prohibition is that it is not the unscrupulous scam telemarketers that are targeted by the TCPA litigation, but, rather, legitimate domestic businesses. And you also mentioned this in your testimony today.

While the TCPA certainly was designed to target scammers, my understanding is it was also designed to prevent robocalls in general even from legitimate businesses. Consumers don't want to be bothered, that's the intent, why Congress acted.

So what I would like to know, is it the position of the U.S. Chamber that robocalls should be entirely legal if not done for a fraudulent purpose?

Mr. DELACOURT. No, that's not the position of the Chamber. The distinction I was trying to draw was between actors in the economy who are constrained by law and regulation and who will comply with things like the Do Not Call list, and others who are scofflaws who are only susceptible to solutions through technology like blocking or apps or things that so you can blacklist those numbers. You generally won't need those against legitimate companies who are concerned with law enforcement, the idea that not only that they will be sued, but that they will suffer brand damage and customer relationship damage as a result of being branded as an abusive robocaller.

Senator CORTEZ MASTO. But there are legitimate businesses that engage in abusive calls is my understanding. Isn't that correct?

Mr. DELACOURT. It is certainly the case that there have been legitimate grievances against businesses and misconduct, but I would say that the mass of the activity that is the source of the consumer complaints is not on that side of the house for the reasons I've discussed today, that what businesses want to do is lawfully communicate with their customers, they want to build a relationship, not destroy a relationship. And so, you know, while there may be instances in which companies have done that either through vendors or other issues, it's not the massive—the complaints from consumers, the activity that's giving rise to consumer complaints is the abusive robocallers.

Senator CORTEZ MASTO. And I know my time is running out, but I see, Ms. Saunders, you're looking to ask a question.

Mr. Chair, is it all right if she responds?

The CHAIRMAN. Quickly.

Senator CORTEZ MASTO. Thank you.

Ms. SAUNDERS. I would beg to differ with my colleague to my right. If you look at the numbers of the top robocallers as compiled by the telecommunications blockers, they are not scammers, they are what we call legitimate businesses. In fact, in the chart in my testimony, we've named them, and those are—many of them are members of the Chamber of Commerce. I'm not saying they've engaged in scams, I'm saying they have engaged in extensive

robocalls which are complained about by consumers. Whether or not those calls are illegal goes to the question of whether consent was originally obtained and whether the calls continue to be made after the consumers have revoked consent. Those are very important questions that consumers need protection on.

Senator CORTEZ MASTO. Thank you.

And thank you, Mr. Chair, for your indulgence.

The CHAIRMAN. Senator Markey.

Senator MARKEY. Thank you, Mr. Chair, very much.

I think Mr. Abramovich is just one bad actor in a universe of bad actors of people who try to exploit the vulnerability of people at home with these phone calls that just keep coming in and disturbing their family peace and quiet. And it's an industry solely predicated on contacting consumers by any means possible, debt collectors, telemarketers, insurance providers, and that's just a short list of the many different industries that seek to exploit this.

And the only thing that protects them is the Telephone Consumer Protection Act of 1991. And I am the author of that law, and I will just tell you that the key word that I wanted to have built in is the word "consent." Consent is the bedrock of the TCPA, and while technology may change, that key principle does not.

Therefore, it is the FCC's obligation to use its authority to adapt to changing technologies and ensure consumers have robust enforceable protections against the onslaught of unwanted and abusive calls and texts. And their work is more important now than ever because the D.C. Circuit Court of Appeals recently struck down portions of the FCC's 2015 rules, which updated protections for the smartphone era.

While the court case was a setback, the spirit and the intent of the TCPA is as clear today as it was in 1991. One, callers must have affirmative permission from the consumer before using autodialers, which are technologies that can call and text countless consumers at one time, and, two, consumers should always have reasonable means to revoke consent, to say no from receiving any more calls or texts.

So, Ms. Saunders, if you would, is there any reason why the FCC cannot use its authority under the TCPA to ensure consumers have an easy way to revoke consent and require callers using autodialers to receive permission before calling or texting a consumer? And what harms could arise if weak protections are adopted?

Ms. SAUNDERS. Senator Markey, thank you for the question. One of the most critical issues that was sent back to the FCC as a result of the D.C. Circuit order was the definition of "autodialer." And if the FCC bows to the calling industry and defines that equipment very narrowly, consumers will be significantly harmed because they won't have the option to consent or revoke consent from calls that are made by equipment that is now covered or considered to be covered by an autodialer.

So one big issue is that if autodialer is not sufficiently—defined sufficiently broadly, it won't cover texts. There's no independent language in the TCPA that will cover texts unless the "autodialer" definition is covered.

The other issue that is bound to come up again at the FCC is how to revoke and whether consumers even have the right to re-

voke. A recent Second Circuit opinion held that consumers, once they've consented, by contract, do not have the right to revoke. That's the position of the caller in the first example in my testimony. They said once she gave consent, she can never say no.

So the harm to consumers is, A, that they may not have the option to consent and then revoke; or, B, they may not be able to revoke at all.

Senator MARKEY. Yes. Right. So it sounds like the "Me Too" movement here. Consent once is consent forever, huh?

Ms. SAUNDERS. Exactly.

Senator MARKEY. And people have a right to say no at any point, that's the way it should be. Now, we made a mistake, and we just don't want that kind of conduct to continue.

So, as I said earlier, I drafted a letter to the Chairman today asking for a comprehensive definition of "autodialer," ensuring all callers must receive permission before robocalling or robotexting a consumer, and preserving consumers' rights to revoke consent should they no longer wish to receive calls or texts.

So, Ms. Harold, will the FCC heed our call and establish robust protections?

Ms. HAROLD. Mr. Chairman—Mr. Markey, sorry—as the Enforcement Bureau Chief, I'm not in a position to tell you exactly what the Commission will do and how soon it will do it, but people of the Commission I can tell you are well aware of the letter that you provided to the Chairman today, as well as the D.C. Circuit opinion in ACA International.

Senator MARKEY. So you're working on this issue? You are going to proceed toward trying to put protections on the books?

Ms. HAROLD. I can't speak for the Commission. I enforce the rules that are already before us as opposed to thinking about how to improve them. But I can take your message back to my colleagues who are working on that.

Senator MARKEY. In light of the court decisions, it's time to go back, redo the rules, and get back out into the marketplace to protect consumers. And I would urge you to do that as quickly as possible.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Markey.

Senator Baldwin.

STATEMENT OF HON. TAMMY BALDWIN, U.S. SENATOR FROM WISCONSIN

Senator BALDWIN. Thank you, Mr. Chairman and Ranking Member.

Thank you to our witnesses.

I have listened to my colleagues and their questioning. Senator Tester talked about the fact that Montanans perhaps might be more prone to using the telephone. I certainly would have that reflection among some of my rural constituencies, depending on access to other alternative communication tools. I would also perhaps have that observation about my elderly constituents. I regularly receive calls from older constituents who I suspect are more greatly affected by robocalls because they rely more on the telephone for

staying in touch with friends and family and accessing services and government benefits and conducting business.

So in today's testimony, we've heard that one approach to addressing unwanted robocalls is giving consumers more options to control which calls they receive, including through new technologies. And I wonder how well these proposals will work for some of our constituencies, as have been described, including older Americans.

Ms. Saunders, can you speak to how robocalls may uniquely affect older or rural-living Americans and how solutions should take into account the needs of these populations?

Ms. SAUNDERS. Yes, I can. Thank you for the question. We do have many blocking solutions that are available in the marketplace, but my understanding is that very few of these blocking solutions are available for landlines, and seniors most often rely on landlines more than younger folks, who rely exclusively on their cell phones. So the blocking technologies are not really helpful for them, which leaves seniors much more vulnerable to both the abusive repeated phone calls and the inability of finding blocking.

I will say that I'm 64, and now I am getting an onslaught of calls from the Medicare Health Center, all who know my name and mispronounce it every time. They call me three or four times a day offering me Medicare health supplement. So that's coming on my home phone and now my cell phone. I don't know where they're getting that information, and they are not stopping calling. So they—that's presumably a legitimate business, but that is—that's not paying any attention to the TCPA requirements.

Senator BALDWIN. Thank you.

Mr. Rupy, how are your member companies working to ensure that the proactive steps that they are taking to address robocalls will work for constituencies that are more reliant on landlines?

Mr. RUPY. Thank you for that question, Senator. It's a great question. And I think from our industry's perspective, as you've heard repeatedly during this panel, there is no silver bullet to this—addressing this problem, and we have to take a holistic solution and we have to take a holistic approach to addressing it.

So, you know, number one, our industry, we have our Industry Traceback Group, which USTelecom leads. That includes cable, wireline, wireless, wholesale providers, a broad range of companies. And we want to identify the source of these calls because our collective view is that by identifying the source, it's like a bad weed, if we pull it out by the root, we're going to stop millions of calls. So that's number one.

Number two, there is importance for tools, so we want to make sure that tools do get out there. And I think, as you've heard, there are more and more tools across a variety of platforms. So you're seeing tools across IP wireline, wireless, and copper. They're going to vary. We always encourage consumers to call their provider, but those tools are out there. And even on the copper point, you know, I would note Verizon's recent deployment of this caller ID service, the spam service, that, you know, provides context for that call, and I think that's important.

So, you know, those are all the areas that our members are focused on this.

Senator BALDWIN. OK. If I could just do a quick follow-up. Just can you just tell me how the industry traceback works?

Mr. RUPY. So the way that effort works, Senator, is that we basically have a collective. We have our 22 member companies. These are some of the largest companies out there: AT&T, Verizon, Frontier, Comcast, Charter, Sprint. And——

Senator BALDWIN. So are they tracing back based on traffic that they notice independently, or do they have to be tipped off by, say, a landline consumer or customer that they're getting these calls in order to enable a traceback?

Mr. RUPY. Generally speaking, Senator, the companies are sourcing these tracebacks internally. So in other words, these companies all have network operations centers where they are actively monitoring for suspicious traffic 24/7/365. When they find an instance where they have identified traffic that they believe is illegal or it verified as illegal, the group will initiate traceback, and what makes traceback difficult today, I equate it to peeling back the layers of an onion. Any call can go through perhaps 10 providers, but each provider, in the course of that call, they can only see to whom they handed it to and from whom they got it from. They don't know the subsequent carriers or the preceding carriers. So we work collectively to accelerate that process so that, you know, we can get the ball down the field closer to the origin of the call.

Senator BALDWIN. Thank you.

The CHAIRMAN. Thank you, Senator Baldwin.

Anything for the good of the—to close it out?

Senator Blumenthal.

Senator BLUMENTHAL. Just an observation. Mr. Rupy, I appreciate your citing a holistic approach and the services that are now available. I would just point out that they're available at a cost, and sometimes significant cost, correct?

Mr. RUPY. Senator, there is both—there are free—free services out there, and some are at a cost. But there is a diversity of services that are available out there both from providers, from third-party providers, carriers. Some are free, some may have a charge.

Senator BLUMENTHAL. Thank you.

Mr. RUPY. But the examples I cited in my oral testimony both are free.

Senator BLUMENTHAL. Thank you.

The CHAIRMAN. Thank you, Senator Blumenthal.

I thank the panel. This has been very helpful, and we appreciate your insights.

I'm going to ask unanimous consent to include in the letter—or I should say in the record—several letters, one from Epic, one from CTIA, and one from CBA.

[The information referred to follows:]

ELECTRONIC PRIVACY INFORMATION CENTER
Washington, DC, April 16, 2018

Hon. JOHN THUNE, Chairman,
Hon. BILL NELSON, Ranking Member,
U.S. Senate Committee on Commerce, Science, and Transportation,
Washington, DC.

RE: "Abusive Robocalls and How We Can Stop Them"

Dear Chairman Thune and Ranking Member Nelson:

We write to you regarding tomorrow's hearing on "Abusive Robocalls and How We Can Stop Them."¹ We appreciate your interest in this important issue.

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C.² EPIC played a leading role in the creation of the Telephone Consumer Protection Act ("TCPA") and continues to defend the Act,³ one of the most important and popular privacy laws in the history of the United States. EPIC supported establishment of the original Do Not Call registry.⁴ EPIC provided numerous comments to the Federal Communications Commission ("FCC") and the Federal Trade Commission ("FTC") on the implementation of the TCPA, and maintains online resources for consumers who seek to protect their rights under the TCPA.⁵ EPIC has testified twice in congressional hearings on robocalling.⁶ Last year EPIC submitted comments to the FCC, expressing support for a new rule that would allow phone companies to block calls from numbers they know are invalid, such as numbers that have not been assigned to a subscriber.⁷ EPIC also submitted an amicus brief in *ACA International v. FCC*, 885 F.3d 687 (D.C. Cir. 2018).⁸

Robocalls are a consistent source of annoyance for American consumers who confront bad actors that engage in identity theft, financial fraud, and debt collection scams. Robocalls are consistently one of the top complaints made to both the FCC and the FTC.⁹ The transition from land lines to mobile phones¹⁰ has only made the problem worse. Unsolicited calls and texts facilitate fraud, drain battery life, eat into data plans and phone memory space, and demand attention when the user would rather not be interrupted. Because we carry our phones with us every-

¹ *Abusive Robocalls and How We Can Stop Them*, S. Comm. on Commerce, Science, & Transportation, 115th Cong. (April 17, 2018), <https://www.commerce.senate.gov/public/index.cfm/hearings?ID=E0EB17D2-A895-40B4-B385-F94EA2716957>.

² EPIC, About EPIC (2016), <https://epic.org/epic/about.html>.

³ See, e.g., Telephone Advertising and Consumer Rights Act, H.R. 1304, Before the Subcomm. on Telecomms. and Fin. of the H. Comm. on Energy and Commerce, 102d Cong., 1st Sess. 43 (April 24, 1991) (testimony of CPSR Washington Office director Marc Rotenberg), <https://www.c-span.org/video/?18726-1/telephone-solicitation>; Brief of Amici Curiae Electronic Privacy Information Center (EPIC) and Six Consumer Privacy Organizations in Support of Respondents, *ACA Int'l v. FCC*, No. 15-1211 (D.C. Cir. Jan. 22, 2016), <https://epic.org/amicus/acaintl/EPIC-Amicus.pdf>; National Consumer Law Center et al., Petition for Reconsideration of Declaratory Ruling and Request for Stay Pending Reconsideration In the Matter of Broadnet Teleservices LLC Petition for Declaratory Ruling, CG Docket No. 02-278 (2016).

⁴ Comments of EPIC, *In the Matter of Rules and Regulations Implementing the Consumer Protection Act of 1991*, FCC Docket No. 02-278 (Dec. 9, 2002), <https://epic.org/privacy/telemarketing/tcpacomment.html>.

⁵ See, e.g., EPIC, EPIC Administrative Procedure Act (APA) Comments, <https://epic.org/apacomment/>; EPIC, Telemarketing and the Telephone Consumer Protection Act (TCPA), <https://epic.org/privacy/telemarketing/>.

⁶ Marc Rotenberg, EPIC President, Testimony and Statement for the Record, *H.R. 5126, the Truth in Caller ID Act of 2006*, H.R. Comm. on Energy and Commerce, Subcomm. on Telecommunications and the Internet, 109th Cong. (2006), <https://epic.org/privacy/iei/hr5126test.pdf>; Allison Knight, EPIC Counsel, Testimony and Statement for the Record, *The Truth in Caller ID Act of 2007*, S. 704, S. Comm. on Commerce, Science, and Transportation, 110th Cong. (2007), <https://epic.org/privacy/iei/s704test.pdf>.

⁷ Comments of EPIC, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, FCC 17-24 (June 30, 2017), <https://epic.org/apacomment/EPIC-FCC-Robocall-Comments.pdf>.

⁸ Brief of Amici Curiae EPIC et al., *ACA International v. FCC*, No. 15-1211 (D.C. Cir.), <https://epic.org/amicus/acaintl/EPIC-Amicus.pdf>.

⁹ Consumer Complaint Center, FCC, <https://consumercomplaints.fcc.gov/hc/en-us/articles/115002234203-Unwanted-Calls>; FTC Releases Annual Summary of Consumer Complaints, FTC, Mar. 3 2017, <https://www.ftc.gov/news-events/press-releases/2017/03/ftc-releases-annual-summary-consumer-complaints>.

¹⁰ 95 percent of American adults own at least one cell phone and 77 percent own smartphones. *Mobile Fact Sheet*, Pew Research Ctr. (Jan. 12, 2017) <http://www.pewinternet.org/fact-sheet/mobile/>; Over half of American households do not have a land line. Stephen J. Blumberg & Julian V. Luke, Ctrs. for Disease Control & Prevention, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July-December 2016*, at 2 (May 2017), <https://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201705.pdf>.

where,¹¹ unwanted calls and texts interrupt sleep, disturb meetings and meals, and disrupt concentration wherever we go. For low-income consumers who often rely on pay-as-you-go, limited-minute prepaid wireless plans,¹² these unwanted calls and texts are particularly harmful.¹³

Current laws and penalties for illegal robocalls have not been enough to stop these calls. Even with the private right of action contained within the TCPA, illegal, predatory behavior continues. This is despite the fact that in general TCPA cases are among the most effective privacy class actions because they typically require companies to change their business practices to comply with the law. However, more must be done. While consumers now have more options to block calls from their home and cell phones, they can only do so after they have received these illegal and bothersome phone calls.

D.C. Circuit Decision

The recent decision in *ACA International v. FCC*¹⁴ was a generally positive outcome for consumers, but created some ambiguity surrounding the definition of “automated telephone dialing system” (“ATDS”). The court upheld the FCC’s interpretation of the consent rule, which allows consumers to revoke consent using “any reasonable means clearly expressing a desire to receive no further messages from the caller.”¹⁵ The court also affirmed the FCC’s conclusion that callers cannot “unilaterally prescribe the exclusive means for consumers to revoke consent.”¹⁶ But the court also held that the FCC’s definition of ATDS under the TCPA was an unreasonably expansive because it could include ordinary smartphones. This creates some uncertainty regarding the scope of ATDS devices.

A broad definition of ATDS should be preserved. The court only struck down the FCC’s 2015 order, leaving the 2003 and 2008 orders in place. The ATDS definition under those orders would cover most autodialers responsible for unwanted calls. But companies and scammers may continue to seek to circumvent the TCPA by developing technology that falls outside of the definition of ATDS. Any further narrowing of the ATDS definition would harm consumers.

EPIC’s Recommendations

EPIC is in favor of rules that would (1) allow phone providers to proactively block numbers that are unassigned, unallocated, or invalid; (2) block invalid numbers without requiring consumer consent; (3) provide strong security measures for any database of blocked numbers that may be created; and (4) prohibit spoofing with the intent to defraud or cause harm.

First, proactive blocking of these numbers is the most effective way to protect consumers. If providers wait until complaints pile up, consumers will be exposed to calls that are predatory and fraudulent. Some consumers choose not to answer calls from numbers that they suspect are invalid based on caller ID information. But some consumers use landlines that may not have or use caller ID, and upon answering the phone they would have no way to be alerted to the fact that the call they are receiving is likely an illegal robocall.

Second, phone providers should not require consent from consumers before blocking calls from invalid numbers. No reasonable consumer wants to receive robocalls. This is evident from the fact that these calls are consistently the number one complaint at both the FTC¹⁷ and the FCC. A consent for blocking requirement would leave individuals and, particularly, seniors at risk of identity theft, fraud, and harassment by phone scammers.

Third, databases and “white lists” of blocked numbers require strong security measures. EPIC has long advocated for strong security measures to protect personal

¹¹More than 70 percent of smartphone users keep their phones within five feet a majority of the time. Harris Interactive, 2013 Mobile Consumer Habits Study (June 2013), <http://pages.jumio.com/rs/jumio/images/Jumio%20-%20Mobile%20Consumer%20Habits%20Study-2.pdf>.

¹²Federal Communications Commission, *Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless*, Eighteenth Report, WT Docket No. 15–125, ¶¶ 44, 73, 95–96 (Dec. 23, 2015).

¹³Bill Moack, *Feds, Fla. Shut Down Robocall Ring That Targeted Seniors*, Clarion Ledger (Jun. 9, 2017), <http://www.clarionledger.com/story/business/2017/06/09/feds-fla-authorities-shut-down-robocall-ring-targeted-seniors/371452001/>.

¹⁴No. 15–1211, 2018 WL 1352922 (D.C. Cir. Mar. 16, 2018), <https://epic.org/amicus/acaintl/15-1211-1722606.pdf>.

¹⁵*Id.* at 5.

¹⁶*Id.* at 17.

¹⁷FTC Releases Annual Summary of Consumer Complaints, FTC, Mar. 3 2017, <https://www.ftc.gov/news-events/press-releases/2017/03/ftc-releases-annual-summary-consumer-complaints>.

data stored in databases.¹⁸ EPIC recommends data minimization, but in this case it is necessary to maintain a list of all numbers that have been blocked by providers. Such a database will be an attractive target for hackers.¹⁹ If compromised, it would not only allow scammers to continue with their illegal behavior, but also would severely hamper any further efforts to implement widespread blocking of invalid numbers. EPIC has suggested the implementation of certain procedures that would help enhance the security of a database of blocked numbers.²⁰

Fourth, any regulation of spoofing should contain an intent requirement—“intent to defraud or cause harm.” This language would cover the problem of pretexting, where bad actors use the number of a trusted entity, such as a bank or government agency, to fool people into giving the caller personal information. But it would also preserve legitimate uses of spoofing where callers wish to withhold their phone number, including drug treatment services, suicide prevention, domestic abuse, and crime tip line. The default for disclosure of identity should be in control of the non-commercial callers. A spoofing regulation without this intent requirement could hurt the privacy interests of callers.

We ask that this Statement from EPIC be entered in the hearing record. EPIC looks forward to working with the Committee on these issues of vital importance to the American public.

Sincerely,

/s/ MARC ROTENBERG
Marc Rotenberg
EPIC President

/s/ ALAN BUTLER
Marc Rotenberg
EPIC Senior Counsel

/s/ CHRISTINE BANNAN
Christine Bannan
EPIC Administrative Law and Policy
Fellow

CONSUMER BANKERS ASSOCIATION
Washington, DC, April 17, 2018

Hon. JOHN THUNE,
Chairman,
Committee on Commerce, Science, and
Transportation,
U.S. Senate,
Washington, DC.

Hon. BILL NELSON,
Ranking Member,
Committee on Commerce, Science, and
Transportation,
U.S. Senate,
Washington, DC.

Dear Chairman Thune and Ranking Member Nelson:

On behalf of the Consumer Bankers Association (CBA), I would like to commend the Committee on Commerce, Science, and Transportation’s for holding the hearing on “Abusive Robocalls and How We Can Stop Them.” CBA is the voice of the retail banking industry whose products and services provide access to credit to millions of consumers and small businesses. Our members operate in all 50 states, serve more than 150 million Americans, and collectively hold two-thirds of the country’s total depository assets.

The influx of fraudulent and illegal robocalls by bad actors has become an ever-growing problem for consumers. As Congress examines how to prevent these burdensome calls and address those with ill-intentions, it is imperative to distinguish

¹⁸ See e.g., Comments of EPIC, *Privacy Act of 1974; Department of Homeland Security/ALL—038 Insider Threat Program System of Records*, Mar. 28, 2016, <https://epic.org/apa/comments/EPIC-DHS-Insider-Threat-Comments.pdf>; Comments of EPIC, *Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) and DoD Component Insider Threat Records System*, Jun. 2, 2016, <https://epic.org/apa/comments/index.php?y=2016>; Comments of EPIC, *Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Customs Enforcement-016 FALCON Search and Analysis System of Records*, Jun. 5, 2017, <https://epic.org/apa/comments/EPIC-DHS-FALCON-Database-Comments.pdf>.

¹⁹ Bruce Schneier, *Data Is a Toxic Asset*, Schneier on Security, Mar. 4, 2016, <https://www.schneier.com/blog/archives/2016/03/data-is-a-toxic.html> (“saving [data] is dangerous because failing to secure it is damaging. It will reduce a company’s profits, reduce its market share, hurt its stock price, cause it public embarrassment, and—in some cases—result in expensive lawsuits and occasionally, criminal charges. All this makes data a toxic asset, and it continues to be toxic as long as it sits in a company’s computers and networks.”)

²⁰ See, e.g., Reply Comments of EPIC, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, 82 Fed. Reg. 22,625 (July 31, 2017).

these robocalls from the beneficial communications between legitimate businesses and their customers.

Consumers utilize many useful communications through calls and texts ranging from low balance notifications to repayment counseling, among other important notices and alerts. While the Telephone Consumer Protection Act (TCPA) was enacted nearly 27 years ago and aimed to protect consumers from intrusive and unwanted telemarketing calls, it has also forced financial institutions to limit many pro-consumer, non-telemarketing communications. Failing to reflect both changes in technology and the contact preference of consumers, the TCPA is barring businesses from providing important information that consumers want and need to receive. CBA members are committed to the spirit of the TCPA and go to great lengths to comply, but the recent interpretations of the law have stifled legitimate businesses' ability to better serve and communicate with their customers.

Since enacted, TCPA litigation has become a thriving industry for class action lawyers. Mobile applications have been created for the sole purpose of collecting and reporting calls to waiting attorneys, helping to drive a 1,272 percent increase in TCPA litigation from 2010 to 2016.¹ Attorneys are benefiting from the outdated law with settlement fees averaging \$2.4 million, dwarfing the average plaintiff award of \$4.12.²

The FCC has an opportunity to re-examine the TCPA, and prescribe new guidelines for the industry. On March 16, 2018, the U.S. Court of Appeals for the D.C. Circuit issued a unanimous decision in *ACA International v. Federal Communications Commission (FCC)* vacating the FCC's overbroad reading of what qualifies as an automatic dialer, most notably addressing the FCC's 2015 interpretation of "capacity" of an automatic dialer, and the FCC's order on reassigned numbers, finding that a one-call safe harbor for companies who inadvertently contacted a number that had been reassigned to be "arbitrary and capricious."

The FCC should re-evaluate the definition of an automatic dialer to include those technologies that use random and sequential numbers—typically for marketing or fraudulent purposes—and not those that employ existing customer contact lists stored by legitimate businesses.

Additionally, the FCC should continue its pursuit of a reassigned numbers database to create an all-encompassing source for businesses to scrub their contact lists, and permit a safe-harbor from any violations of the law for those businesses that voluntarily use the database to determine if a phone number has been reassigned or improperly entered to their lists. Establishing a solution that permits, but does not require the industry to scrub numbers against such a list is crucial. We urge the Committee to encourage the FCC to take prompt action in these matters.

CBA members greatly appreciate this thoughtful approach to examining the issues surrounding illegal and burdensome robocalls. We remain committed to working with the Committee to protect consumers from abusive robocalls while providing legitimate businesses with much needed clarification and reasonable standards on how to reach their customers.

Sincerely,

RICHARD HUNT,
President and CEO,
Consumer Bankers Association.

CTIA
April 18, 2018

Hon. JOHN THUNE, Chairman,
Hon. BILL NELSON, Ranking Member,
Committee on Commerce, Science, and Transportation,
United States Senate,
Washington, DC.

Dear Chairman Thune and Ranking Member Nelson:

CTIA commends the Committee for holding today's hearing to examine the problem of abusive robocalls. CTIA understands consumer annoyance over these calls and we have continued to work actively and in close coordination with Congress, the Federal Communications Commission (FCC), and the Federal Trade Commission (FTC) to address this serious issue on many fronts. Unfortunately, the tactics

¹ <https://webrecon.com/2016-year-in-review-fdcpa-down-fcra-tcpa-up/>

² <https://ecfsapi.fcc.gov/file/60001016697.pdf>

used by today's malicious spoofers, scammers and other bad actors that generate abusive robocalls have evolved dramatically from when Congress passed the Telephone Consumer Protection Act (TCPA) over twenty-five years ago. Aggressive enforcement of bad actors is key to combatting the scourge of illegal robocalls and we applaud this Committee for its focus on enforcement of illegal robocallers. Tracking down and prosecuting bad actors should be the centerpiece of robocall mitigation efforts. In addition to robust FCC and FTC enforcement efforts, CTIA and its members have implemented a multifaceted approach to robocalls—one that includes a variety of technical solutions and industry initiatives to protect consumers, including development of new applications, new network-based tools, and industry work to deploy call authentication to mitigate caller id spoofing.

Industry Technical Solutions. Industry has been at the forefront of the fight against malicious spoofing and robocalls, having collectively blocked *billions* of robocalls. CTIA and its members continue to innovate new solutions to stop illegal and unwanted robocalls, including by adopting new call blocking and spam call prediction tools for customer use. The application ecosystem around robocall blocking technology has exploded in recent years. In 2016 there were over 85 call-blocking applications available across all platforms, including several offered by carriers to their customers at no charge. CTIA has launched a website devoted to providing consumers instructions on how to stop robocalls, and our website has links to these call blocking applications. Since launch of our website, there are now over 550 applications available, a *495 percent increase in call blocking*, labeling, and identifying applications to fight malicious robocalls.

Wireless Industry Cooperation with Government and Other Stakeholder Initiatives. In addition to technology development, the wireless industry has worked with other stakeholders, including government entities, to reduce abusive robocalls. For example, the industry has implemented recommendations from the October 2016 FCC Strike Force Report, including partnering with standards bodies and accelerating STIR/SHAKEN call authentication development by six months. This technology will give service providers the tools to consistently authenticate, digitally sign, and verify calling party numbers—acting like a digital fingerprint to determine callers are who they say they are. CTIA members also participate in U.S. Telecom's Traceback efforts, and that Working Group is sharing its information with the FCC and FTC to identify the source of illegal robocall traffic. A component of these efforts is preventing false positives to protect communications from legitimate callers. CTIA and its members also assist the FCC and FTC with enforcement actions against robocallers and maintain relationships with call fraud bureaus that may initiate investigations after a suspected mass calling event. CTIA has also created its own Robocall Working Group and provides consumer-facing resources on how to limit and report illegal robocalls.

CTIA Member Actions. CTIA's members have also taken strides to combat malicious robocalls. Many providers, including all of the national wireless carriers, offer robocall abatement options for their customers that are not dependent on the customer first downloading a third-party application. Just some of the efforts of several CTIA members are described below:

- *AT&T* launched *AT&T Call Protect* in December 2016 as a free network service. It can flag suspected spam calls, allowing the customer to choose whether to answer or not, and allowing customers to manually block an unlimited number of specific telephone numbers for thirty-day intervals. In November 2017, AT&T made Call Protect available to its IP Wireline Home Phone Users Network. In addition, AT&T has blocked 3.5 billion unwanted robocalls in cases where its business contracts allow it to block impermissible traffic using a new program that detects violators through network data analysis. Call data analysis and heuristics are powered by Hiya.
- *Sprint* offers *Premium Caller ID service*, which allows users to identify nuisance calls and provides an option to block them. This solution directly leverages data and network intelligence powered by a partnership with Cequent, a wholly owned subsidiary of Transaction Network Services.
- *T-Mobile* launched *Scam ID* in March 2017 as an automatic network-based free service for all postpaid T-Mobile customers and MetroPCS customers. Scam ID identifies calls from known phone scammers and displays "Scam Likely" on the device, giving customers the option to answer or block the number. Customers may also choose to use *Scam Block*, another free service to have calls from known scammers blocked. These solutions are powered by network call data analysis and heuristics provided by PrivacyStar, and have resulted in more than 3 billion scam calls tagged since launch.

- *Verizon* offers all wireless customers who subscribe to its Caller Name ID service a free feature that identifies potential spam calls and displays the level of risk with a “risk meter.” The service is also powered by Cequent. They also offer a free robocall labeling solution called *Spam Alerts* for all wireline customers with Caller ID. The feature warns customers about robocalls identified by Verizon’s analytics engine and its robocall mitigation team.

These strategies and technologies highlight the wireless industry’s hard work to stay ahead of malicious robocallers, and that work continues. We appreciate this Committee’s efforts to explore ways to further reduce the transmission of illegal robocalls and continue to encourage aggressive enforcement of bad actors. We look forward to continuing to work with you and your colleagues on this important issue.

Regards,

MEREDITH ATTWELL BAKER,
President and CEO.

The CHAIRMAN. And I would also note that we’ll keep the hearing record open for a couple of weeks, and if the members of the Committee have questions that they can submit for the record, that you could get those back to us as quickly as possible, that would be most appreciated.

But thank you all again for your willingness to participate today and for your honest answers about what’s happening out there in the world of robocalls. It’s something that affects literally pretty much every American who has a phone.

So thank you. This hearing is adjourned.

[Whereupon, at 12:03 p.m., the hearing was adjourned.]

A P P E N D I X

April 17, 2018

Hon. JOHN THUNE,
Chairman,
Committee on Commerce, Science, and
Transportation,
U.S. Senate,
Washington, DC.

Hon. BILL NELSON,
Ranking Member,
Committee on Commerce, Science, and
Transportation,
U.S. Senate,
Washington, DC.

Dear Chairman Thune and Ranking Member Nelson,

The undersigned trade associations and industry groups, who represent thousands of financial institutions and other businesses across the country, appreciate the opportunity to comment on the Senate Commerce, Science, and Transportation Committee's hearing entitled "Abusive Robocalls and How We Can Stop Them."

Illegal and fraudulent robocalls can be a time-consuming and annoying burden on consumers. Congress should rightfully evaluate how it can prevent these invasive and burdensome calls and remove bad actors from the marketplace. However in doing so, it is important to distinguish between fraudulent and illegal robocalls and calls from legitimate businesses seeking to communicate with their members and customers.

Today, many businesses call or text their members and customers in an effort to communicate time-sensitive, critical information, such as low balance notifications, due date reminders, and fee avoidance alerts. Consumers want and expect these types of communications in the most convenient way possible, including via cell phone. Unfortunately, the Telephone Consumer Protection Act (TCPA), while enacted in 1991 to reduce consumers' costs at a time when cell phone users were charged by the minute, has had the unintended consequence of stifling pro-consumer, non-telemarketing communications. The TCPA has become rife with litigation, with a 1,272 percent increase in TCPA lawsuits from 2010 to 2016. This litigation risk has led businesses to limit—and, in certain instances, to eliminate—communications consumers want and expect to receive.

On March 16, 2018, the U.S. Court of Appeals for the D.C. Circuit issued a decision in *ACA International v. Federal Communications Commission* (FCC), vacating portions of a 2015 FCC Order interpreting various sections of the TCPA. This ruling gives the FCC an opportunity to re-examine the TCPA, and prescribe new guidelines for the industry.

It is critical the FCC seize this opportunity to clarify the definition of an Automatic Telephone Dialing System (ATDS) so that it is consistent with the statute and take other action to ensure that consumers whose mobile phone numbers have been reassigned continue to receive important communications. Doing so will permit businesses to provide beneficial communications to their members and customers without the threat of costly litigation driven by serial plaintiffs and attorneys who have taken advantage of the ATDS definition recently vacated by the D.C. Circuit. We urge the Committee to encourage the FCC to take prompt action in these matters, and to continue its efforts to establish a free or low-cost reassigned numbers database and provide a safe-harbor for businesses that use the database.

Legitimate businesses need clarification and standards for how to best serve their members and customers, and are equally concerned about the level of fraudulent and illegal actors in this space. We support the FCC's efforts to deter bad actors while facilitating the ability of legitimate businesses to contact consumers promptly and efficiently. We look forward to working with the Committee as it pursues this issue.

Sincerely,

American Bankers Association
Consumer Bankers Association
Credit Union National Association

Electronic Transactions Association
 Independent Community Bankers of America
 National Association of Federally-Insured Credit Unions
 National Council of Higher Education Resources
 Student Loan Servicing Alliance

April 28, 2017

Ms. Marlene H. Dortch
 Secretary
 Federal Communications Commission
 Washington, DC.

Ex Parte Submission

RE: Advanced Methods to Target and Eliminate Unlawful Robocalls, Notice of Proposed Rulemaking, CG Docket No. 17-59

Dear Ms. Dortch:

On behalf of ACT | The App Association, Alliance for Telecommunications Industry Solutions (ATIS), CTIA and USTelecom, we are filing the attached Industry Robocall Strike Force report. Linda Vandeloop (AT&T) provided a copy of this report to Mark Stone and Micah Caldwell on April 26, 2017. In accordance with section 1.1206(b)(2) of the rules of the Federal Communications Commission, this letter is being filed electronically with your office. Please feel free to contact us if you have any questions.

Sincerely,

/s/ BRIAN SCARPELLI
 Brian Scarpelli
 Senior Policy Counsel
 ACT | The App Association

/s/ THOMAS E. GOODE
 Thomas E. Goode
 General Counsel
 ATIS

/s/ KRISTA L. WITANOWSKI
 Krista L. Witanowski
 Assistant Vice President, Regulatory Affairs
 CTIA

/s/ KEVIN G. RUPY
 Kevin G. Rupy
 Vice President, Law & Policy
 USTelecom

Attachment

cc: Micah Caldwell
 Mark Stone

INDUSTRY ROBOCALL STRIKE FORCE REPORT

1. Introduction (*AT&T*)

1.1. Overview

On October 26, 2016, the Industry Robocall Strike Force issued a report describing progress made during the first sixty days and outlining a process for continuing the work necessary to develop an industry solution to the robocall problem. The industry committed to continue to work together and to issue another status report in six months. ACT, ATIS, CTIA and USTelecom, who count among their members many Strike Force members, agreed to facilitate that process and work together toward long term goals.

Many industry leaders in robocall mitigation have concluded that there is no “silver bullet” to solve the problem. However, 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 organizations focused on continuing work in the same areas identified by the Industry Strike Force during the first sixty days:

- Authentication
- Empowering Consumer Choice
- Detection, Assessment, Traceback and Mitigation
- Regulatory Support

Each organization met with their members on a regular basis and the organizations held planning meetings at least twice a month. Additionally, monthly meetings were held with all strike force members.

Over the past six months much additional progress has been made and is outlined in this report. Additionally, this report will summarize how the industry will continue its efforts.

1.2. Description of Organizations and Membership

1.2.1. ACT | The App association (“ACT”) represents more than 5,000 app makers and connected device companies in the mobile economy. Organization members leverage the connectivity of smart devices to create innovative solutions that make our lives better. ACT is the leading industry resource on market strategy, regulated industries, privacy and security.

1.2.2. ATIS is a technology and solutions development organization that brings together global ICT companies to advance the industry’s pressing business priorities. In addition to the extensive work being done by ATIS and its members to address caller ID spoofing and robocalling, ATIS’ nearly 200 member companies are also working to address 5G, Cybersecurity, Smart Cities, the evolution to content optimized networks (eCON), the Connected Car, NFV, unmanned aerial vehicles, emergency services, M2M, quality of service, billing and operations, and more. These priorities follow a fast-track lifecycle of development—from design and innovation through standards, specifications, requirements, business use cases, software tool kits, open source solutions, and interoperability testing.

ATIS also is a founding partner and the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), the global collaborative which has developed the Long Term Evolution (LTE) and LTE-Advanced wireless specifications. It is also a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL).

ATIS’ membership is diverse and includes participants from key service providers and vendors, including the following 21 of the 33 Strike Force members: AT&T, Bandwidth.com, Blackberry, CenturyLink, Charter, Comcast, Cox, Ericsson, FairPoint, GENBAND, Google, Inteliquent, LG, Nokia, Qualcomm, Samsung, Sprint, T-Mobile, U.S. Cellular, Verizon, and West.

1.2.3. CTIA represents the U.S. wireless communications industry. With members from wireless carriers and their suppliers to providers and manufacturers of wireless data services and products, the association brings together a dynamic group of companies that enable consumers to lead a 21st century connected life. CTIA members benefit from its vigorous advocacy at all levels of government for policies that foster the continued innovation, investment and economic impact of America’s competitive and world-leading mobile ecosystem. The association also coordinates the industry’s voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry’s leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

CTIA created a Robocall Working Group (RWG) in early November 2016, shortly after the October 26th release of the Initial Strike Force Report. Since November of last year, CTIA has engaged in weekly meetings of the RWG, and has facilitated members’ substantial progress on making robocall control mechanisms and techniques available to consumers.

Of the 33 Strike Force participants, 15 are CTIA members who participate actively in CTIA’s RWG. Participating members are: Apple, AT&T, Bandwidth, Ericsson, Inteliquent, LG, Nokia, Qualcomm, Samsung, Sprint, Syniverse, T-Mobile, US Cellular, Verizon, West. These members span the wireless ecosystem and include carriers, VoIP providers, handset and equipment vendors, infrastructure suppliers and system aggregators.

1.2.4. USTelecom is the premier trade association representing service providers and suppliers for the telecommunications industry. USTelecom members provide a full array of services, including broadband, voice, data and video over wireline and wireless networks. USTelecom’s members are comprised of companies of all sizes—urban and rural, publicly traded, privately held, and cooperatives. Collectively, these companies have a distinguished history of serving America’s communications’ needs.

USTelecom members have long demonstrated their commitment to finding solutions to mitigate robocalls. USTelecom’s member companies understand and appreciate the annoyance and potential monetary harms inflicted on

consumers and businesses resulting from illegal robocalls. USTelecom has a long track record of working with consumer, industry and regulatory stakeholders on ways to mitigate such harms, and has developed strong relationships with law enforcement agencies at the local, state and Federal level. The association has also established an industry working group of more than 20 companies that are committed to working together to fight the robocall problem.

2. Authentication and Other Technical and Operational Work (ATIS)

The October 26, 2016, Robocall Strike Force Report (Initial Strike Force Report) noted the significant work that ATIS and its members have done to address issues associated with robocalling and caller ID spoofing. In addition to recognizing the significant progress made as of October 2016, the report also acknowledged the work that ATIS had underway to further resolve technical and operational impacts. This report provides a progress update on these efforts, including a summary of the significant work completed since October and the on-going efforts to craft technically feasible and broadly implementable mitigation tools. As ATIS has noted in its monthly updates to the Strike Force, work to address robocalling and caller ID spoofing began long before the Strike Force was assembled; this work will not stop when the Strike Force ends. However, because of the focus of the strike force and the commitment from the strike force members, ATIS has been able to accelerate its timeline.

2.1. Introduction and Background

ATIS is examining issues associated with robocalling and caller ID spoofing from a number of different perspectives:

- *Technical work.* On the technical front, one of the main focuses of ATIS' work has been the development of the SHAKEN framework and associated governance structure by the ATIS and SIP Forum Joint Network-to-Network Interoperability Task Force (Joint IP-NNI Task Force). However, ATIS' technical work also includes projects undertaken by ATIS' Packet Technologies and Systems Committee (PTSC) and the Joint IP-NNI Task Force to examine SHAKEN-related Best Practices, Attestation and Origination Identifiers and to develop a framework for the display of verified caller ID; as well as PTSC efforts to: (1) examine the feasibility of using Vertical Service Codes to identify unwanted robocalls; and (2) further analyze its initial recommendations for Integrated Services User Part (ISUP) screening indicator interworking.
- *Testing.* The ATIS Testbed Focus Group has also worked on technical issues associated with the testing of SHAKEN, including the development of SHAKEN test plans. ATIS has also partnered with Neustar Trust Labs to offer the ATIS Robocalling Testbed, a virtualized testbed to advance industry efforts to mitigate unwanted robocalls and caller ID spoofing.
- *Operational Work.* ATIS' Next Generation Interconnection Interoperability Forum (NGIIF) is examining SHAKEN and the proposed governance authority framework to provide operational guidance to facilitate implementation by the industry.
- *Numbering-related impacts.* ATIS' Industry Numbering Committee (INC) is examining potential impacts from the implementation of SHAKEN, the SHAKEN governance framework, and the potential use of vertical service codes to report unwanted robocalls.

Finally, ATIS notes that it has continued to collaborate with other key stakeholder organizations, including CTIA, USTelecom and ACT to share progress and foster cooperation.

2.2. SHAKEN Framework

ATIS continues to make progress on technical issues and operational issues associated with the Signature-based Handling of Asserted information using toKENs (SHAKEN). This work includes publication of the SHAKEN framework, as well work to facilitate industry implementation of this framework.

2.2.1. SHAKEN Framework Publication

As noted in the Initial Strike Force Report, ATIS and the SIP Forum accelerated their development of the SHAKEN framework.¹

¹ Strike Force Initial Report, Section 1.10.1.

ATIS and the SIP Forum successfully completed the efforts on this framework, concluding with its availability in December 2016 and formal publication in January 2017.² The SHAKEN framework provides a mechanism for managing the deployment of Secure Telephone Identity (STI) technologies with the purpose of providing cryptographic authentication and verification of telephone numbers associated with calls traversing Internet Protocol (IP)-voice networks. This specification defines the framework for telephone service providers to create signatures in Session Initiation Protocol (SIP) and validate those signatures at the call termination. It defines the various classes of signers and how the verification of a signature can be used toward the identification of illegitimate uses of telephone numbers.

The document has broad industry support, having been approved by both ATIS and SIP Forum under their respective transparent, consensus-based approval processes. Initial feedback has been positive. This document is available to the industry electronically at no charge.³

2.2.2. SHAKEN Operational Guidance

A related ATIS work program not referenced in the Initial Strike Force Report was the development and publication of a document providing operational guidance for interoperability when implementing the SHAKEN framework.

ATIS NGIIF developed *Interoperability Standards between Next Generation Networks (NGN) for Signature-Based Handling of Asserted Information Using Tokens (SHAKEN)* as a companion to the SHAKEN framework. It provides Next Generation Network (NGN) telephone service providers with a framework and guidance for interoperability as calls process through their networks implementing SHAKEN technologies ensuring the mitigation of illegitimate spoofing of telephone numbers. This document was published in January 2017. This document is available to the industry electronically at no charge.⁴

2.3. SHAKEN Authentication/Verification/Attestation Best Practices and Additional STIR Use Cases

In the Initial Strike Force Report, it was noted that ATIS was working on the creation of SHAKEN-related Best Practices that carriers would maintain.⁵ Work is progressing on these two initiatives within the Joint IP–NNI Task Force.

The first is focused directly on SHAKEN Best Practices. It describes how SHAKEN should be deployed along with guidance on implementing the authentication and verification functions. It shows how SHAKEN components would map onto the network under representative deployment scenarios.

The second initiative is focused on the SHAKEN Attestation and Origination Identifiers, which were discussed in Section 1.5 of the Initial Strike Force Report.⁶ This work focuses on how the service provider decides what level of attestation is appropriate, as well as provides guidance on how the Orig ID can be used to help with traceback. This document describes problems associated with originating party spoofing in IP communication networks, identifies potential options and/or Best Practices related to attestation and the use of the origination identifiers, and analyzes the pros and cons of mitigation options.

While work has progressed, there remains a good deal of work to be completed. ATIS and the industry remain committed to completing this work and hope to complete this by end of 2017.

2.4. Joint Lab Prototype Testing

As noted in the Initial Strike Force Report, ATIS had agreed to further progress its work to facilitate prototype testing of SHAKEN.⁷ Since the publication of the initial report, ATIS launched a virtualized testbed to advance industry efforts to mitigate illegal robocalls and caller ID spoofing.

The ATIS Robocalling Testbed, hosted by the Neustar Trust Lab, allows the testing of SHAKEN by generating end-to-end calls that include all network functions.

²A pre-publication draft was made available in December 2016; final industry approval and publication occurred on January 6, 2017.

³This document is available electronically at no charge from the ATIS Document Center at <https://www.atis.org/docstore/product.aspx?id=28297> and from the SIP Forum at <https://www.fcc.gov/news-events/events/2016/10/second-meeting-industry-led-robocall-strike-force>.

⁴This document is available electronically at no charge from the ATIS Document Center at: <https://www.atis.org/docstore/product.aspx?id=28298>.

⁵Initial Strike Force Report, Section 10.1.7

⁶Section 1.5 of the Initial Strike Force Report addresses this issue but does not identify a specific long-term objective associated with this action. Nonetheless, the industry has been working on a related deliverable.

⁷Initial Strike Force Report, Section 1.0.4.

The testbed allows service providers and vendors to test their implementations of SHAKEN in a test environment to ensure full interoperability. The testbed can provide various configurations to test individual SHAKEN components or complete network implementations.

The test plans were developed by the ATIS Testbed Focus Group in parallel with the development of the SHAKEN framework. This work started well before the Strike Force, and will continue as the best practices documents identify additional areas for testing. Updates to the test plans to cover extensions to SHAKEN are being considered by the ATIS Testbed Focus Group.

Testing of SHAKEN via the ATIS Robocalling Testbed will be provided at no cost to the industry through the end of 2017. Membership in ATIS is not required—any service provider with an assigned Operating Company Number (OCN) is eligible to participate. Other parties, such as equipment manufacturers, may participate if they have solutions relevant to the SHAKEN framework available to test.

There has been active outreach to organizations that have previously expressed interest in SHAKEN testing. ATIS notes that active testing is underway. To date, approximately 10 companies have executed or are in the process of executing the relevant agreements to test, and a total of 16 companies have executed the testing NDA that would allow possible future participation in testing.

Strike Force members and others interested in learning more about the ATIS Robocalling Testbed may visit <https://www.neustar.biz/atis-testbed/index.php>.

2.5. Governance Model and Certificate Management Policy Framework

In addition to the development of the underlying technical framework (*i.e.*, SHAKEN), there is work underway to advance the governance model associated with this framework. The three initiatives below would define the ecosystem in which end-to-end cryptographic authentication and verification of the telephone identity would occur.

2.5.1. Governance Model/Framework

One of the long term goals identified in the Initial Strike Force Report was to further progress the SHAKEN governance model.⁸ Significant progress has been made on this deliverable by the Joint IP–NNI Task Force.

The SHAKEN governance model identifies the key roles/functions involved in distributing and managing SHAKEN certificates. The model envisions a governance authority that would oversee a policy administrator, which would determine who is entitled to get SHAKEN certificates, which would be issued by certificate authorities.⁹ The chart below provides a high-level view of the various roles, including what is currently addressed by the governance model (“in scope”) and what is being defined through other work (“out of scope” for the framework but addressed in section E.3 below).

⁸Initial Strike Force Report, Section 1.10.7.

⁹The Initial Strike Force Report identified the role of the TA Administrator, which would do the manual process of working with service providers to validate they are who they say they are and manage credentials of Telephone Authorities to have a secret key and the Service Providers to do Certificate Signing Requests (CSR) transactions with the Telephone Authorities. This role is now defined under the draft framework as the STI Policy Administrator.

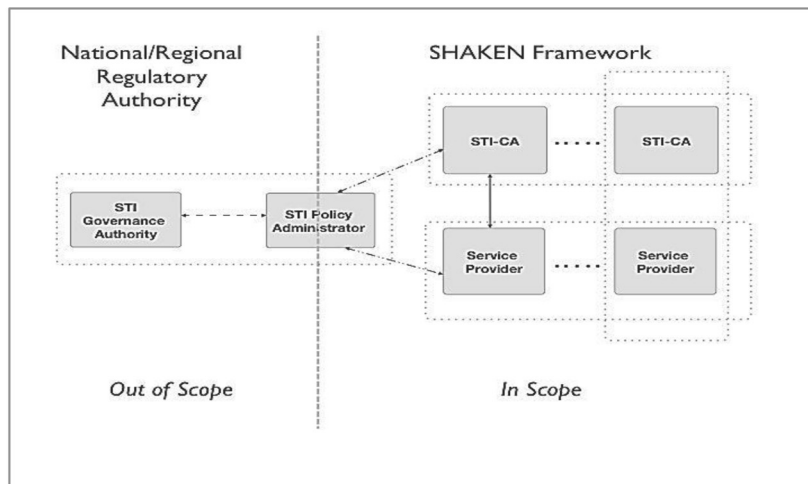


Chart 1 -- SHAKEN Governance Model

The model would specify the protocols that will be used to obtain certificates and the “key” that service providers will obtain from the STI Policy Administrator to prove that they are entitled to get SHAKEN certificates. ATIS notes that, while this model identifies at a high-level the functions associated with the STI Governance Authority and policy administrator, it does not specify the structure of, or detailed functions associated with, the STI Governance Authority or STI Policy Administrator.

The work to ensure that the proposed model results in an implementable solution that is both technically and operationally feasible has been complex. Proposals to align with existing service provider certificate management processes are expected to facilitate and expedite implementation. This work is expected to be completed in 2Q2017.

2.5.2. Framework Operational Guidance

ATIS NGIIF is developing a document examining the operational implications of the SHAKEN governance model and certificate management. This document will complement the governance framework currently under development by the Joint IP-NNI Task Force (see section E.1 above). The target is to align the publication date with Joint IP-NNI Task Force governance document.

2.5.3. Governance Ecosystem

ATIS is also working with its members to identify the detailed functions associated with the governance framework. This work will complement the governance framework document by examining the ecosystem that will be necessary to implement that framework by defining in a more granular fashion the roles of the STI Governance Authority and STI Policy Administrator. This work, which is expected to result in consensus-based proposal for the structure of the ecosystem that would be necessary to support the implementation of SHAKEN by the industry, is expected to be completed in 2Q2017.

2.6. Display Framework

The Initial Strike Force Report noted the work that ATIS had underway to further progress its Signaling Verification and Analytics Information, and Display Framework.¹⁰ The industry continues to make progress on the draft *Framework for the Display of Verified Caller ID*. Additionally, ATIS notes that there are other initiatives within the Joint IP-NNI Task Force to: (1) assess mechanisms to signal verification to legacy call display; and (2) provide input to 3GPP and track progress on “verstat” TEL URI parameter to signal verification to SIP client. All three deliverables are anticipated to be completed by the end of 2017.

¹⁰Initial Strike Force Report, Section 1.8.

2.7. Feasibility of Using Vertical Service Codes to Report Unwanted Robocalls

The Initial Strike Force Report recommended that ATIS investigate the feasibility of using vertical service codes (i.e., *XX codes) to report unwanted robocalls.¹¹ Two initiatives are under development on this topic.

The first initiative is being undertaken by ATIS PTSC. Its objective is to examine the feasibility of using these codes to report unwanted robocalls, including whether codes in use for other services (such as *57-Call Trace) could be used, the benefits and challenges of sharing codes and/or selecting a new code and effective alternatives to the use of vertical service codes. The PTSC (and subsequently Joint IP-NNI Task Force) reviewed contributions on the use of VSC and agreed with the preference to use alternative methods to report robocalls, such as using web portals and smartphone apps, rather than using VSC.

ATIS INC has also examined this issue and will address any numbering related impacts, including the development of and/or revision of industry guidelines should the use of an existing or new vertical service code be recommended. INC's initial review of the existing framework draft identified no unusual numbering-related impacts from the use of these codes.

2.8. Technical Review on SS7 Feasibility

As noted in the Initial Strike Force Report, ATIS' *Technical Report on Use of the ISUP Screening Indicator for Conveying Caller ID Authentication Information* was completed in October 2016.¹² This Technical Report assessed three potential industry solutions for using the ISUP Screening Indicator to convey Caller ID Authentication information. The industry Strike Force evaluated these potential solutions and identified one of the proposed solutions¹³ as the most viable, in that it would provide the greatest integrity of the Calling Party Number (CgPN), while being the least impactful to existing customer expectations with respect to delivery of CgPN.

Based upon the completed work and the input from the Strike Force, ATIS PTSC has initiated a project to further analyze one of its recommendations for ISUP screening indicator interworking. This work has been targeted for completion by the end of 2017.

2.9. Other ATIS Strike Force Work

In addition to the work projects described above, ATIS has also worked cooperatively with the other stakeholder organizations on Strike Force matters. ATIS has provided feedback, for example, to the USTelecom Industry Traceback Group (ITB Group) on Canadian service provider interest in the group, resulting in a new service provider participant.

ATIS has provided feedback from ATIS INC to this group noting that 555 numbers may be good candidates for Do Not Originate trials. These numbers should not be used for any natively legitimate purpose to originate calls, and thus any originating use would identify the call as spoofed.

2.10. Conclusion

ATIS notes that the efforts to mitigate robocalling and caller ID spoofing are complex, with a significant number of interdependencies. However, ATIS and its members are committed to addressing these issues with the requisite urgency, including relevant work outside of those projects identified in the Initial Strike Force Report. ATIS' work is a careful balance of the need for quick action with the need to develop implementable, technically-and operationally-effective and sound mitigation techniques that reflect the consensus of the industry.

3. Empowering Consumer Choice

Consumer choice is critical to effectively managing illegal robocalls. Many marketing, charitable and other communications are wanted and lawful, while unscrupulous telemarketers abuse technology and flout the law. Consumers should be empowered to better control their communications. Fortunately, mitigation tools are available in the form of applications that are providing increased options to con-

¹¹ Initial Strike Force Report, Section 2.5.2. Although VSCs are originally defined for TDM networks, concepts could be extended to SIP networks for SHAKEN.

¹² Initial Strike Force Report, Section 1.10.3. This ATIS technical report is available from the ATIS Document Center at: <https://www.atis.org/docstore/product.aspx?id=28295>.

¹³ This solution involves the successfully verified signed PAI or FROM headers, attesting that the device can use the TN, being interworked into the CgPN with a SI value of "user provided, verified and passed," but differs from other solutions in that, if the PAI or FROM headers are not signed, a "network provided" number (e.g., pseudo number that is unique to each carrier) is populated into the outgoing ISUP CgPN parameter with an indication of "network provided" in the SI field.

sumers. And industry associations are acting as force multipliers for company efforts and consumer education.

3.1. App Development (ACT)

As the world has quickly embraced mobile technology, the hyper-competitive app ecosystem continues to produce more innovative and more efficient solutions that leverage mobile technologies to drive the global digital economy across modalities and segments, augmenting consumer interactions and experiences throughout their personal and work lives.

Service providers, manufacturers, app developers, government, and consumers all have a role in reducing unwanted robocalls. ACT agrees that third-party apps can play a critical role in empowering consumers to control robocalls. As a part of our commitment to stop unwanted robocalls, ACT, representing the developer community, has worked within the Strike Force to support the development of more effective apps to increase consumer control over robocalls. ACT has completed three key deliverables following the completion of the Strike Force. They are:

- A public-facing website that provides technical information and recommendations for current and potential robocall control app developers, including technical updates related to changes to information provided by networks and vendors on call spoofing or signaling systems that applications can harness. The website provides app developers information on privacy and privacy policy best practices. ACT designed this information to make it easy for app developers to capitalize on the approaches developed by the Strike Force and to create innovative new solutions.¹⁴
- Targeted outreach to the ACT's members, including more than 5,000 app companies and IT firms from across the mobile economy to educate members about opportunities to develop robocall control apps.
- An online workshop for developers offering both real-time participation and access to ACT's archives. The workshop will work to catalyze the creation of new apps by helping developers quickly get up to speed on the technical and policy considerations behind robocall control apps.¹⁵

ACT is pleased to satisfy its obligations as part of the Strike Force, and we are proud of the incredible work every member has contributed in taking meaningful steps to contribute to the mitigation of unwanted robocalls.

While further innovative apps are in development, apps today are already playing a major role in mitigating unwanted robocalls (examples include AT&T Call Protect, Nomorobo, Hiya, PrivacyStar, and many others), and will continue to do so. We encourage developers, consumers, and other stakeholders to explore the apps available today; and to collaborate and develop innovative apps to mitigate unwanted robocalls.

As discussed in this report, the Robocall Strike Force is examining the development of a standardized framework for delivering information from networks to devices with the aim of better empowering consumers to make informed call handling decisions. Moving forward, ACT will continue to encourage its members to rely on these important consensus documents as they find new and innovative ways to provide for consumers to take control over robocalls.

3.2. Consumer Education Efforts by Strike Force Members

3.2.1. Wireless

The wireless sector has been actively working to address abatement of illegal robocalling, and promoting consumer awareness of existing tools.

With release of the Industry Strike Force Report, CTIA convened the RWG and immediately began work on wireless stakeholder engagement, working with other trade associations, and committing to and providing regular updates to the Industry Strike Force. Specifically, since CTIA convened its RWG:

- CTIA has highlighted and facilitated members' efforts to keep their consumer-facing robocall prevention content current in collaboration with Industry Strike Force initiatives.
- CTIA conducted a survey of its members to learn about spam-scoring services available in the marketplace today.
- CTIA convened six third party vendor presentations to educate members on innovative robocall mitigation techniques.

¹⁴<http://actonline.org/2017/03/28/robocalls-app-developers/>

¹⁵*Id.*

- CTIA has integrated a robocall mitigation use case into its ongoing Automated Cyber-Threat Information Sharing (AIS) Pilot being sponsored by CTIA's Cybersecurity Working Group.
- CTIA is working with members on the best ways to display verified caller ID information graphically on a user's handset.

CTIA's consumer education efforts have been robust and effective. CTIA's webpage on Robocall Mitigation provides a comprehensive list of well over 80 mitigation apps and step-by-step video instructions for Android, BlackBerry, iOS and Windows devices. Many, if not most, of these apps are free. Carriers often refer their customers to the CTIA website to guide consumers to the rich variety of available third-party apps. Likewise, CTIA and other associations have supported ACT in its efforts. CTIA has updated its website to contain references to numerous tools, including apps, as well as important consumer tips. Go to: <http://www.ctia.org/your-wireless-life/consumer-tips/blocking-robocalls>.

- In March 2017 alone, CTIA's robocall consumer tip pages received over 15,000 views
- Since November 2016, CTIA's robocall consumer tip pages has received an average of nearly 10,000 views each month

Several carrier and vendor members of CTIA's RWG have their web resources on robocall mitigation mirrored on the dedicated FCC Resource webpage: <http://fcc.gov/unwanted-calls>. In turn, CTIA uses social media to heighten public awareness on robocall mitigation. CTIA also facilitated members' efforts to keep their consumer-facing content current in collaboration with Industry Strike Force initiatives.

CTIA looks forward to continuing to support the efforts of the Industry Strike Force and other industry efforts. Attention will be directed to authentication, empowering consumer choice, and efforts to automate what are today the largely manual and iterative Traceback and/or Do Not Originate processes, which are described in detail below.

CTIA considers illegal robocalling to be a potential cyber threat. So, looking ahead to automation, CTIA has integrated a robocall mitigation use case into the ongoing Automated Cyber-Threat Information Sharing (AIS) Pilot sponsored by CTIA's Cybersecurity Working Group. This pilot seeks to build toward automated examination and sharing of call detail records associated with suspected robocalls to inform Traceback and Do Not Originate capabilities.

3.2.2. Wireline

After the initial meeting of the Industry Strike Force at the FCC on August 19, 2016,¹⁶ USTelecom worked with its association members and Strike Force participants to increase consumer awareness on robocall issues. After the conclusion of the first Strike Force meeting, USTelecom and CTIA, in coordination with the FCC, published consumer-centric websites providing them with information on robocall issues, including consumer tools available to them.¹⁷

USTelecom's webpage includes a broad variety of consumer-centric information regarding robocalls, including consumer safety tips and robocall mitigation tools. The website also includes a link to several tools available to consumers to block and/or mitigate robocalls on a range of consumer voice platforms, including traditional TDM networks, IP networks and wireless services.¹⁸ A link to USTelecom's website is also available through the FCC's robocall portal. Several consumer groups and other organizations also maintain resources on their respective websites educating consumers about robocall issues.¹⁹ In addition, several companies participating in

¹⁶See, Public Notice, FCC to Host First Meeting of Industry-Led Robocall Strike Force, DA 16-917 (August 12, 2016); see also, FCC website, First Meeting of Industry-Led Robocall Strike Force (available at: <https://www.fcc.gov/news-events/events/2016/08/first-meeting-industry-led-robocall-strike-force>) (visited March 30, 2017).

¹⁷See, USTelecom website, Robocalls (available at: <http://www.ustelecom.org/issues/robocalls>) (visited April 22, 2017); see also, CTIA website, How to Stop Robocalls (available at: <http://www.ctia.org/consumer-tips/robocalls>) (visited April 22, 2017).

¹⁸See, USTelecom website, Robocalls (available at: <http://www.ustelecom.org/issues/robocalls>) (visited April 25, 2017).

¹⁹See e.g., Consumer Reports, *Robocall Blocker Review*, August 14 (2015) (available at: <http://www.consumerreports.org/cro/magazine/2015/07/robocall-blocker-review/index.htm>) (visited April 25, 2017); see also, AARP website, Robocalls (available at: <http://blog.aarp.org/tag/robocalls/>); AARP website, Scam Alert (available at: <http://blog.aarp.org/2014/08/01/how-to-avoid-robocall-scams/>) (visited April 25, 2017); FTC website, *Consumer Information, Robocalls* (available at: <https://www.consumer.ftc.gov/features/feature-0025-robocalls>) (visited April 25, 2017).

the Industry Strike Force have also taken steps to educate customers about robocalls, as well as make mitigation tools available to consumers on their company websites.²⁰

There is strong industry support for increased consumer education about robocalls, to include increasing awareness of the threat, as well as tools available to consumers. Such an approach can have a tangible and positive impact on robocall issues, and educational outreach has been previously identified by the FCC and the Federal Trade Commission as an essential component to raising awareness of this issue.²¹ Public outreach measures have been successfully implemented by the Federal government in the past and are ideally suited in the current context. Whether implemented on a broad public relations scale, or through targeted multi-industry efforts, such outreach measures ensure that valuable information is disseminated and shared amongst target audiences.

3.3. Industry Input from Non-Strike force members

3.3.1. Wireless

CTIA has worked to bring non-members into the discussion and activity on illegal robocall abatement. CTIA convened numerous meetings to share technology and solutions. As discussed in the October Strike Force report, CTIA undertook the task of working with members to provide robocall mitigation information to customers.

CTIA surveyed its RWG members and learned about spam-scoring services in the market today. As noted, CTIA then reached out to the third party vendor community, and facilitated presentations from six companies to the RWG regarding robocall mitigation opportunities. The companies below presented:

- Cequent: Provides spam scoring, based on real-time network data analytics to ensure that legitimate enterprise calls to customers are not placed incorrectly on a blacklist. <https://www.cequent.com/personal/>
- Hiya: Provides network-based caller ID and spam detection and protection natively integrated for all clients, and O/S platform independent. <https://hiya.com/#page-top>
- iconectiv: Certified Caller ID: Demonstrated the process of certificate assignment (and revocation) pursuant to STIR/SHAKEN protocol. <http://iconectiv.com/thought-leadership/existing-robocalling-and-spoofing-mitigation-techniques>
- Neustar: Smart ID product, which integrates APIs on: CNAM (to include business logos); subscriber insights; and certified caller ID. Includes Neustar's Trust Lab, selected by ATIS as its Robocalling Test Bed. <https://www.neustar.biz/communications/caller-id>
- Nomorobo: A wireless, network-agnostic application based on new API capabilities available with the release of iOS 10 and higher. A nominal subscription-based service, it allows the download of updated number blacklists to the iPhone. <http://www.nomorobo.com/>
- PrivacyStar, a First Orion company: Originally app-based, expanded their in-network deployments which leverage data analytics and call heuristics to aid in call labeling and categorization and offer consumers more information to reduce blocking of "wanted" robocalls (pharmacy, school, enterprise). <https://www.privacystar.com/>

CTIA and its members are encouraged by the level of communication about these issues, and look forward to pressing forward on new solutions and approaches, in-

²⁰See e.g., AT&T website, *Call Blocking options: Nomorobo* (available at: <https://www.att.com/esupport/article.html#!/u-verse-voice/KM1074689>) (visited April 25, 2017); CenturyLink website, *Ways to block unwanted calls from your home phone* (available at: <http://www.centurylink.com/home/help/products/calling-features/ways-to-block-unwanted-calls-from-your-home-phone.html>) (visited April 25, 2017); Verizon website, *What are robocalls* (available at: <https://www.verizon.com/support/consumer/consumer-education/robocalls>) (visited April 25, 2017); Frontier website, *Call Block & Priority* (available at: <https://frontier.com/helpcenter/categories/phone/calling-features/call-block-priority-residential>) (visited April 25, 2017).

²¹See e.g., Public Notice, FCC to Host Consumer Webinar on Dealing with Robocalls (released February 2, 2017); See e.g., Comments of FTC Chairman Jon Leibowitz, FTC Robocall Workshop, October 18, 2012 (noting that the FTC "pride ourselves on the fact that we take a multi-faceted approach to consumer protection issues that includes enforcement, education, policy, and advocacy." (available at: https://www.ftc.gov/sites/default/files/documents/public_events/robocalls-all-rage-ftc-summit/robocallsummittranscript.pdf) (visited April 25, 2017). See also, FTC website, *Phone Scams* (available at: <https://www.consumer.ftc.gov/articles/0076-phone-scams>) (visited April 25, 2017); FCC website, *Unwanted Calls* (available at: <https://www.fcc.gov/unwanted-calls>) (visited April 25, 2017).

cluding those developed by third parties. In fact, some CTIA members already make services from these third party vendors available to their customers.

3.3.2. Wireline

Since the start of the industry-led Strike Force efforts, USTelecom has also made significant outreach and inroads to non-Strike Force members. For example, in January, 2017, USTelecom met with representatives from Duke Energy, which is leading a coalition of approximately 90 electric utility organizations called “Utilities United Against Scams” (Utilities Coalition). The Utilities Coalition was formed last year by Duke Energy to address and combat ongoing fraud targeted towards electric utility customers through illegal robocalls. The calls would fraudulently advise consumers that their electricity services would be cut off, unless payment was immediately submitted.

In January, 2017, USTelecom delivered a presentation to the coalition regarding the ITB Group²² efforts, and USTelecom will also be attending its first face to face meeting in Fort Worth, Texas in May. In addition, USTelecom was able to facilitate discussions between the Utilities Coalition and other industry partners in order to shut down several toll free numbers that were hosting fraudulent interactive voice response (IVR) systems that were spoofing legitimate electric utility companies. Fraudsters were using the spoofed IVR systems to facilitate communications between targeted consumers and the scammers (*i.e.*, consumers were led to believe they were contacting legitimate electric utility companies).

As a result of this coordination, the Utilities Coalition was able to identify toll free numbers being used in the IVR scams and have them removed from service. This industry-wide coordination is ongoing, and the group is working to establish a more streamlined and effective system for electric utilities to remove these fraudulent IVR numbers from service on an expedited basis.

In addition to this effort, USTelecom continues its outreach and coordination with various Federal agencies regarding areas of potential cooperation. For example, USTelecom staff met with IRS investigators in September, 2016, to discuss the IRS scam, and additional cooperation between industry and the agency. As a result of these efforts, USTelecom staff conducted in-person training for Treasury Department staff, including Treasury Inspector General for Tax Administration (TIGTA) personnel on November 9, 2016. The class, “Telephony 101 and Robocall Fundamentals” provided Treasury Department personnel with an overview of how telecom networks function, the nature of robocalling, the wide variety of robocall schemes and industry traceback efforts.

These efforts are ongoing, and in addition to the IRS, USTelecom has coordinated with Health and Human Services and Immigrations and Customs Enforcement on industry-led efforts to combat robocalls. Finally, USTelecom has also conducted outreach to various industry stakeholders engaged on the robocall issue. For example, USTelecom has met on several occasions with various stakeholders deploying robocall mitigation tools, including several vendors of telecommunications services. USTelecom intends to continue this outreach and coordination in the coming year.

3.4. Network to Device Display

3.4.1. Wireless and other IP-based Networks

The telecommunications industry has been working on the complexities surrounding on-device displays about illegal robocalling. To date, industry efforts on Robocall Mitigation have focused on the transmission of “verified Caller ID” using the “STIR/SHAKEN” framework where a SIP-based network is available, *e.g.*, a VoLTE network supporting wireless subscribers. Using this protocol can enable a carrier to determine if an originating service provider has authenticated a particular telephone number. Industry has been considering how verified Caller ID information can and should be displayed on a user’s wireless handset to enable real time decision making by consumers about incoming calls. Questions include whether there should be standardization with respect to a minimum set of display requirements or whether that is best left to the network, OEM and app communities.

Industry participants are investigating how an OEM or carrier can graphically display verified caller ID information on the user’s handset. Work on network-to-device display is in early stages and ongoing. CTIA is working with its carrier, handset and system vendor members, and standards organizations, on how to best display information to the consumer about an incoming call. Considerations include

²² See sections below, “USTelecom Efforts on Detection, Assessment, Traceback and Mitigation” and “USTelecom Status of Traceback Initiatives” for further details on the ITB Working Group.

whether minimum set of requirements for network-to-device display is preferred, versus giving carriers greater flexibility to pursue innovation in graphical design from the handset, system vendor, and carrier communities.

3.4.2. Wireline

On the wireline side, substantial innovation is ongoing to address the display challenges associated with existing customer premises equipment. For example, for several months Verizon has been trialing, to millions of its wireline customers, a new service that warns about potential spam by inserting a warning indication in the Caller Name field of the home user's phone display that the incoming call may be spam related. One advantage of this approach is that because it rides on the CNAM database that carriers use to associate a calling party name with a particular telephone number, it uses the customer's existing 15-character display, and it does not require either a VoIP connection or the transmission of a new SS7 field. This trial is an implementation of the patented prototype technology that Verizon presented to strike force members last fall, which Verizon has offered to share with interested carriers.

3.5. Industry Member Activity

Industry participants and Strike Force members continue to improve and expand mitigation tools to combat illegal robocalling. Much of this work cannot be made public because it would provide too much information to the robocallers but here are some examples of what is being done. The market is working.

- **AT&T:** Launched AT&T Call Protect in December 2016 as a free network service. It allows customers with iPhones and HD Voice-enabled Android handsets to automatically block suspected fraudulent calls. It can flag suspected spam calls so the customer can choose whether to answer or not. And, using the interface provided by the AT&T Call Protect app, customers can manually block an unlimited number of specific telephone numbers for 30-day intervals. The customer can download the app via the AT&T website or on their device through the App Store. Network call data analysis and heuristics that power this solution are provided by Hiya. In addition, AT&T blocked its billionth unwanted robocall in cases where its business contracts allow it to block impermissible traffic using a new program that detects violators through network data analysis.
- **Comcast:** Comcast offers Nomorobo, a free cloud-based service that hangs up on or blocks illegal robocaller or telemarketing calls from calling the intended home telephone number, to its wireline customers
- **Sprint:** Sprint offers Premium Caller ID service on a subscription basis. It now includes, for select Android smartphones, the ability to not only the ability to identify a higher percentage of nuisance calls, but also an option to block them. This solution directly leverages data and network intelligence powered by a partnership with Cequnt, a wholly owned subsidiary of Transaction Network Services (TNS).
- **T-Mobile:** T-Mobile launched Scam ID in March 2017 as a free, network-based automatic service that identifies calls from known phone scammers, across all handset platforms, on smartphones and feature phones. If a scam call is detected, the Caller ID will display "Scam Likely" on the device, giving customers the option to answer, or permanently block the number. Customers that choose to invoke Scam Block, another free service, will have all calls from known scammers blocked. These solutions are powered by network call data analysis and heuristics provided by PrivacyStar, a First Orion company.
- **Verizon:** Verizon has used the CNAM-based solution described above to warn more than four million wireline Fios Digital Voice customers about calls identified by Verizon's analytics engine and its robocall mitigation team, including calls relating to the well-known IRS impersonation scam. Verizon's network team also worked with Nomorobo to develop a "one click" solution that simplifies Fios Digital Voice customers' ability to sign up for that third-party blocking service. And since November 2016, Verizon Wireless has been trialing a service that scores all incoming calls to its Caller Name ID customers, identifying potential spam and calling-out the level of risk with a "risk meter." The service is powered by Cequnt, a wholly owned subsidiary of Transaction Network Services (TNS), and is currently available on ten Android devices. Verizon expects a broader product launch later in 2017.
- **Apple:** Apple introduced CallKit for iOS 10 and higher. API developers can create a call directory app extension to identify and block incoming callers by their

phone number. This opens the iPhone ecosystem to an important call control capability, for devices running iOS 10 and higher, across all service provider networks. <https://developer.apple.com/reference/callkit>

- West: In response to the rise of spam calls, West is working with the various call blocking solution providers to promote decision support tools for the entities whose numbers have been compromised.
- Google: In late 2016, Google introduced spam protection functionality on the Google Phone application for Pixel, Nexus, and Android One devices, which warns users about potential spam callers and provides users with the choice to block and report these numbers. (See, e.g., <https://support.google.com/pixelphone/answer/3459196>) The user interface and reporting aspects of Google Phone spam protection have also been made openly available at no cost to third parties via the Android Open Source Project (<https://source.android.com/>). In addition, there are plans to provide platform APIs in upcoming builds of Android that would offer new forms of spam solution support for carriers and manufacturers.
- Strike Force members worked with the CFCA in developing customer education messaging about how consumer can protect themselves from fraud, including the attached the attached fraud-related message: <https://www.youtube.com/watch?v=rE53QDNP8Is>.

4. Detection, Assessment, Traceback and Mitigation (USTelecom)

In June of 2015, USTelecom formed a Robocall Engineering Working group. USTelecom invited its carrier members to participate in this working group with the goal of easing and simplifying the process of tracing the origins of robocalls, otherwise known as traceback. During the course of these Robocall Engineering Working Group efforts, the group noted that the sharing of certain network intelligence and traceback information among its participants could and did lead to the successful thwarting and mitigation of unwanted and illegal phone traffic. A key lesson learned from USTelecom's extensive experience and leadership in traceback efforts is that with investments in personnel and IT systems, along with providers' contact information for traceback and subpoena requests being readily available, voice providers can establish the systems and processes needed to efficiently process requests (whether government subpoenas or requests from other carriers) to identify the source of suspicious traffic traversing their networks. Unfortunately, while numerous providers have formally joined our traceback efforts, and many others cooperate in good faith in tracebacks, there are still upstream carriers who refuse to cooperate, which prevents carriers from tracing these malicious calling events back to the origin of the call.

In May of 2016, the Robocall Engineering Working group felt it would be beneficial for wide-scale industry participation, and to include service providers from outside of USTelecom's membership in these robocall mitigation efforts. USTelecom therefore developed a framework for participation and governance and began to invite numerous service providers to participate in traceback efforts.

Many service providers accepted the invitation and the terms of the framework. On June 28, 2016, USTelecom conducted the first Industry Traceback Working Group (ITB Group) conference call. There are currently twenty-one members of the ITB Group, which includes traditional wireline phone companies, wholesale carriers, wireless providers, and cable companies. The membership also includes foreign carriers (e.g., Bell Canada), and non-traditional voice providers (e.g., Google). USTelecom will continue to reach out to industry stakeholders in an effort to continue expanding membership in the ITB Group.

The ITB Group conducts biweekly conference calls to discuss malicious calling events that were observed on the members' respective networks. Various network actions and mitigation practices are discussed and shared with the group. Between conference calls, when a malicious calling event occurs on one or more networks, the ITB Group is alerted via e-mails that are sent out by the detecting service provider. The remaining group members conduct network scans, research and analysis to determine if these events are occurring on their respective networks. Each ITB Group member explains their observations, their respective notification actions, network actions, and shares any traceback information with the rest of the working group.

Subsequent to the October meeting of the Industry Strike Force, USTelecom and the ITB Group focused its efforts on completing a Do Not Originate (DNO)²³ trial in order to assess the feasibility of DNO as a robocall mitigation tool. During No-

²³See section below, "USTelecom Status of Do Not Originate Initiatives" for further details on the DNO.

vember and December of 2016, USTelecom staff and individual ITB Group members reached out to relevant stakeholders to identify potential DNO candidates. This included outreach to industry trade associations, individual companies, and government stakeholders. Once suitable candidates for DNO were identified, a series of trials were conducted during January and February of 2017.

Finally, the ability of carriers to institute a DNO varies by ITB Group members. Each ITB Group member oversees a diverse range of network facilities, some of which are more capable of instituting DNOs in a more seamless manner. In addition, the resources and capabilities available to each of the ITB Group members also varies, with some members having fully staffed fraud and network engineering departments operating on a round-the-clock basis. In addition, implementation of DNOs by individual ITB Group members was wholly voluntary throughout this process.

4.1. USTelecom Status of Traceback Initiatives

With the establishment of the ITB Group, efforts were primarily focused on the mechanics and processes for initiating industry traceback efforts. Initial efforts of the group were focused on identifying possible illegal robocall incidents, and threat intelligence was shared between ITB Group members. This initial information sharing effort enabled ITB Group members to scale the scope of suspected robocall incidents, and enabled individual ITB Group member efforts to institute mitigation measures on their own networks to address these call incidents.

As the ITB Group grew in membership size, these information sharing efforts significantly accelerated awareness of such incidents across a broad range of industry stakeholders. In addition, these initial efforts facilitated coordination between individual ITB Group members, who could more easily cooperate on analyzing suspected robocalling events. Also, efforts have been implemented for faster responses to traceback requests, by working in conjunction with ATIS to update ATIS' Service Provider Contact Directory (SPCD).²⁴ The SPCD, available upon request across the industry ecosystem (*e.g.*, service providers, regulators and enforcement bureaus) to provide contact information for reporting or passing along trouble reports to inter-connecting companies, has been expanded to include contacts related to traceback and for subpoena requests. As more providers submit their contact information for the SPCD, traceback efforts can be investigated in a more expeditious manner.

In late 2016 (between November and December), USTelecom staff began exploring enhancements to its initial efforts. These reforms were instituted to make the ITB Group's traceback process more focused and more effective in tracing back specific call paths closer to their point of origin in the network. These reforms included: (1) more targeted traceback requests; (2) expanded outreach to upstream carriers; and (3) detailed cataloguing of information collected during individual tracebacks.

Regarding the first reform, ITB Group members focused on exercising their ability under Section 222(d) of the Communications Act, which allows carriers to share CPNI in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services."²⁵ The sharing of such information by telecommunications providers can benefit consumers by enabling providers 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 carriers' ability to trace calls through several networks can substantially assist law enforcement personnel in subsequent investigations.

Regarding expanded outreach to upstream carriers, USTelecom initiated an effort whereby non-ITB Group upstream carriers were contacted by USTelecom staff. Because any particular call flow can include both ITB Group members, and non-ITB Group members, it was essential to reach out to carriers in the latter category to encourage them to participate in the industry-led effort to identify the source of illegal robocalls.

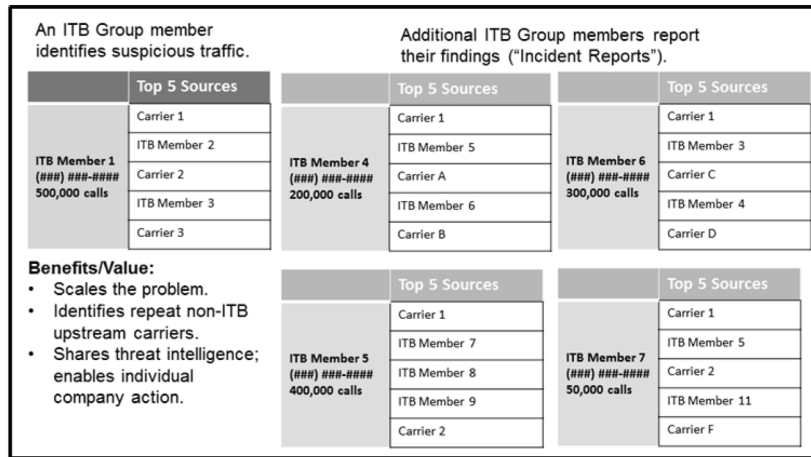
Finally, USTelecom instituted a process whereby the association catalogues certain information relating to traceback efforts by the ITB Group. The information is retained in a password-protected Microsoft Access database by USTelecom. Once a traceback effort is initiated by an ITB Group member, a reference number is assigned for that particular call incident. This information includes the requesting ITB Group member, the date of the calling incident, the date the traceback effort was

²⁴ See section below, "Work with enforcement to shorten the cycle time between identification and action to stop illegal activity" for further details on the SPCD.

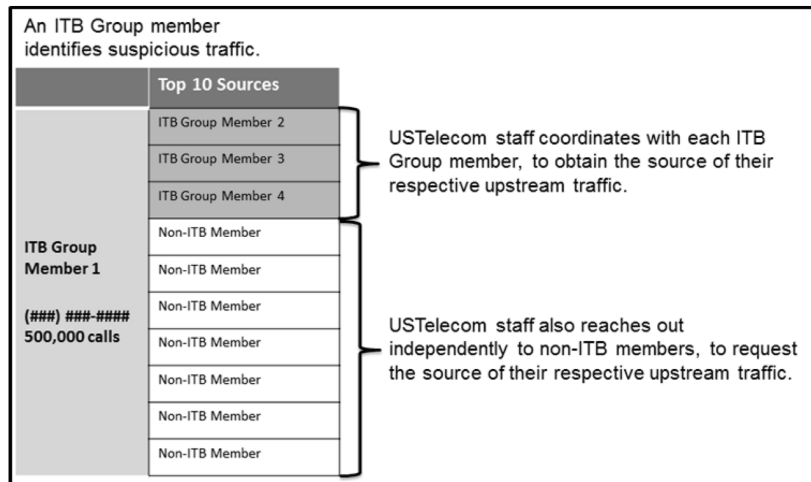
²⁵ 47 USC 222(d)(2).

initiated within the ITB Group, the volume of calls associated with the calling incident, and the phone number associated with the calling incident (Traceback Number).

Once this data is entered, ITB Group members are asked to scan their respective networks for the Traceback Number to see whether it has transited their respective networks. If this is the case, ITB Group members report back to USTelecom with a listing of the top 5 or 10 upstream carriers (that may include both ITB Group members, and non-ITB Group members), as well as associated call volumes (Incident Reports). The Incident Reports from responding ITB Group members are entered into a separate table that tracks upstream carriers and call volumes for the Traceback Number. The general process for this effort is highlighted in the below diagram.

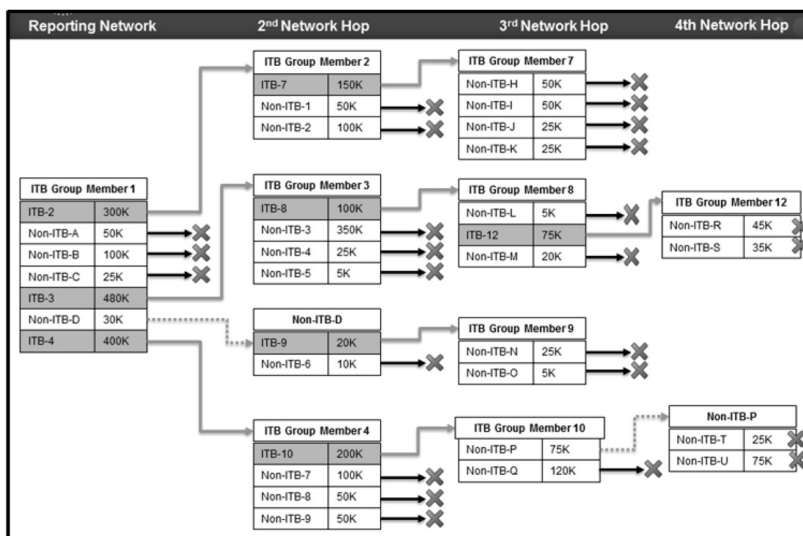


USTelecom will then select an Incident Report from an ITB Group member for an active traceback effort. USTelecom staff coordinates separately with each ITB Group member identified as a source of upstream traffic to obtain the source of their upstream traffic. In addition, USTelecom also reaches out to non-ITB Group members, requesting that the source of their upstream traffic be provided to USTelecom for further traceback efforts. This process is reflected in the below diagram.



This process is repeated through each network hop: USTelecom coordinates with ITB Group members to push back deeper into the network path; while also reaching

out to non-ITB Group members requesting additional traceback information. The process continues, until such point that USTelecom can no longer continue to traceback the Incident Report further into the network path due to the absence of participating ITB Group members and/or non-responsive non-ITB Group members. A sample call path scenario is illustrated below.



In January, 2017, the ITB Group initiated its first traceback effort under the enhanced traceback process. The number at issue involved an IRS-related scam using a non-toll free number. Between January 13, 2017, and January 27, 2017, USTelecom staff identified approximately 70 upstream carriers, and sent approximately forty separate communications to upstream carriers requesting assistance on the ITB Group Traceback efforts (several of these upstream carriers lacked readily available contact information). None of the non-ITB Group members provided actionable information. However, working with just the members of the ITB Group, USTelecom was able to trace the call back through four distinct network hops by the end of the traceback effort.

Finally, USTelecom recently met with staff from the FCC's Enforcement Bureau to discuss the traceback efforts of the ITB Group, and potential handoffs of information collected by the ITB Group during the traceback process. During this initial meeting, USTelecom staff provided FCC personnel with an overview of the enhanced traceback process, discussed areas of potential cooperation, as well as certain challenges faced by industry in these efforts. USTelecom will continue to work with its partners in government and law enforcement, in order to maximize the effectiveness of industry-led efforts.

4.2 USTelecom Status of Do Not Originate Initiatives

On October 26, 2016, USTelecom was directed to complete a report on one component of robocall mitigation efforts known as Do Not Originate (DNO).²⁶ That report was delivered to Strike Force members on March 31, 2017 (DNO Report). The DNO Report provided an overview of the DNO process, including spoofing challenges associated with this approach, as well as DNO's application as a highly specialized tool. It also included a summary of industry efforts on this issue, including the development of USTelecom's ITB Group, and provided an analysis of three completed DNO trials, and the findings from those efforts. It finally discussed lessons learned over the last two months from these DNO efforts, and provides an analysis on the effectiveness and feasibility of DNO.

This is a process whereby certain telephone numbers are identified at VoIP gateways or interconnection points, and prevented from terminating to the end user based upon the originating telephone number. A measured and tightly controlled process is implemented, and can be instituted by some or many carriers. Calls from

²⁶Id., Section 3.2.3, p. 34.

numbers that have been placed on a DNO list are rejected by the first service provider in the call path that has implemented DNO based on the originating telephone number and thus blocked from entering the phone system. This is no substitute for authentication, but USTelecom's testing efforts demonstrated that the process can prevent a certain subset of narrowly defined harmful calls from reaching consumers.

The USTelecom DNO trials demonstrates that applied in a narrow and tightly controlled manner, this can be an effective deterrent in mitigating certain types of large and medium scale attacks. It is important to note that the calls themselves will still route across networks up until the point that the traffic is handed off to a carrier that is instituting a block. Because there are potentially multiple paths for any call to take, the effectiveness of any given effort will rely on the participation rate of carriers. In other words, the more carriers that are instituting a block on a given number, the more effective that particular undertaking will be.

The DNO Report discussed a series of three DNO trials using certain criteria.²⁷ The three completed trials involved efforts involving the Internal Revenue Service, a toll free directory assistance number, and the Immigration and Customs Enforcement agency. A complete analysis of these efforts was provided to the industry-led Strike Force on March 31, 2017.

4.3 The Effectiveness and Feasibility of DNO

Blocking DNO numbers can be an effective tool for addressing certain types of robocalls (specifically, ones where bad actors spoof known "vanity" numbers to impersonate legitimate callers), when it is applied in a narrow and targeted manner. As USTelecom has previously noted, there is no single 'silver bullet' to the robocall problem,²⁸ and the process of blocking DNO numbers should be viewed as one of a growing number of tools available to address the robocall problem. In general, robocalls are best addressed in a holistic manner through deployment of a wide variety of tools by a broad range of stakeholders. These stakeholders include consumer groups (*e.g.*, education/awareness, adoption of consumer-based blocking tools), government entities (*e.g.*, enforcement, education, coordination, regulatory protection), standards organizations (*e.g.*, development of industry standards such as SHAKEN/STIR), and industry (*e.g.*, Blocking DNO numbers, traceback, robocall mitigation tools, etc.).

In particular, this process should be paired with robust traceback efforts in order to ensure that the bad actors whose illegal spoofing is being partially mitigated by these policies can be investigated fully and prosecuted if appropriate. As discussed below, the calls that are candidates for the DNO blocking are often among the most egregious legal violations of all categories of robocalls.

USTelecom concludes that the DNO trials outlined in this report were effective due to the efforts being narrowly targeted towards the specific set of telephone numbers identified and confirmed as inbound-only. That is no guarantee that they will be similarly effective in the future, or that they could be successfully scaled without creating harmful unintended consequences. If DNO blocking procedures were more widely deployed beyond a narrow set of numbers (*i.e.*, inbound-only telephone numbers), bad actors could easily and rapidly transition to randomized and/or legitimate telephone numbers in order to circumvent DNO blocks. In fact, the widespread deployment of a broader range of DNO numbers (*e.g.*, unassigned telephone numbers) could have the perverse effect of quickly nullifying any protections, while also making robocallers more difficult to identify. This could also increase instances of both "false positives" (*i.e.*, blocking numbers that should not have been blocked) and "false negatives" (*i.e.*, fail to block numbers that should have been blocked).

Accordingly, due to the nature of the DNO blocking process (*i.e.*, outright blocking in the network), its use should currently be limited to those instances where the number in question (i) is used by bad actors as part of an impersonation scam, (ii) is confirmed as an 'inbound-only' number using strong vetting procedures that go beyond merely asking the subscriber or its carrier about the number's use, and (iii) appropriate authorizations are obtained from the entity to whom the number is assigned. In addition, the process should also be deployed in a highly controlled environment. Carriers must carefully and continually coordinate with the telephone number owner before and during the entire process, in order to ensure that issues arising from inadvertent blocking of legitimate calls do not arise. As happened dur-

²⁷ See *e.g.*, USTelecom Comments, CG Docket No. 02-278, WC Docket No. 02-278, p. 17 (submitted January 23, 2015) (available at: <https://ecfsapi.fcc.gov/file/60001015988.pdf>) (visited April 22, 2017).

²⁸ See *e.g.*, USTelecom Comments, CG Docket No. 02-278, WC Docket No. 02-278, p. 17 (submitted January 23, 2015) (available at: <https://ecfsapi.fcc.gov/file/60001015988.pdf>) (visited April 22, 2017).

ing one of the trials, legitimate calls will be blocked if any carrier attempts to implement blocks of purported inbound-only numbers without fully vetting the subscriber's understanding that the number is inbound-only.²⁹ Such false positives should of course be avoided in the first instances, and if they do occur they need to be remedied promptly.

In the near term, any widely deployed efforts would likely face significant technical scalability issues, in addition to the policy risks (*e.g.*, incentivizing more spoofing of legitimate numbers in order to get around DNO blocks) discussed above. For example, the network capabilities for all providers operating in today's voice ecosystem varies widely. In some instances, an individual carrier may even have disparate network capabilities within their respective networks (*e.g.*, portions of the network may be TDM, while other portions may be IP-based). As a result, as any centralized list of DNO numbers grows, it may very well exceed the capacity of certain network systems.

In addition, there is currently no centralized method for obtaining blocking authorizations across the universe of network providers. As a result, letters of authority (LOAs) from each number's owner must ideally be sent to each organization seeking to institute a DNO blocking process, since there is currently no form of 'transitive' authorization. In order to implement DNO blocking process on a broader scale, some form of universal LOA would need to be developed. In addition, some form of centralized distribution method for such LOAs would need to be developed, along with a list management framework. Regarding this latter point, any such list would need to be continually monitored and updated as telephone numbers are added to, or removed from, the list of authorized DNOs, while keeping such information out of nefarious hands.

Because of the risks of unintended consequences if the blocking were implemented in an unmeasured way, USTelecom supports the permissive approach outlined by the Commission in its recent Notice of Proposed Rulemaking.³⁰ This is an appropriate starting point for considering its applicability to other categories of phone numbers. Specifically, the Commission's proposal is to permit voice service providers to block telephone calls in certain, narrow circumstances to protect subscribers from fraudulent and illegal robocalls. Under the proposal, the Commission would codify the Consumer and Governmental Affairs Bureau guidance public notice that providers may block calls when the subscriber to a particular telephone number requests that calls originating from that number be blocked.³¹ USTelecom intends to participate in the Commission's rulemaking proceeding, and it is anticipated that this current report to the Industry Strike Force will help to further inform industry's analysis of this proposal.

4.4. *Work with enforcement to shorten the cycle time between identification and action to stop illegal activity*

In October 2016, ATIS completed its work on a process to maintain a contact list for robocall related subpoenas as noted by the Initial Strike Force Report. The list is included as part of ATIS' larger service provider contact directory that allows the industry to identify contacts for other key issues, including call termination issues. ATIS maintains this list and has been working to promote the completion of contact information and its use by the industry. ATIS efforts since the Initial Strike Force report include efforts to streamline and automate input processes. This streamlining/automation is expected to be finalized in April 2017.

The ATIS Service Provider Contact Directory is available electronically at no charge. However, because this document is intended only for use only by service pro-

²⁹Customers who attest that they never initiate calls with a particular number often find other parts of their business, or third parties contracted services, that do. And a carrier that has assigned a number to a customer cannot conclusively and uniquely tell that customer that no other carrier originates traffic using that number to initiate legitimate calls. Outbound services using the telephone number could be hosted in the cloud or third party providers and carried over multiple wholesale provider networks. Given the highly dynamic and competitive call processing and handling ecosystem, which involves a diversity of business arrangements and call center structures, simplistic assumptions about a number's appropriateness for DNO are likely to result in unintended consequences.

³⁰See *e.g.*, Blocking NPRM, p. 10 (stating that "it is also important for the Commission to protect the reliability of the nation's communications network and to protect consumers from provider-initiated blocking that harms, rather than helps, consumers. The Commission therefore must balance competing policy considerations—some favoring blocking and others disfavoring blocking—to arrive at an effective solution that maximizes consumer protection and network reliability.").

³¹The Commission also seeks comment on authorizing providers to block calls from three categories of numbers: invalid numbers, valid numbers that are not allocated to a voice service provider, and valid numbers that are allocated but not assigned to a subscriber.

vider and enforcement agencies, it is password protected. More information about this document, including how to request the password, is available from: http://www.atis.org/01_committ_forums/NGIIF/contact_directories.asp.

USTelecom also realizes the importance of participation in the ATIS carrier directory. It will continue to coordinate with all of the ITB Group members and the association's individual members to ensure that their updated contact information is added to the list maintained by ATIS. In addition to direct communication and coordination with its individual members and members of the ITB Group, USTelecom has also utilized additional tools to expand awareness of this ATIS effort. These efforts include articles in the association's weekly newsletter, as well as blog entries regarding the importance of the ATIS initiative.

Further, CTIA has ensured that all national carriers have added their contact information to the ATIS service provider contact directory to help expedite investigations into the sources of illegal robocalls.

5. Regulatory Support

During the first sixty days, the Strike Force identified several regulatory road blocks and asked the Commission for rule clarifications and, if necessary, rule changes. The Commission addressed those requests in its NPRM and NOI released on March 23, 2017. Industry members expect to comment on the proposed rules and the technical and definitional questions raised by the FCC. Abating illegal robocalls is a complex undertaking, with potential unintended consequences, so carriers must have clear guidelines and protections for actions they may take to facilitate illegal robocall abatement. As new regulatory issues arise, the industry will continue to work with the Commission to remove any additional regulatory road blocks.

6. Conclusion

Significant progress has been made over the past six months. But this is not the end of the industry effort to develop ways to stop unwanted and illegal calls. The industry is committed to continuing to develop mitigation tools and techniques until these illegal harassing calls are stopped.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO ADRIAN ABRAMOVICH

Question 1. Deterrence—In your statement you said that a major reason that robocallers do what they do is because the software is easily accessible and inexpensive. One person can now make millions and millions of calls with just a computer. You mentioned the need to regulate the companies that sell autodialers and other software that makes this practice easy for telemarketers.

Other than looking at these companies, what actions can we take that would deter people from engaging in illegal robocalls?

Answer. No response to received.

Question 2. Do believe criminal penalties, with possible jail time, would deter some callers from making robocalls?

Answer. No response received.

Question 3. Size of the Industry—You said in your testimony you would make a good faith effort to work with the committee with your knowledge of the telemarketing industry. With regards to that industry, I am curious about its size. Obviously we see billions of these calls made but with modern technology one person can initiate an endless amount of calls.

From your experience, do you have any sense of the quantity of actors out there?

Answer. No response received.

Question 4. Are there bigger players that are responsible for a majority of the calls? Or is the industry much larger and diversified?

Answer. No response received.

Question 5. Are people in the industry worried about government action? Or is there a general sense that the chances of being caught are very small?

Answer. No response received.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JOHN THUNE TO
ROSEMARY HAROLD

Question. Would a longer statute of limitations improve the Commission's ability to focus its enforcement efforts against knowing and willful violators of the TCPA?

Answer. Yes, even a one-year longer statute of limitations for enforcement of the TCPA would improve the Commission's enforcement efforts against knowing and willful violators.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO
ROSEMARY HAROLD

Question 1. What is the interplay between privacy and robocalls? How do robocallers get access to our private information in order to target consumers for robocalls?

Is there any evidence that robocallers share call lists with each other or on the dark web which has the potential of creating repeat victims?

Answer. Taking each question in turn:

- *Interplay between privacy and robocalls:* Consumers widely consider unauthorized robocalls to be intrusive and an invasion of privacy. When Congress passed the Telephone Consumer Protection Act (TCPA) in 1991, one of the stated bases for placing additional restrictions on robocalls was that

" . . . automated telephone calls that deliver an artificial or prerecorded voice message are more of a nuisance and a greater invasion of privacy than calls placed by 'live' persons. These automated calls cannot interact with the customer except in preprogrammed ways, do not allow the caller to feel the frustration of the called party, fill an answering machine tape or a voice recording service, and do not disconnect the line even after the customer hangs up the telephone. For all these reasons, it is legitimate and consistent with the Constitution to impose greater restrictions on automated calls than on calls placed by 'live' persons."

(See S.Rep. No. 102-178, 102d Cong., 1st Sess. (1991) at 4-5.)

- *How robocallers get access/target consumers:* Different robocallers use different techniques, depending on the goal of the communication. For example, during his testimony before the Committee, Adrian Abramovich generally described his intention to reach certain demographics (married, over the age of 30, etc.), and explained that he targeted certain area codes in an attempt to reach consumers fitting the profile. While we make no assessment about the truthfulness of those statements, we note that the process Abramovich describes is fairly typical for target demographic-based telemarketing. Some robocall telemarketers purchase lists of phone contacts from data brokers or lead generators. Some robocallers use a scattershot or broadcast approach, hitting as many phone lines as possible in as short a time as possible. This type of robocaller tends to dial phone numbers randomly.
- *Robocallers sharing lists/dark web:* Over the course of our investigations, we have found indications that similar (or even identical) robocall scams have been perpetrated by apparently unrelated persons or entities. These indications suggest that scammers are trading information in some way.

Question 2. Last year the FCC initiated a proceeding seeking public comment on ways to authenticate caller ID information to further secure our telephone networks against illegal robocallers. What is the status of that proceeding?

Answer. A robust call authentication framework is part of the Commission's multi-pronged effort to combat the scourge of spoofed robocalls that American consumers know all too well. In July 2017, the Commission sought public input on the best way to establish a reliable system to verify caller ID information and tasked the North American Numbering Council (NANC) with recommending a governance framework. In May 2018, Chairman Pai accepted the recommendations of the NANC regarding the call authentication ecosystem, namely the adoption and deployment of "SHAKEN/STIR," the set of procedures and protocols intended to eliminate the use of illegitimate spoofed numbers from the telephone system. Industry stakeholders have now completed the first step of this process—formation of the governance authority for implementing SHAKEN/STIR. The governance authority is a stakeholder group established to determine the policies by which a carrier and its calls are considered trusted enough to "sign" calls originating on their networks. Next, a policy administrator will be established to certify carriers that are authorized to approve a call as legitimate. Finally, certification authorities will be chosen

to provide the “keys” that digitally stamp a call as legitimate. Although some carriers are expected to start signing calls even before this process is complete, operationalizing this system will help all carriers sign calls, attesting to their validity from start to finish—and conversely, making clear which calls are not valid.

The Commission expects this effort to move forward as quickly as possible to protect consumers. Industry has been making progress, but success requires sustained investment in this next-generation call authentication standard. To address this, on November 5, 2018 Chairman Pai sent letters to the phone industry demanding that voice providers adopt a robust call authentication system to combat illegal caller ID spoofing and launch that system no later than next year. In particular, the Chairman sent letters asking those that have not yet established concrete plans to protect their customers using the SHAKEN/STIR framework to do so. Chairman Pai also thanked those companies that have committed to implement a robust call authentication framework in the near term.

Question 3. Would it decrease enforcement matters if the FCC adopts a call authentication system to combat illegal robocalls?

Answer. Caller ID authentication appears to be an important tool to combat illegal, malicious spoofing. And illegal spoofing makes it difficult for law enforcement to locate the violators and protect consumers from unwanted communications. Accordingly, we are hopeful that, to the extent that caller ID authentication removes the ability of malicious callers to hide behind falsified information, the increased risk of detection will cause many fraudsters to cease using robocalling as a vehicle for their scams.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO
TO ROSEMARY HAROLD

Question 1. Impact on Immigrants—Robocalls, and particularly those done by illegitimate businesses are obviously a nuisance and can pose a danger to anyone who receives them. But some populations are particularly vulnerable, we had a hearing in the Aging committee last fall on the impact of these calls on seniors. Another population that can be impacted is immigrants, especially those who have recently arrived or may be still developing English skills. There is some reporting suggesting that scammers actively target immigrants.

Can any of you talk about cases where this has happened? A deliberate targeting of immigrants and non-English speakers?

Answer. Yes. For example, in recent months, the FCC has received numerous consumer complaints about Chinese-language robocalls from scammers trying to steal money or personal information by posing as Chinese consulate employees. According to multiple news reports, random consumers in areas with large Chinese communities have been targeted. The FCC issued a public notice warning consumers of the scam (available in English and Chinese), here: <https://www.fcc.gov/chinese-americans-targeted-consulate-phone-scam>.

Question 2. Are there any steps your agency is taking to reach these populations with educational campaigns?

Answer. Yes, the Commission extends information to immigrant populations and non-English speakers through the Commission website and via distribution of tip cards in Spanish, Korean, Tagalog, Vietnamese, and Chinese. The Commission has provided information on particular scams targeting immigrants, such as calls from scammers posing as representatives from:

- Charitable organizations collecting donations in the wake of Hurricanes Harvey, Irma and Maria and most recently Hurricanes Florence and Michael.
- Insurance companies offering additional flood insurance.
- The IRS, seeking to collect supposedly overdue taxes.
- Chinese embassy representatives asking for personal information.

Question 3. Deterrence—There was an article in the Washington Post in January about an FTC action against a robocaller from California who had made *billions* of illegal robocalls. He was living in a wealthy neighborhood and paying \$25,000 a month for his house, had a personal chef, and drove two Mercedes. The FTC brought him in for questioning and he basically admitted he did it without remorse, he was fined \$2.7 million and banned from telemarketing. While it’s clear that in the digital age your agencies need more resources to police this behavior, it’s evident from the article that even when cases are brought fines are often negotiated down by the perpetrators of these calls and robocallers have clearly concluded that the financial benefits outweigh and costs of this behavior.

How does the FCC find individuals to pursue?

Answer. The Commission identifies enforcement targets principally via consumer complaints filed with the FCC's Consumer & Governmental Affairs Bureau. The FCC also accepts and may act on referrals from other governmental agencies, members of the U.S. Congress, state or local officials, and industry stakeholders. For example, USTelecom leads the efforts of an Industry Traceback Group, which attempts to identify the source of illegal robocalls and shares the results of its efforts with the Commission. To encourage further participation in the Industry Traceback Group, on November 6, 2018, the Commission's Chief Technology Officer and I sent letters to voice providers, calling on them to assist in industry efforts to trace scam robocalls that originate on or pass through their networks. In addition to complaints or referrals from third parties, Enforcement Bureau staff may identify potential violators through independent research (such as media reports or consumer complaints filed online, among others).

Question 4. If the person is found to engage other criminal behavior, such as fraud, while making robocalls how does the FCC work with other law enforcement organizations to bring charges related to those crimes?

Answer. The FCC coordinates with other law enforcement agencies at the local, state, federal, and international level. The Commission has executed Memoranda of Understanding with multiple entities to allow each entity to share relevant evidence with the other in pursuit of respective law enforcement goals. We continue to look for ways to strengthen these relationships and build processes to better and more quickly communicate with outside agencies that may have an interest in pursuing criminal charges against identified targets.

Question 5. How does the FCC ascertain what the content of the calls was and how difficult is it to prove that a person engaged in fraudulent behavior beyond just making illegal robocalls?

Answer. FCC investigators use multiple techniques to determine the content of the robocalls, including interviewing robocall victims, reviewing consumer complaints, and obtaining evidence via the agency's investigatory subpoena powers (*e.g.*, actual recordings of the call). Proving fraud in the context of robocalling, as in any other context, presents challenges.

Question 6. Does the FCC have a sense of the size of the illegal robocalling industry? How many people or organizations are engaging in these illegal calls?

Answer. We do not have a precise calculation of the number of people/organizations who deliberately make unlawful robocalls. Our data indicate that a relatively small number of entities account for a very large portion of the total number of unlawful robocalls.

Question 7. On average, how many fines does the agency levy in recent years?

Answer. From January 1, 2017, through September 30, 2018, the agency has issued or proposed fines of \$242,536,000.00 pursuant to the Truth in Caller ID Act (TICIDA) and the Telephone Consumer Protection Act (TCPA). From January 1, 2010 through December 31, 2016, the agency issued or proposed fines of \$3,387,500 under the TICIDA and TCPA.

Question 8. Do you believe that the current fines are a significant enough deterrent, or do you think that increased levels of fines would also increase the level of deterrence?

Answer. The current fines under the TCPA and TICIDA are assessed on a per-call basis, so any robocaller making millions of illegal robocalls may find itself facing penalties in the hundreds of millions of dollars. This is a significant deterrent against abuse. A more limiting factor to enforcement is likely to be the applicable statute of limitations periods. The statute of limitations is one year for TCPA violations and two years for TICIDA violations, which may not be enough time to complete investigations involving complex robocalling cases. Accordingly, the FCC's enforcement tools might be enhanced if Congress considered expanding the current statute of limitations for violations under TCPA and TICIDA.

Question 9. Banking—In 2014 a couple won a lawsuit against Bank of America for more than \$1 million after they were flooded with robotic collection calls over the course of several years. It is understandable that banks and other companies want to contact their customers about issues, but we cannot have financial institutions blatantly ignoring the law and instituting a policy of annoying their customers with illegal phone calls.

Can you provide data on how many illegal calls originate from the financial industry?

Answer. The Commission does not have that data.

Questions 10. Is there evidence of organizations in the financial industry systematically ignoring existing law?

Answer. We cannot comment on matters that may be under investigation by the FCC's Enforcement Bureau. We encourage all aggrieved persons to file complaints on fcc.gov to alert us to illegal robocalls they have received from any industry segment. We note that in 2016, the Commission's *Broadnet Declaratory Ruling* held that the TCPA does not apply to Federal government contractors, including those in the financial industry. See *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Broadnet Teleservices LLC Petition for Declaratory Ruling*, CG Docket No. 02-278, Declaratory Ruling, 31 FCC Rcd 7394 (2016). There are two pending petitions for reconsideration of that decision.

Question 11. A one million dollar cost, as shown in this case, is not a significant sum for a large bank, are the financial risks great enough to discourage this behavior?

Answer. As noted above, the fines for large robocalling schemes can provide a substantial financial deterrent.

Question 12. Educating Seniors—I appreciate the efforts people are making in the government and private sector to hold competitions and develop apps. Ultimately, as we well know, seniors are the most vulnerable to scam calls. We have a lot of seniors moving to Nevada and a lot of retirement communities in places like Las Vegas, which received an estimated 26.7 million robocalls in March of this year.

Seniors are harder to reach with some of this new technology that can be of real assistance in blocking these calls.

Can you provide examples of how your agency is trying to educate seniors about new technology?

Answer. We have undertaken a major outreach campaign to reach older Americans and alert them to robocalls scams. In September, the FCC teamed up with AARP on two tele-townhalls to inform older Americans about phone scams and what they can do to avoid being victims. We also work with the American Library Association to furnish libraries throughout the Nation with FCC Consumer Guides and Tip Cards for all patrons, many of whom are 65 and over. We use information gathered from consumer complaints about robocalls to post consumer alerts concerning current scams such as "grandparent scams," "Social Security scams," "IRS scams," and others that target older Americans. We also share this information with national and local community groups.

Question 13. Is there data available on how educated our seniors on our robocalls? If so, can you please provide it?

Answer. While we do our best to educate seniors and will continue our efforts to help them avoid unwanted robocalls, we do not have data on how well-informed seniors are about robocalls.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO
LOIS GREISMAN

Question 1. What is the interplay between privacy and robocalls? How do robocallers get access to our private information in order to target consumers for robocalls?

Is there any evidence that robo callers share call lists with each other or on the dark web which has the potential of creating repeat victims?

Answer. Robocalls are not only a mechanism for perpetrating fraud, they are also an intrusion on consumer privacy. Some robocallers purchase lists containing consumer information from data brokers to target specific communities, but in the FTC's experience these data brokers operate in plain sight on public websites. For example, telemarketers selling home security systems, solar panels, replacement windows, and other goods for residential use can legally purchase lists of new homebuyers. Most of these data brokers, which range from small businesses to large, publicly traded firms, usually provide this information to legitimate businesses that responsibly use it for legal marketing and other purposes.

At the same time, in our experience, some robocallers obtain information on potential targets through online lead generation, while others are simply random-dialing numbers throughout the country.

Question 2. What is your budget for robocalls enforcement? Is it enough?

Answer. The FTC does not have a discrete robocall enforcement budget. Rather, divisions within the FTC's Bureau of Consumer Protection, along with our regional offices, bring robocall cases and engage in outreach and educational initiatives as part of their efforts to protect consumers from fraud and abusive telemarketing. The

costs of running the FTC's robocall enforcement program are included within the total request for funding the FTC submits to Congress on an annual basis. Like any law enforcement challenge, additional resources and enforcement tools could yield even greater results.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO
LOIS GREISMAN

Question 1. Most people recognize the fines leveled by the FTC are a drop in the bucket compared to the injury and harm consumers experience from bad actors. Does the FTC have the resources to increase its enforcement activity?

Answer. The FTC has expended significant time and effort to combat illegal robocalls. The FTC uses every tool at its disposal to tackle this pernicious consumer protection problem. Like any law enforcement challenge, additional resources and enforcement tools could yield even greater results. In order to advance its robocall enforcement program, the FTC seeks to repeal the common carrier exemption from its jurisdiction. The exemption impedes investigations, complicates litigation, and prevents the FTC from challenging common carriers of telecommunications that violate the TSR.

Question 2. Yesterday, my staff googled "autodialer." One of the top hits was a video on YouTube from a user showing how to use Excel and Skype to make hundreds of calls. This is just one of many videos showing how to buy equipment and call lists from the Internet and spam people. How can the FTC stop this problem if it is so simple to make fraudulent calls?

Answer. The FTC is keenly aware of the low barriers to entry and ease of placing illegal robocalls. This is one reason the FTC believes that civil law enforcement alone will not completely solve the problem. The FTC partners with industry to help spur innovative technological solutions such as call blocking applications, which enable consumers to limit the calls they wish to receive. The FTC will continue to work with the FCC and the telecommunications industry to advance call verification and call labeling protocols that will offer consumers even more tools to avoid unwanted, fraudulent, or abusive calls.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO
TO LOIS GREISMAN

Question 1. Impact on Immigrants—Robocalls, and particularly those done by illegitimate businesses are obviously a nuisance and can pose a danger to anyone who receives them. But some populations are particularly vulnerable, we had a hearing in the Aging committee last fall on the impact of these calls on seniors. Another population that can be impacted is immigrants, especially those who have recently arrived or may be still developing English skills. There is some reporting suggesting that scammers actively target immigrants.

Can any of you talk about cases where this has happened? A deliberate targeting of immigrants and non-English speakers?

Are there any steps your agency is taking to reach these populations with educational campaigns?

Answer. The FTC periodically encounters robocall scams that target foreign language speakers or non-native English speakers. In 2017, the FTC sued a telemarketing operation that impersonated the government and used spoofed caller ID numbers to sell English-learning products to Spanish-speaking consumers. In that case, *FTC v. ABC Hispana Inc., et al.*, the FTC obtained a court order banning the defendants from all telemarketing and imposing a \$6.3 million judgment.¹ Most recently, we learned of Chinese language robocalls purporting to be from the Chinese Consulate. Some of the robocall messages falsely stated that consumers needed to pick up a package at the Consulate, while others falsely stated that consumers needed to pay fees to avoid trouble with the Chinese government. In response, in April the FTC coordinated with the Chinese Embassy to publish a consumer notice about these scams in English and Simplified Chinese.²

¹The FTC's pleadings and press releases are available here: <https://www.ftc.gov/enforcement/cases-proceedings/152-3108/abc-hispana-inc-et-al>.

²A copy of the FTC consumer warning is available here: <https://www.consumer.ftc.gov/blog/2018/04/scammers-impersonate-chinese-consulate>. The publication of this alert, both on the FTC and Chinese Consulate websites, was followed by a series of media interviews by FTC staff.

In addition, as part of its longstanding *Every Community* initiative, the FTC engages in frequent consumer education to immigrants and non-native English speakers. For example, to date the FTC has held a series of 22 Ethnic Media Roundtables around the country, bringing together the FTC, state attorneys general offices, local agencies and law enforcement, community-based organizations, and ethnic media to discuss how scams affect diverse local communities. Also, as part of this initiative, the FTC does targeted outreach to legal services providers, teachers of English as a second language, librarians, and other local community members who can help us amplify our consumer protection messages.

The FTC also educates consumers about avoiding scams targeting immigrants in English, Spanish, Arabic, Chinese, Creole, Korean, Russian, and Vietnamese at [FTC.gov/immigration](https://www.ftc.gov/immigration). We created a plain language fraud handbook in English, Spanish, Amharic, Arabic, Dari, French, and Somali for refugees and recent immigrants at [FTC.gov/refugee](https://www.ftc.gov/refugee). And we offer the top ten things to do to avoid fraud in English, Spanish, Arabic, Chinese, Korean, Russian, Tagalog, and Vietnamese. Our community partners can order large quantities of these resources for free at [FTC.gov/bulkorder](https://www.ftc.gov/bulkorder).

Question 2. Deterrence—There was an article in the *Washington Post* in January about an FTC action against a robocaller from California who had made *billions* of illegal robocalls. He was living in a wealthy neighborhood and paying \$25,000 a month for his house, had a personal chef, and drove two Mercedes. The FTC brought him in for questioning and he basically admitted he did it without remorse, he was fined \$2.7 million and banned from telemarketing. While it's clear that in the digital age your agencies need more resources to police this behavior, it's evident from the article that even when cases are brought fines are often negotiated down by the perpetrators of these calls and robocallers have clearly concluded that the financial benefits outweigh and costs of this behavior. How does the FTC find individuals to pursue?

Answer. The FTC analyzes consumer complaints, reviews evidence compiled in prior investigations and litigation, and pursues tips from informants and third parties to identify targets in robocall cases. As is true of any law enforcement agency, the details of the FTC's process for initiating specific investigations are generally non-public.

Question 3. If the person is found to engage other criminal behavior, such as fraud, while making robocalls how does the FTC work with other law enforcement organizations related to bring charges related to those crimes?

Answer. The FTC has a Criminal Liaison Unit (CLU), which, when appropriate, coordinates law enforcement initiatives with state and Federal criminal prosecutors. Through CLU, the FTC has referred numerous cases to criminal prosecutors. In the first three quarters of Fiscal Year 2018, criminal prosecutors relied on FTC information and support to charge twenty-two new defendants and obtain forty-four new pleas or convictions.

Question 4. How does the FTC ascertain what the content of the calls was and how difficult is it to prove that a person engaged in fraudulent behavior beyond just making illegal robocalls?

Answer. In challenging certain types of illegal robocalls, the FTC has numerous means through which to ascertain the content of the calls and, accordingly, to challenge that content as deceptive. Such means include obtaining declarations from consumers who received the telemarketing pitches, obtaining telemarketing scripts, and transcribing FTC investigators' undercover recordings of calls by telemarketers.

Question 5. Does the FTC have a sense of the size of the illegal robocalling industry? How many people or organizations are engaging in these illegal calls?

Answer. We have no precise way to measure the size of the illegal robocalling industry. In its robocall and Do Not Call enforcement cases, the FTC has sued 454 companies and 367 individuals to date. The FTC knows these illegal robocalls are supported by several different types of businesses and service providers:

- software companies that provide autodialing software;
- VoIP providers that provide the telephone lines to connect the calls;
- data brokers and lead generators that sell lists of consumers to call;
- call centers that field robocalls after consumers press 1 to speak with a live operator;
- caller ID resellers that license "local area code" telephone numbers that telemarketers use to entice consumers to answer the phone;
- sellers of goods and services who reap the financial benefits of blasting out low-cost robocalls to reach a wide audience; and

- fraudsters who rely on robocalls as a low cost way to reach potential victims

To the extent the Commission has jurisdiction, it targets parties in these industries that assist and facilitate illegal robocalling. In this regard, we observe that the common carrier exemption to the Commission's jurisdiction impedes investigations, complicates litigation, and prevents the FTC from challenging common carriers of telecommunications that violate the TSR.

Question 6. On average, how many fines does the agency levy in recent years?

Answer. The FTC does not have authority to levy fines. Rather, to enforce the robocall and Do Not Call provisions of the Telemarketing Sales Rule (TSR), the FTC litigates in Federal court to obtain disgorgement of ill-gotten profits, consumer redress, and injunctive relief. The FTC can also refer enforcement of TSR violations to the Department of Justice ("DOJ") to obtain civil penalties; the DOJ can refer the matter back to the FTC to litigate. To date, the FTC has brought 138 Do Not Call and robocall cases against 454 corporate entities and 367 individuals, resulting in actual collections of more than \$121 million. The \$121 million in collections includes \$71 million in equitable monetary relief (disgorgement/redress) and \$50 million in civil penalties. This does not include the \$280 million civil penalty trial verdict against Dish Network (litigated by DOJ on the FTC's behalf), which is now on appeal to the Seventh Circuit Court of Appeals.³ Since January 2017, the FTC has brought ten cases alleging violations of the TSR's robocall or Do Not Call rules, seeking civil penalties and/or equitable monetary relief.

Question 7. Do you believe that the current fines are a significant enough deterrent, or do you think that increased levels of fines would also increase the level of deterrence?

Answer. The FTC is authorized to obtain judgments, including a civil penalty of up to \$41,484 per violation of the TSR. As a practical matter, in our law enforcement experience, defendants very rarely have sufficient assets to pay a significant civil penalty. As such, we think it unlikely that increasing the maximum civil penalty would have any deterrent effect.

Question 8. Banking—In 2014 a couple won a lawsuit against Bank of America for more than \$1 million after they were flooded with robotic collection calls over the course of several years. It is understandable that banks and other companies want to contact their customers about issues, but we cannot have financial institutions blatantly ignoring the law and instituting a policy of annoying their customers with illegal phone calls. Can you provide data on how many illegal calls originate from the financial industry?

Is there evidence of organizations in the financial industry systematically ignoring existing law?

A one million dollar cost, as shown in this case, is not a significant sum for a large bank, are the financial risks great enough to discourage this behavior?

Answer. The FTC does not have data on the volume of illegal calls from financial institutions or information on the possible scope of non-compliance with telemarketing rules by such entities. As a general matter, the FTC does not have jurisdiction over banks and other financial institutions.⁴ We further observe that while the FTC enforces the Fair Debt Collection Act, debt collection robocalls are outside the scope of the FTC's Telemarketing Sales Rule, as such calls do not seek to sell any good or service. Debt collection robocalls, however, may be covered under other Federal statutes, such as the Telephone Consumer Protection Act and the Truth in Caller ID Act, both enforced by the Federal Communications Commission.

Question 9. Educating Seniors—I appreciate the efforts people are making in the government and private sector to hold competitions and develop apps. Ultimately, as we well know, seniors are the most vulnerable to scam calls. We have a lot of seniors moving to Nevada and a lot of retirement communities in places like Las Vegas, which received an estimated 26.7 million robocalls in March of this year.

Seniors are harder to reach with some of this new technology that can be of real assistance in blocking these calls.

Can you provide examples of how your agency is trying to educate seniors about new technology?

Is there data available on how educated our seniors on our robocalls? If so, can you please provide it?

³See *USA et al., v. Dish Network L.L.C.*, No. 3:09-cv-03073 (C.D. Ill.). Pleadings and press releases from the case are available here: <https://www.ftc.gov/enforcement/cases-proceedings/052-3167/dish-network-llc-united-states-america-federal-trade>.

⁴The exemption is explicit in the FTC Act, 15 U.S.C. § 45(a)(2).

Answer. The FTC has a robust program to educate older adults. Through *Pass It On*, the FTC's signature consumer education campaign directed at active older adults, the agency enlists older adults to share their experiences with scams and fraud with their peers. This includes, at [FTC.gov/PassItOnImposters](https://www.ftc.gov/PassItOnImposters), strategies for handling calls from imposters pretending to be online technical support, the IRS, a romantic interest, or a family member with an emergency. These efforts at reaching older adults are complemented by ongoing advice via consumer alerts (consumer.ftc.gov/blog) on a range of issues, including robocalls⁵ and online technical support scams,⁶ which affect many older adults.

While we are not aware of particular research about older consumers' level of education regarding robocalls, we know that robocalls involve a complex set of technological issues that are challenging for many consumers. We try to address these challenges by creating an array of educational messages that take many forms, including handouts, videos, and blog posts. This spring, we also created [FTC.gov/calls](https://www.ftc.gov/calls), which features three new shareable graphics telling people how to block unwanted calls on their mobile and home phones. These graphics provide key information on the various call-blocking options that are available for different types of phones, including a landline that uses the Internet (VoIP) or traditional copper line.

Question 10. Common Carrier Exemption—At a recent panel you called for getting rid of the common carrier exemption as a way for the FTC to crack down on robocalls. Can you explain the mechanism by which repealing this exemption would help the FTC increase enforcement efforts?

Answer. Robocallers use VoIP lines to make a significant number of commercial robocalls. Telecommunications carriers typically provide VoIP lines to telemarketers, and we have observed that many small VoIP carriers appear to market their services specifically to robocallers. The common carrier exemption to the FTC jurisdiction likely precludes the FTC from bringing any law enforcement actions against VoIP providers, even if they knowingly sell or lease telephone lines to telemarketers making illegal robocalls.

As such, the common carrier jurisdictional exemption creates a significant gap in the FTC's robocall enforcement work and impedes the agency's ability to more effectively protect consumers. For instance, in *FTC v. Christiano*, a case the FTC filed on May 31, 2018, the FTC sued James Christiano and two of his companies for assisting and facilitating illegal robocalls.⁷ The FTC alleged that the defendants provided robocallers with autodialing software and servers to host that software—even while knowing the robocallers were using that software to place illegal calls. Mr. Christiano owned a third company that provided the robocallers with VoIP lines. The FTC did not pursue the VoIP company for its knowing participation in the illegal robocalls due to the common carrier exemption.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. MARIA CANTWELL TO
KEVIN RUPY

Question. What is the interplay between privacy and robocalls? How do robocallers get access to our private information in order to target consumers for robocalls?

Is there any evidence that robocallers share call lists with each other or on the dark web which has the potential of creating repeat victims?

Answer. Unwanted, unconsented to robocalls can be considered a nuisance or affront to privacy as they cause unnecessary and unwarranted interruption and distraction. In the past year, however, there are a growing number of tools and services that are helping consumers better manage these calls, thereby providing them with increased control over their privacy.

Robocallers can gain access to consumers' telephone numbers from a variety of sources. These include publicly available sources, and so-called "lead-lists." In addition, illegal robocallers can also generate telephone numbers randomly or sequentially without regard to the actual identity of the subscriber.

⁵ *Untangling a Robocaller Web* (June 5, 2018), at <https://www.consumer.ftc.gov/blog/2018/06/untangling-robocaller-web>; *That's Not Your Neighbor Calling* (Jan. 31, 2018), at <https://www.consumer.ftc.gov/blog/2018/01/thats-not-your-neighbor-calling>.

⁶ *Warn Your Friends about Tech Support Scams* (July 27, 2018), at <https://www.consumer.ftc.gov/blog/2018/07/warn-your-friends-about-tech-support-scams>; *No Gift Cards for Tech Support Scams* (June 6, 2018), at <https://www.consumer.ftc.gov/blog/2018/06/no-gift-cards-tech-support-scammers>.

⁷ See *FTC v. Christiano et al.*, No. 8:18-cv-00936 (C.D. Cal.). The complaint and press release from the case are available here: <https://www.ftc.gov/enforcement/cases-proceedings/162-3124/james-christiano-et-al-neidotsolutions-inc>.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. RICHARD BLUMENTHAL TO
KEVIN RUPY

Question. I recently introduced S. 2705, the Repeated Objectionable Bothering of Consumers on Phones (ROBOCOP) Act to require phone companies to offer effective tools to block robocalls to consumers at no extra cost to them. Do you support this legislation?

Answer. USTelecom supports the goal of the ROBOCOP Act. Its member companies are actively pursuing the development of the technologies described in the bill under the auspices of the Federal Communications Commission and an industry-created governance board. In addition, USTelecom member companies already offer a number of free, effective tools to block robocalls at no extra cost to their customers.

Given the development of marketplace solutions in this area, a legislative approach that mandates robocall tools is unnecessary. Today, a broad range of voice providers, independent application developers and a growing number of diverse companies are offering services that can help Americans reduce unknown and potentially fraudulent calls. While these tools are not a panacea to the robocall problem, they are an important component that empowers consumers with the increased ability to better identify and/or block illegal or unwanted robocalls.

An increasing number of robocall mitigation tools are being deployed by facilities-based providers themselves. For example, AT&T has deployed its “Call Protect” service, and has partnered with robocall blocking service “Hiya.” Similarly, Verizon’s new Spam Alerts service utilizes TNS’s Call Guardian and Neustar’s Robocall Mitigation solution to proactively identify illegal robocalls and other fraudulent caller activity with more accuracy. Various carriers have also 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.

In addition, in the last year alone the number of scoring and labelling analytics tools for consumers has exploded. In 2016 there were over 85 call-blocking applications available across all platforms, including several offered by carriers to their customers at no charge. As of today, there are now over 550 applications available, a 495 percent increase in call blocking, labeling, and identifying applications to fight malicious robocalls. The diversity in tools across multiple platforms demonstrates industry’s commitment to empower consumers, regardless of the type of network utilized by their chosen voice service provider. The significant availability in services and offerings throughout the marketplace is an important component of the battle against illegal robocalls. Specifically, the diversity in robocall analytics and tools means that illegal robocallers face a wide variety of mitigation techniques that makes their countermeasure efforts less effective—in other words, they must overcome multiple mitigation techniques, as opposed to a single standard.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO
KEVIN RUPY

Question 1. Your testimony identified products that are available to telephone customers, even those with “plain old telephone service.” Are there costs associated with these services? Do any of your member companies offer discounts for certain populations, such as those who receive basic telephone service through the Lifeline program?

Answer. There are a growing number of tools available to consumers today that mitigate illegal and/or unwanted robocalls. These tools work across various platforms and services, including cable, wireless, IP, and “plain old telephone service.” Given the diversity in robocall scoring and analytics services, as well as the variety of voice platforms, some of these consumer services are free, while others include a charge.

For example, Verizon’s new Spam Alerts service provides its wireline customers who have Caller ID—whether they are on copper or fiber—with enhanced warnings about calls that meet Verizon’s spam criteria by showing the term “SPAM?” before a caller’s name on the Caller ID display. By using existing Caller-ID technology, the service empowers consumers to better decide if they should answer a particular call. Various carriers have also worked with Nomorobo to facilitate their customers’ ability to use that free, third-party blocking service by establishing a “one click” solution that simplifies customers’ ability to sign up for the service.

Programs such as Lifeline are not directly tailored to provision robocall mitigation services to consumers. Rather, the program provides consumers with a pre-determined subsidy that can be utilized for voice or broadband services. Of course, it is possible that the consumer’s choice for subsidized Lifeline service may include a free

robocall mitigation service. In the alternative, a consumer could choose to utilize the savings from the Lifeline subsidy to acquire a subscription-based robocall service.

Question 2. AARP partners with organizations to warn seniors, especially homebound men and women, about fraudulent calls—like the “grandparent” or IRS scam. Do any of your members work with outside organizations to help provide information about these scams?

Answer. Education is an important tool in the fight against illegal robocalls, and several of our members—and other industry stakeholders—have implemented education efforts to provide information to consumers on robocall tools and scams. Verizon, for example, has developed a package of consumer education materials to help consumer-facing personnel, such as staffers at consumer protection agencies or in constituent-services offices, effectively counsel consumers about robocalls. AT&T has developed a website that provides customers with easy access to consumer information and tips about identifying and avoiding unwanted calls, as well as alerts on recently identified scams. AT&T’s website also provides links to other important consumer resources, as well as instructions for reporting various types of fraud (including telephone call fraud).

In addition to the efforts of individual companies, other stakeholders are also engaged in consumer education. For example, the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) have correctly focused on raising customer awareness of their options, including with the successful Stop Illegal Robocalls Expo in April 2018. The Expo featured technologies, devices and applications to minimize or eliminate the number of illegal robocalls consumers receive. It also provided a platform for showcasing innovative technologies, devices and applications that are available to consumers to assist in combatting illegal robocalls.

Similarly, several industry and governmental organizations are also focused on consumer education. For example, CTIA—the Wireless Association, has published a webpage devoted to increasing awareness of robocall prevention tools and provides consumers with instructions on how to stop robocalls. In addition, the Communications Fraud Control Association (CFCA), maintains a consumer education channel on YouTube that includes various educational videos, including on robocalls. The Better Business Bureau Institute has also started publishing an annual “Scam Tracker” report that collects reports of scams and fraud and displays the information in real time on an interactive map that warns consumers.

Similar educational outreach has been conducted by the FCC and FTC for some time. For example, the FTC maintains a wide range of educational materials on its website that provides timely and informative information to consumers regarding robocall related scams and information. USTelecom, CTIA and several other industry and consumer organizations are also members of the FCC’s Consumer Advisory Committee (CAC). One of the first recommendations adopted by the members of the CAC, focused on ways for the FCC to improve consumer education efforts, particularly with respect to robocalls.

Question 3. Have your members considered ways to help notify or enable consumers’ complaints about the abusive or fraudulent robocalls?

Answer. Empowering consumers through streamlining the complaint process is an important component to addressing the robocall issue. Both the FCC and the FTC provide portals where consumers can file robocall complaints. In addition, both agencies publish portions of the complaint data (excluding any personal information), which is then used by industry stakeholders to assist in their robocall efforts. For example, analytic companies use the public data to improve their scoring of illegal robocalls, and USTelecom has used the same data to match consumer complaints with active traceback investigations.

In order to simplify the FCC’s complaint process for consumers, the FCC’s CAC—of which USTelecom is a member—adopted a series of proposals for the agency’s consideration. Among other things, the CAC encouraged the FCC to simplify the consumer complaint filing process for unwanted calls by developing a form that allows for information to be entered about multiple unwanted calls at once, and creating a separate intake portal for unwanted-call complaints. The FCC subsequently created the proposed intake portal, and was in the process of exploring alterations to its portal to allow for multiple calls to be entered at once.

Question 4. Are your members Customer Service Representatives able to assist callers that complain about the robocalls?

Answer. Consumer education is a critical component to increasing consumer protection from illegal robocalls. Many of USTelecom’s member companies are taking active steps to educate consumers. For example, recognizing that consumer education may be particularly beneficial if provided at the moment consumers are complaining about robocalls, Verizon has developed a package of consumer education

materials to help consumer-facing personnel, such as staffers at consumer protection agencies or in constituent-services offices, so they may effectively counsel consumers about robocalls. Counselors are encouraged to first ask questions to elicit the nature of the consumer's service and facility (*e.g.*, smartphone, wireline VoIP, wireline copper), and then the talking points have a "decision tree" that counselors can follow to tailor their advice to each customer's particular technology platform and his or her needs. The package includes different educational brochures to be mailed or e-mailed to consumers based on what makes sense for each one.

In addition, AT&T's website provides customers with easy access to consumer information and tips about identifying and avoiding unwanted calls. More specifically, AT&T's Cyber Aware Resources page includes alerts on recently identified scams and provides links to other important consumer resources, as well as instructions for reporting various types of fraud (including telephone call fraud). AT&T also issues consumer alerts when fraud events are identified.

USTelecom and its member companies actively work with other stakeholders to increase consumer education. For example, in April, 2018, several USTelecom members worked with the FCC and the Federal Trade Commission to put on a public expo to raise customer awareness of their options. In addition, as member of the FCC's Consumer Advisory Committee, USTelecom worked with FCC staff, industry stakeholders and consumer groups to propose a variety of consumer education initiatives that the agency has since adopted. For example, in response to a CAC recommendation asking that the FCC incorporate educational information into replies to consumer complaints, the agency began linking resources (including consumer guides) in their response to complaints.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO
TO KEVIN RUPY

Question 1. There was an article in the *Washington Post* in January about an FTC action against a robocaller from California who had made *billions* of illegal robocalls. He was living in a wealthy neighborhood and paying \$25,000 a month for his house, had a personal chef, and drove two Mercedes. The FTC brought him in for questioning and he basically admitted he did it without remorse, he was fined \$2.7 million and banned from telemarketing. While it's clear that in the digital age your agencies need more resources to police this behavior, it's evident from the article that even when cases are brought fines are often negotiated down by the perpetrators of these calls and robocallers have clearly concluded that the financial benefits outweigh and costs of this behavior. In your testimony, you emphasized the need for *criminal enforcement* to crack down on illegal robocalls, and in questioning, you said that tools exist to criminally target those who engage in "hardcore fraud."

Would U.S. Telecom and its members support an expansion of criminal penalties for robocalls already illegal under the TCPA, including those that may not otherwise prosecuted for other criminal statutes like fraud?

Answer. USTelecom is supportive of criminal enforcement actions against illegal robocallers, however, we believe that criminalizing violations under the TCPA is not the correct approach. TCPA violators are already subject to substantial no-fault, class action litigation exposure for alleged violations of the statute and the Federal Communications Commission's (FCC) rules implementing the statute. Although USTelecom believes that S.3149 (the Do Not Call Act) is motivated by a sincere desire to address the behaviors of firms and individuals such as the witness featured at the April 18 Senate hearing, there is no indication that there is a lack of any Federal authority to address those behaviors adequately, either by the FCC or the U.S. Attorney.

For example, last month, the Department of Justice announced that twenty-one members of a "massive India-based fraud and money laundering conspiracy that defrauded thousands of U.S. residents of hundreds of millions of dollars" were sentenced to terms of imprisonment up to 20 years. These individuals were all prosecuted under various existing criminal statutes. Given that sufficient legal authorities exist for Federal prosecutors to prosecute egregious robocallers under the Communications Act, the FTC Act and the Federal criminal statutes, USTelecom recommends that the U.S. Attorney General should issue guidance to Federal prosecutors outlining these authorities and prioritizing Federal law enforcement activities in this area.

USTelecom stands prepared to work with and assist Federal agencies in putting these predatory criminals behind bars. Indeed, this criminal prosecutorial effort—which was given "significant support" by both the FCC and TIGTA—proves that through appropriate collaboration, these criminal elements can be located, identi-

fied, and aggressively prosecuted. If criminal enforcement agencies join the FCC and the FTC to conduct robocall fraud investigations, such joint enforcement—especially if coupled with stronger private sector traceback activity—could reduce the number of illegal robocalls American consumers receive.

Question 2. What steps are your members taking to help Federal law enforcement identify the source of these calls?

Answer. USTelecom, along with several of its member companies, works closely with Federal law enforcement to identify the source of illegal robocalls. For the last several years, USTelecom has led the efforts of the Industry Traceback Group (ITB Group), whose primary mission is to vigorously protect participating carriers' networks, and users of their services, from fraudulent, abusive, and/or unlawful robocalls. With 24 voice provider members from a broad range of industry (*i.e.*, cable, wireline, wireless, wholesale, etc.), the ITB Group identifies illegal and fraudulent traffic, and through its cooperative framework of sharing call detail information, traces these calls to their origins.

Once the ITB Group has traced a call back through the network as far as possible, it will share this information with the appropriate Federal enforcement agencies. In particular, USTelecom will provide referrals to the enforcement departments of the FCC and/or FTC. In fact, just this week, the FCC's Enforcement Bureau sent a letter to USTelecom expressing its "gratitude for the work of USTelecom and the USTelecom Industry Traceback Group." It also noted that due to the information obtained from the USTelecom Industry Traceback Group, the amount of time necessary for the Enforcement Bureau to conduct a traceback investigation from start to finish has "shrunk from months to weeks."

While current Federal enforcement efforts are laudatory, they are mostly limited to civil enforcement. As a result, bad actors currently engaged in criminal robocall activities are—at most—subject only to civil forfeitures. USTelecom believes there is an acute need for coordinated, targeted and aggressive criminal enforcement of illegal robocallers at the Federal level through the use of existing Federal statutes. Given the felonious nature of their activities, criminal syndicates engaged in illegal robocalling activity should be identified, targeted and brought to justice through criminal enforcement efforts.

USTelecom and its industry partners stand ready to further assist in these efforts to bring these bad actors to justice. Indeed, the ultimate goal of USTelecom's Industry Traceback Group is to identify the source of the worst of these illegal calls, and further enable aggressive enforcement actions by Federal agencies.

Question 3. Common Carrier Exemption—At a recent panel the FTC has called for getting rid of the common carrier exemption as a way for the FTC to crack down on robocalls.

What is the position of USTelecom on the common carrier exemption as it relates to illegal robocalls?

Answer. USTelecom maintains that the FTC has sufficient authority to pursue illegal robocallers, and that there is no need to remove the common carrier exemption. Moreover, in a memorandum of understanding (MOU) between the FCC and the FTC, both agencies expressly address the common carrier exemption, and commit to coordinate their respective jurisdictions. For example, the agencies "express their belief that the scope of the common carrier exemption in the FTC Act does not preclude the FTC from addressing non-common carrier activities engaged in by common carriers."

They also agree that enforcement authority exercised by the FTC should not be viewed as a limitation of the FCC's authority, including "FCC authority over activities engaged in by common carriers and by non-common carriers for and in connection with common carrier services." The MOU further notes that no exercise of enforcement authority by the FCC "should be taken to be a limitation on authority otherwise available to the FTC." In other words, the common carrier exemption only preempts the FTC's authority over common carriers in instances where they engage in common carrier activities. The MOU underscores that both the FTC and FCC have sufficient authority to pursue common and non-common carriers in appropriate instances.

Question 4 Why does USTelecom think that this would, or would not be, an effective means of policing robocalls?

Answer. Because the FCC already has full authority to pursue appropriate remedies against carriers, USTelecom is concerned that elimination of the common carrier exception could lead to regulation of the communications industry by two separate agencies. This in turn has the potential to create duplicative or conflicting regulatory requirements, resulting in additional consumer confusion and frustration.

Moreover, USTelecom believes that existing statutory tools are sufficient for addressing the robocall issue both in terms of civil and criminal enforcement.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JOHN THUNE TO
SCOTT DELACOURT

Question. During the hearing, Ms. Saunders testified that “one big issue is that if auto dialer is not sufficiently defined broadly, it won’t cover texts. There is no independent language in the TCPA that’ll cover texts unless the auto dialer definition is covered.” Do you agree with Ms. Saunderson’s assessment? Please explain.

Answer. No, I do not agree the above assessment, as it is incorrect and shows a fundamental misunderstanding of the Telephone Consumer Protection Act (“TCPA”) and its implementation. Additionally, Ms. Saunders’s assessment does not account for the robust protections that consumers have to prevent unwanted text messages, nor does the assessment consider the common and best practices of legitimate U.S. companies seeking to build positive relationships with consumers.

First, the statement that “[t]here is no independent language in the TCPA that’ll cover texts unless the auto dialer definition is covered” is simply incorrect. The independent language in the statute that allows the TCPA to cover text messages is “any call.”¹ Specifically, the statute prohibits any person from “mak[ing] any call (other than a call made for emergency purposes or made with the prior express consent of the called party) using any automatic telephone dialing system or an artificial or prerecorded voice” to certain telephone lines and numbers, including wireless numbers.² “Call” is not defined in the statute, and has therefore been interpreted by both the Federal Communications Commission (“FCC”) and various courts. It is now well-settled law that the term “any call” encompasses text messages. In 2003, the FCC affirmed that “*any call* . . . encompasses both voice calls and text calls to wireless numbers including, for example, short message service (SMS) calls.”³ Courts agree that texts are calls for TCPA purposes, and have held that the FCC’s interpretation of the word “call” is entitled to *Chevron* deference.⁴ In sum, text messages are covered under the TCPA based on the statute’s “any call” language, not its “ATDS” language.

Second, there is no direct relationship between the definition of “automatic telephone dialing system” or “ATDS” and the TCPA’s application to text messages. The ATDS definition is key to determining whether the TCPA’s consent restrictions apply to calls to wireless numbers, among other things. It has nothing to do with whether text messages—as a broad category of calls—are covered under the TCPA. As described above, that issue rests on the definition of another term in the statute: “any call.” If the Commission narrows the definition of ATDS in line with the plain meaning of the statute, text messages will still be covered.

Third, in addition to being incorrect and reflecting a misunderstanding of the implementation of the TCPA, Ms. Saunders’s statement ignores a key and robust protection that consumers have against unwanted telemarketing text messages—the Do Not Call rules. The TCPA gives consumers the ability to register numbers on the National Do Not Call Registry to prevent unwanted telemarketing calls. This protection extends to wireless telephone numbers as well as wireline numbers.⁵ In addition, consumers may take advantage of the TCPA’s company-specific do-not-call lists to prevent unwanted telemarketing messages.⁶ The Do Not Call rules are not triggered by whether a caller uses an ATDS—even manual telemarketing calls must

¹ 47 U.S.C. § 227(b)(1)(A); *see also* 47 C.F.R. § 64.1200(a)(1) (prohibiting “any telephone call” initiated using an ATDS or an artificial or prerecorded voice without consent or an emergency purpose).

² *See* 47 U.S.C. § 227(b)(1)(A).

³ *In the Matter of Rule and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02–278, Report and Order, 18 FCC Rcd. 14014 (¶165) (July 3, 2003) (“2003 TCPA Order”); *see also In the Matter of Rule and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02–278, Report and Order, 27 FCC Rcd. 1830 (¶4) (Feb. 15, 2012) (“2012 TCPA Order”) (“The Commission has concluded that the prohibition encompasses both voice and text calls, including short message service (SMS) calls, if the prerecorded call is made to a telephone number assigned to such service.”).

⁴ *See Satterfield v. Simon & Schuster, Inc.*, 569 F.3d 946 (9th Cir. 2009).

⁵ 2003 TCPA Order at ¶33 (“We conclude that the national database should allow for the registration of wireless telephone numbers, and that such action will better further the objectives of the TCPA and the Do-Not-Call Act.”).

⁶ *See* 47 C.F.R. § 64.1200(e).

comply with Do Not Call.⁷ Accordingly, narrowing the definition of ATDS in line with the plain language of the statute would not affect a consumer's ability to prevent unwanted telemarketing texts using the Do Not Call rules.

Fourth, consumers are also protected against unwanted text messages by the common and best practices of legitimate U.S. companies. Independent of the TCPA framework, it is a best practice to include an option for consumers to opt-out of text messages and to honor such opt-outs. Not only is this good business—as I testified, U.S. businesses have no interest in engaging in abusive practices and fear the brand and customer relationship damage of being cast as an illegal and abusive robocaller—but it is also enforced by industry itself. For example, CTIA—The Wireless Association administers the Short Code Registry program, a common way of sending marketing text messages. As part of the program, CTIA publishes the Short Code Monitoring Handbook, which describes best practices for short code programs and “requires all short code programs to comply with a basic code of conduct that promotes the best possible user experience.”⁸ One key best practice is that, “[f]unctioning opt-out mechanisms are crucial for all short code programs to comply with the CTIA Short Code Compliance Handbook. Programs must always acknowledge and respect customers’ requests to opt out of short code programs. Short code programs must respond to, at a minimum, the universal keywords STOP, END, CANCEL, UNSUBSCRIBE, and QUIT by sending an opt-out message and, if the user is subscribed, by opting the user out of the program.”⁹ CTIA audits against this and other best practices, and failure to comply with the Handbook may result in suspension from the short code registry.¹⁰ Accordingly, even if a non-marketing text message is not covered under the TCPA because it is not made using an ATDS, industry common and best practices still value and protect consumer choice.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO
SCOTT DELACOURT

Question 1. What is the interplay between privacy and robocalls?

Answer. The TCPA reflects a balance between consumer protection and the benefits of communications between businesses and consumers. In enacting the TCPA in 1991, Congress made clear that regulation of calling must balance consumers’ rights to privacy with legitimate business interests: “[i]ndividuals’ privacy rights, public safety interests, and commercial freedoms of speech and trade must be balanced in a way that protects the privacy of individuals and permits legitimate telemarketing practices.”¹ The TCPA does not prohibit all technologically assisted calling, and does not regulate all calls by businesses.

The FCC has acknowledged this. For example, in formulating TCPA rules, the Commission has stated that, “the rules the Commission adopts” aim to “strike an appropriate balance between maximizing consumer privacy protections and avoiding imposing undue burdens on telemarketers.”² Time and again, the FCC has “affirm[ed] the vital consumer protections of the TCPA while at the same time encouraging pro-consumer uses of modern calling technology.”³ Recently Commissioner O’Rielly recognized the importance of balancing these interests, noting that the Commission’s actions should “protect consumers from unwanted communications while enabling legitimate businesses to reach individuals that wish to be contacted. That is the balance that Congress struck when it enacted the [TCPA] in 1991.”⁴

With the TCPA’s passage in 1991, Congress’s primary aim was to alleviate intrusive telemarketing calls—like nuisance calls during dinner—and junk faxes. As Chairman Pai has said, “Congress passed the [TCPA] to crack down on intrusive telemarketers and over-the-phone scam artists.”⁵ In the Preamble to the TCPA,

⁷ See *id.* § 64.1200(c) (restricting “any telephone solicitation[s]”); *id.* § 64.1200(d) (restricting “any call[s] for telemarketing purposes”).

⁸ Short Code Monitoring Handbook, CTIA Short Code Monitoring Program, Version 1.7, at 3 (March 27, 2017).

⁹ *Id.* at 4.

¹⁰ *Id.* at 14–16.

¹ *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02–278, Report and Order, 27 FCC Rcd. 1830, ¶24 (Feb. 15, 2012).

² *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02–278, Report and Order, 18 FCC Rcd. 14014, ¶1 (July 3, 2003).

³ *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02–278; Declaratory Ruling and Order, 30 FCC Rcd. 7961, ¶2 (July 10, 2015) (“2015 Declaratory Ruling and Order”).

⁴ *Id.* at 8084 (Statement of Commissioner Michael O’Rielly Dissenting in Part and Approving in Part).

⁵ *Id.* at 8072 (Dissenting Statement of then-Commissioner Ajit Pai).

Congress cited the “proliferation of intrusive, nuisance calls to [consumers’] homes from telemarketers” as a reason for acting.⁶ According to the Supreme Court, “Congress determined that Federal legislation was needed because *telemarketers*, by operating interstate, were escaping state-law prohibitions on *intrusive nuisance calls*.”⁷

Question 2. How do robocallers get access to our private information in order to target consumers for robocalls?

Answer. As I discussed during my oral testimony, the term robocallers often encompasses two very different types of callers—the first being bad actor telemarketers, the second being companies trying to lawfully contact their consumers for a legitimate business purpose. The Chamber’s knowledge only extends to those in the second category of callers. There are varied methods for compiling and building customer and target lists for legitimate communications. The Chamber represents companies who place calls based on valid consent (either written or non-written, depending on the context), which can be obtained in several ways, including through business transactions, customer inquiries, or written consent.

Question 3. Is there any evidence that robo callers share call lists with each other or on the dark web which has the potential of creating repeat victims?

Answer. Chamber members engage in legal calling campaigns. I am not familiar with how bad actors obtain phone numbers, whether on the Dark Web or otherwise.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO
TO SCOTT DELACOURT

Question 1. Calls from Legitimate Businesses—In your testimony, you said “The TCPA prohibits making phone calls to wireless telephone numbers “using any automatic telephone dialing system” (“ATDS”) without the prior express consent of the called party. The Act focuses on technology, not bad conduct such as harassment or fraud.” How does the Chamber think the law could be changed to ensure that robocall enforcement targets harassment?

Answer. This question rightly inquires how to focus enforcement on bad actors, not on well-intentioned U.S. businesses that use a new technology or make a technical error.

Currently, the TCPA is abused by class action plaintiffs’ lawyers to seek from U.S. businesses enormous statutory damages that bear no relationship to harm. These lawsuits, while profitable for lawyers, do not benefit class members and do nothing to deter truly bad actors.⁸

It would be preferable for the law to focus on calls that are placed with the intent to defraud or otherwise do harm. Rather than focus on technology (*i.e.*, whether an automated telephone dialing system (“ATDS”) was used to place the call), Congress could look to the Truth in Caller ID Act of 2009,⁹ which outlaws “*intentionally harmful or fraudulent* spoofing of caller ID information.”¹⁰ Specifically, the Truth in Caller ID Act makes it “unlawful for any person within the United States, in connection with any telecommunications service or IP-enabled voice service, to cause any caller identification service to knowingly transmit misleading or inaccurate caller identification information *with the intent to defraud, cause harm, or wrongfully*

⁶Telephone Consumer Protection Act of 1991, PL 102–243, 105 Stat. 2394, § 2 (Dec. 20, 1991).

⁷*Mims v. Arrow Financial Services, LLC*, 565 U.S. 368, 370 (2012) (also citing the Preamble of the TCPA) (emphasis added); see also *Emanuel v. Los Angeles Lakers, Inc.*, 2013 WL 1719035, at *3 (“Courts “broadly recognize that not every text message or call constitutes an actionable offense; rather, the TCPA targets and seeks to prevent the proliferation of intrusive, nuisance calls.” (internal quotations omitted)).

⁸*Unstable Foundation: Our Broken Class Action System and How to Fix It*, U.S. Chamber Institute for Legal Reform, at 15 (October 2017), [https://www.instituteforlegalreform.com/uploads/sites/1/UnstableFoundation Web 10242017.pdf](https://www.instituteforlegalreform.com/uploads/sites/1/UnstableFoundation%20Web%20242017.pdf) (“Critics of the current class action system point to the absence of any substantial compensation for class members, the control by plaintiffs’ lawyers of the class action process, and the unchecked conflict of interest between class members and class counsel. Defenders of the current system argue that these points should all be disregarded, because class actions supposedly deter unlawful conduct and provide potential defendants with a powerful incentive to act lawfully. This deterrence argument may sound good, but there is a big difference between theory and practice. The reality of class actions shows that there is no credible basis for a deterrence justification.”).

⁹Truth in Caller ID Act of 2009, PL 111–331, 124 Stat. 3571 (Dec. 22, 2010) (codified at 47 U.S.C. § 227(e)).

¹⁰*Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, WC Docket No. 11–39, Notice of Proposed Rulemaking, 26 FCC Rcd. 4128 ¶1 (March 9, 2011).

obtain anything of value.”¹¹ Amending the TCPA to include a similar focus on intentionally harmful or fraudulent actions would more effectively target the behavior that is likely to harm consumers while protecting the modern communications that consumers desire.

There are several other steps that could move the TCPA in the right direction to benefit consumers without unduly harming U.S. businesses. For example, Congress could create robust safe harbors for legitimate businesses that take reasonable steps to avoid violating the TCPA. Congress also should remove the private right of action and leave enforcement to the agencies that have the tools and expertise to attack the problem in a concerted and consistent fashion.

Question 2. If the perpetrator of calls makes millions of billions of calls that are non-fraudulent but nonconsensual, how does the Chamber believe the law should impact those robocallers?

Answer. Your question raises two main concerns: consumer consent to receive calls and call volumes. Regarding consent, the Chamber believes that the TCPA is in need of reform. The TCPA—as interpreted by the FCC—dictates consent requirements based on (1) the technology used to place the call, (2) the type of number to which a call is delivered, and (3) the content of a call.¹² The consent requirement is subject to change if any one of these three elements changes. For example, if the caller uses an ATDS or an artificial or prerecorded voice to place a *telemarketing* call to wireless number, then the caller must first obtain written consent from the consumer; if the caller uses an ATDS or an artificial or prerecorded voice to place a *non-telemarketing* call to wireless number, then the consent from the consumer does not need to be in writing, but still must be obtained expressly from the consumer and prior to the call being placed. These consent requirements are overly complicated, and they detract from what should be the real focus of policymakers: stopping bad actors that purposefully evade the consent requirement and that call with the intent to defraud. The TCPA should not—as it does today—expose to ruinous liability well-intentioned companies that take advantage of modern technology to communicate quickly and efficiently with consumers.

Regarding call volume, I respectfully suggest that this is a red herring. The mere fact that a caller places a high volume of calls is not inherently bad, as there are calls that consumers want to receive. So long as a caller in good faith attempts to comply with the consent requirements and does not have the intention of defrauding or otherwise doing harm to consumers, the caller should be able to place as many calls as it sees fit to communicate lawfully with customers. Fundamentally, call volume—on its own—is not a relevant metric on which policymakers should focus. Whether a legitimate company places one hundred or one million calls with consumer consent, no consumer harm occurs.

Question 3. Banking—In 2014 a couple won a lawsuit against Bank of America for more than \$1 million after they were flooded with robotic collection calls over the course of several years. It is understandable that banks and other companies want to contact their customers about issues, but we cannot have financial institutions blatantly ignoring the law and instituting a policy of annoying their customers with illegal phone calls. Does the Chamber believe that banks, because they are legitimate businesses, should be able to make collection calls without user consent?

Answer. Businesses have every incentive to cultivate positive customer relationships while using modern technology to efficiently communicate with customers, including about debt collection.

As it happens, debt collection calls are ordinarily made with consent. As the FCC has recognized, the provision of a phone number in the context of incurring a debt constitutes consent for the purposes of the TCPA.¹³ We support the FCC’s practices of permitting legitimate businesses to communicate with their customers regarding repayment of debts. Importantly, the TCPA is not the only, or even the primary, law that governs the debt collection process.¹⁴ Debt collection activities are heavily

¹¹ 47 U.S.C. § 227(e)(1).

¹² See 47 C.F.R. § 64.1200(a)(1) (imposing one consent requirement on *any* call to a wireless number utilizing an ATDS or an artificial or prerecorded voice); *id.* § 64.1200(a)(2) (imposing a different consent requirement on a telemarketing or advertising call to a wireless number utilizing an ATDS or an artificial or prerecorded voice); *id.* § 64.1200(a)(3) (imposing consent requirements on calls placed to residential landlines utilizing an artificial or prerecorded voice).

¹³ *Request of ACA International for Clarification and Declaratory Ruling*, CG Docket No. 02–278, Declaratory Ruling, 23 FCC Rcd. 559, ¶9 (Jan. 4, 2008) (“2008 Declaratory Ruling”) (“We conclude that the provision of a cell phone number to a creditor, *e.g.*, as part of a credit application, reasonably evidences prior express consent by the cell phone subscriber to be contacted at that number regarding the debt.”).

¹⁴ See, *e.g.*, Fair Debt Collection Practices Act, 15 U.S.C. § 1692 et seq.

regulated at the Federal and state levels. The Chamber supports its members' compliance with these regulations.

Question 4. A one million dollar cost, as shown in this case, is not a significant sum for a large bank, does the Chamber believe this is significant enough to deter "harassment?"¹⁵

Answer. The fundamental problem with the TCPA is its statutory damages, coupled with its private right of action. TCPA class action lawsuits have skyrocketed in recent years. As the Chamber recently explained "Settlement is where almost all TCPA cases end up if a class is certified, or if certification seems at all likely, because of the in terrorem value of classwide claims. In TCPA litigation, every 2,000 calls can equate to \$1 million in potential statutory damages, even before potential 'willfulness' damages are considered."¹⁵



¹⁵*Id.* at 9.