DO NOT CALL: COMBATING ROBOCALLS AND CALLER ID SPOOFING

HEARING

BEFORE THE

SUBCOMMITTEE ON DIGITAL COMMERCE AND
CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

———

APRIL 27, 2018

———

Serial No. 115–123

COMMITTEE ON ENERGY AND COMMERCE

GREG WALDEN, Oregon
Chairman

JOE BARTON, Texas
  Vice Chairman
FRED UPTON, Michigan
JOHN SHIMKUS, Illinois
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY McMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. McKINLEY, West Virginia
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
LARRY BUCSHON, Indiana
BILL FLORES, Texas
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
CHRIS COLLINS, New York
KEVIN CRAMER, North Dakota
TIM WALBERG, Michigan
MIMI WALTERS, California
RYAN A. COSTELLO, Pennsylvania
EARL L. "BUDDY" CARTER, Georgia
JEFF DUNCAN, South Carolina

FRANK PALLONE, JR., New Jersey
  Ranking Member
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DeGETTE, Colorado
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
G.K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY McNERNEY, California
PETER WELCH, Vermont
BEN RAY LUJÁN, New Mexico
PAUL TONKO, New York
YVETTE D. CLARKE, New York
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY, III, Massachusetts
TONY CÁRDENAS, California
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan

SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER PROTECTION

ROBERT E. LATTA, Ohio
Chairman

GREGG HARPER, Mississippi
  Vice Chairman
FRED UPTON, Michigan
MICHAEL C. BURGESS, Texas
LEONARD LANCE, New Jersey
BRETT GUTHRIE, Kentucky
DAVID B. McKINLEY, West Virginia
ADAM KINZINGER, Illinois
GUS M. BILIRAKIS, Florida
LARRY BUCSHON, Indiana
MARKWAYNE MULLIN, Oklahoma
MIMI WALTERS, California
RYAN A. COSTELLO, Pennsylvania
JEFF DUNCAN, South Carolina
GREG WALDEN, Oregon *(ex officio)*

JANICE D. SCHAKOWSKY, Illinois
  Ranking Member
BEN RAY LUJÁN, New Mexico
YVETTE D. CLARKE, New York
TONY CÁRDENAS, California
DEBBIE DINGELL, Michigan
DORIS O. MATSUI, California
PETER WELCH, Vermont
JOSEPH P. KENNEDY, III, Massachusetts
GENE GREEN, Texas
FRANK PALLONE, JR., New Jersey *(ex officio)*

(II)

CONTENTS

DO NOT CALL: COMBATING ROBOCALLS AND CALLER ID SPOOFING

FRIDAY, APRIL 27, 2018

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER
PROTECTION,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 9:03 a.m., in room 2123, Rayburn House Office Building, Hon. Robert Latta, (chairman of the subcommittee) presiding.

Present: Representatives Latta, Kinzinger, Lance, Guthrie, Bilirakis, Mullin, Costello, Duncan, Walden (ex officio), Schakowsky, Dingell, Matsui, Welch, Kennedy, Green, and Pallone (ex officio).

Staff Present: Mike Bloomquist, Staff Director; Daniel Butler, Staff Assistant; Margaret Tucker Fogarty, Staff Assistant; Melissa Froelich, Chief Counsel, Digital Commerce and Consumer Protection; Adam Fromm, Director of Outreach and Coalitions; Ali Fulling, Legislative Clerk, Oversight and Investigations, Digital Commerce and Consumer Protection; Elena Hernandez, Press Secretary; Zach Hunter, Director of Communications; Paul Jackson, Professional Staff, Digital Commerce and Consumer Protection; Bijan Koohmaraie, Counsel, Digital Commerce and Consumer Protection; Drew McDowell, Executive Assistant; Hamlin Wade, Special Advisor, External Affairs; Greg Zerzan, Counsel, Digital Commerce and Consumer Protection; Michelle Ash, Minority Chief Counsel, Digital Commerce and Consumer Protection; Jeff Carroll, Minority Staff Director; Lisa Goldman, Minority Counsel; Jerry Leverich, Minority Counsel; Caroline Paris-Behr, Minority Policy Analyst; and Michelle Rusk, Minority FTC Detailee.

OPENING STATEMENT OF HON. ROBERT E. LATTA, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

Mr. LATTA. Well, good morning. I would like to call the Subcommittee on Digital Commerce and Consumer Protection to order. And the chair now recognizes himself for 5 minutes for an opening statement.

Good morning again. We thank our witnesses for being here. We especially appreciate your patience and flexibility, adjusting your travel plans after the hearing was rescheduled from last week.

We want to thank you for being here to help us explore the range of solutions and strategies available to consumers to combat the scourge of robocalls, caller ID spoofing, and telemarketing scams.

It is critical that we help consumers understand their options when it comes to robocalls and spoofing.

For example, consumers can download robocall-blocking apps for their mobile phones and contact their landline and wireless providers for call-blocking options.

They can register their home or mobile phones with the national Do Not Call Registry, which protects their number from legitimate telemarketing calls they do not want to receive.

And there are other commonsense strategies, like not answering your calls from unknown numbers and not following any prompts if you do not know who the call is from. For example, do not "press 1 to take your name off this list."

Good options are available, but I think all of us, including industry, can and should do a better job of education, particularly with our seniors, to make sure that new scam ideas are stopped quickly.

So what is a robocall? When the phone rings with an automated prerecorded telemarketing message, that is a robocall. They are a nuisance and they are illegal. Yet every day tens of thousands of American consumers report receiving a robocall. And I would like to just play a real quick "robocall" from the IRS.

[Audio recording played.]

Mr. LATTA. And that message goes on.

A staggering 3.2 billion robocalls were placed nationwide in the month of March, according to one source, alone. InOhio's 419 area code alone, my area code, nearly 12 million robocalls were placed. For every month in the past year robocalls made up the majority of Do Not Call Registry complaints at the Federal Trade Commission.

As technology evolves allowing for a greater volume of robocalls, so are the tactics used to trick consumers into answering. In the past scammers would fake caller ID information to trick consumers into thinking their bank was calling or the phone number was unknown. Scammers are now deliberately falsifying caller ID information knowing I am likely to answer a phone call that appears to be local from my family, a doctor, or the church. Neighbor spoofing, as it is known, is a deliberate tactic behind unwanted calls and texts to both wireline and wireless phones.

Robocalls and spoofing have the potential for real financial harm. Fraud from unwanted calls amounts to almost $9.5 billion annually, according to the FTC. It is not hard to see how scammers could use deceptive tactics to convince people, often senior citizens, to hand over their personal information or to purchase fraudulent goods and services.

Take the IRS tax scam, for example. You get that unexpected phone message claiming to be from the IRS. The call might say you owe taxes that must be paid immediately with a credit card or a debit card. Scammers have been known to use the threat of a lawsuit or arrest by the police to convince victims to hand over bank account information.

Consumers may also get out-of-the-blue calls offering to help them lower debt or interest rates or promising other limited-time deals. Senior citizens are often targets of elderly-specific roboscams relating to Medicare, healthcare, or funeral arrangements. But they are not the only ones who fall victim to these scams.

Fortunately, American consumers have options and strategies to fight robocalls and caller ID spoofing and to protect themselves, which we will explore today with our witnesses.

The technology and tactics used by scammers may change, but as subcommittee chairman, I remain focused on empowering consumers and keeping them safe from unfair, deceptive, and malicious practices.

Again, I want to thank our witnesses for being here today.

And with that I will yield back and recognize the gentlelady from Michigan for 5 minutes.

[The prepared statement of Mr. Latta follows:]

PREPARED STATEMENT OF HON. ROBERT E. LATTA

Good morning. We thank our witnesses for being here today. We especially appreciate your patience and flexibility adjusting your travel plans after this hearing was rescheduled from last week.

Thank you for being here to help us explore the range of solutions and strategies available to consumers to combat the scourge of robocalls, caller ID spoofing, and telemarketing scams. It is critical that we help consumers understand their options when it comes to robocalls and spoofing.

For example, consumers can download robocall-blocking apps for their mobile phones, or contact their landline and wireless providers for call-blocking options.

They can register their home or mobile phones with the National Do Not Call Registry, which protects their number from legitimate telemarketing calls they do not want to receive.

And there are common sense strategies like not answering calls from unknown numbers and not following any prompts if you do not know who the call is from-for example do not "press 1 to take your name off this list."

Good options are available, but I think all of us, including industry, can and should do a much better job of education, particularly with our seniors, to make sure that new scam ideas are stopped quickly.

So what's a robocall? When the phone rings with an automated, pre-recorded telemarketing message that's a robocall. They're a nuisance, and they're illegal. Yet, every day tens of thousands of American consumers report receiving a robocall.

A staggering 3.2 billion robocalls were placed nationwide in the month of March, according to one source. In Ohio's 419 area code alone, my local area code, nearly 12 million robocalls were placed. For every month in the past year, robocalls made up the majority of Do Not Call Registry complaints at the Federal Trade Commission.

As technology evolves allowing for a greater volume of robocalls, so are the tactics used to trick consumers into answering. In the past, scammers would fake caller ID information to trick consumers into thinking their bank was calling or the phone number was "unknown." Scammers are now deliberately falsifying caller ID information knowing I'm likely to answer a phone call that appears to be local, from my family, doctor or church. "Neighbor spoofing," as it's known, is a deliberate tactic behind unwanted calls and texts to both wireline and wireless phones.

Robocalls and spoofing have the potential for real financial harm. Fraud from unwanted calls amounts to almost $9.5 billion annually, according to the FTC. It's not hard to see how scammers could use deceptive tactics to convince people—often senior citizens—to hand over their personal information or to purchase fraudulent goods and services.

Take the IRS tax scam, for example: you get an unexpected phone message claiming to be from the IRS. The call might say you owe taxes that must be paid immediately with a credit card or debit card. Scammers have been known to use the threat of a lawsuit, or arrest by the police, to convince victims to hand over bank account information.

Consumers may also get out-of-the blue calls offering to help lower debt or interest rates, or promising other "limited time" deals. Senior citizens are often targets of elderly-specific robocall scams relating to Medicare, health care, or funeral arrangements. But they are not the only ones who fall victim to these scams.

Fortunately, American consumers have options and strategies to fight robocalls and caller ID spoofing, and to protect themselves, which we will explore today with our witnesses.

The technology and tactics used by scammers may change, but as subcommittee chairman I remain focused on empowering consumers and keeping them safe from unfair, deceptive, and malicious practices.

Thank you again to our witnesses for being here today for this important discussion.

OPENING STATEMENT OF HON. DEBBIE DINGELL, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mrs. DINGELL. Thank you, Mr. Chairman, and thank you for holding today's hearing on robocalls and spoofing.

And thank you to the witnesses for being here today.

Robocalls are a great annoyance for American families, especially American seniors. One third of the calls now are unwanted robocalls. Just in March, a record 3 billion robocalls were placed to American consumers, and about a quarter of those calls are scam calls.

We are now at a point in my household when the hard line rings I tell my husband, "Don't answer it." And he thought I didn't pay our taxes. He got pretty upset with me actually. It took me a while to convince him I had.

I hear repeatedly from my constituents that they want these calls to stop. One constituent in Ann Arbor wrote:

"My landline and cell numbers are both on the Federal Do Not Call Registry. I checked. I am so angry about all the calls from offshore call banks telling me that my computer is broken or that I need help with medical insurance and my college loans.

"Exactly what does the Do Not Call list do? Not answering and letting someone call back isn't an option, as I have an elderly parent who does call. I am also not wanting to go to the expense of updating my phone system to get caller ID."

There were many more just like this, and to no one's surprise there wasn't one letter in support of robocalls.

Democrats on the Energy and Commerce Committee have been listening to their constituents and we are taking action. This week Democrats are introducing three bills to help stop robocalls.

Ranking Member Pallone introduced the Stopping Bad Robocalls Act, which would strengthen the Telephone Consumer Protection Act and help the FCC take action against robocallers.

Congresswoman Eshoo introduced the HANGUP Act, which would require debt collectors contracted with the Federal Government to get consumers' permission before robocalling or auto dialing consumers.

And last, but certainly not least, today we have released a discussion draft titled the CEASE Robocalls Act. This draft legislation would lift the common carrier exemption in the Federal Trade Commission Act so that the FTC can take action against these smaller Voice over Internet Protocol, otherwise called VoIP services, that are a huge player and heavily involved in illegal robocalls.

I am looking forward to getting feedback from all of you today about the discussion draft.

Today we will hear from witnesses about some of the exciting and promising tools available to consumers wishing to block

robocalls. But consumers don't just need new tools. They need new protections.

We have put forward commonsense ideas to stop Americans from being harassed by unwanted calls. I hope we can all work together to move this legislation forward and make progress on the issue because many of us are growing tired of having to leave their phones on silent.

Thank you, Mr. Chairman, and I yield back my time.

Mr. LATTA. Thank you very much. The gentlelady yields back.

The chair now recognizes the gentleman from Oregon, the chairman of the full committee, for 5 minutes.

OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

Mr. WALDEN. Thank you, Mr. Chairman.

I share the passion of the rest of the members here about these unwanted, unnecessary, and oftentimes fraudulent calls. I get them on my cell phone all the time. They appear to be coming from I think my home at times, they are that good anymore. And we have got to do something about this. And we have. I am going the talk about that in my opening statement here a bit.

And then we appreciate our witnesses for being here.

Robocalls and caller ID spoofing have exploded in recent years, 3 billion calls placed last month alone, they estimate. And we all get them. And they interrupt our dinners, they interrupt our family time, they interrupt meetings. They are real annoying, to say the least.

At worst, they have the potential to scam and defraud both consumers, seniors, and others. According to the Department of Justice, scams targeting the elderly are increasing dramatically and fraudsters steal an estimated $3 billion from American seniors every year. It is now more important than ever to educate consumers on how to detect and avoid fraud stemming from these robocalls.

The Federal Trade Commission and the Federal Communications Commission, as well as our committee, have taken steps to protect consumers from robocalls and spoofing. Both the FTC and the FCC operate consumer complaint Web sites and hotlines where consumers can report illegal telemarketing calls. Reporting can help the agencies crack down on illegal callers and improve the data they share with the industry players and telecommunications companies, who then develop solutions. The Federal Trade Commission also manages the Do Not Call Registry, where anyone can register their home or mobile phone for free.

Here at the Committee we recently passed the RAY BAUM'S Act, which includes provisions directing the Federal Communications Commission to expand and clarify the prohibition on misleading or spoofed caller ID information. It also requires that they, in consultation with the Federal Trade Commission, create consumer education materials on how to avoid this type of spoofing. These provisions were signed into law by the President in March.

This is just one of many steps in the right direction. But as communication technology continues to advance, so do the tools and tactics of these illegal telemarketers, and they use those tactics and

tools to evade existing protections. So we have to stay ahead of them. So-called neighbor spoofing is one of the most effective new tactics. It is particularly hard to detect. Scammers use phone numbers with your area code and/or an area code nearby, and that gets your trust. Many consumers are likely to answer when it looks like the call could be coming from, let's say, their child's school, their local church, or their dentist's office.

What do we need to do to stop these bad actors? As I said earlier, I, for one, am pretty sick and tired of them.

We also finished up another tax season last week. IRS scammers are going after taxpayers as well. Using the internet and social media, fraudsters can convincingly portray IRS employees by naming a few identifying facts, like your home address or current city of residence.

To avoid falling prey to these calls and others never give personal identifiable information over the phone. Government officials will never ask you for your bank account information or Social Security number over the phone. Consumers should hang up and then they should call the IRS office and check if it was a legitimate call.

And the bad actors keep evolving. So we need to make sure that our consumers have what they need to stay ahead of them. There are a wide array of technical and marketplace solutions consumers can use to block, avoid, or otherwise protect themselves from robocalls or caller ID spoofing. There are now 500 call-blocking apps for Android, Apple, and other devices. Many home phone providers offer the option to add robocall-blocking functions to their service for free, and today, because of our witnesses, we will hear from some of these innovators.

And again, we thank you for your work and your willingness to be here.

I have found, too, if I just let it go to voicemail they never leave voicemail, and then I know it is just a spoof.

So anyway, Mr. Chairman, I will yield back the balance of my time. Thanks for having this hearing.

[The prepared statement of Mr. Walden follows:]

PREPARED STATEMENT OF HON. GREG WALDEN

Good morning and thank you to our witnesses for being here today. Robocalls and caller ID spoofing have exploded in recent years, with over 3 billion calls placed last month alone. We all get them. Whether they're interrupting a family sitting down to dinner in Bend, or ringing during a meeting in Washington, everyone experiences the pervasive and invasive effects.

At best, these calls are annoying. At worst, they have the potential to scam and defraud consumers, especially senior citizens. According to the Department of Justice, scams targeting the elderly are increasing dramatically, and fraudsters steal an estimated 3 billion dollars from American seniors each year. It is now more important than ever to educate consumers on how detect and avoid fraud stemming from robocalls.

The Federal Trade Commission and Federal Communications Commission, as well as our own Committee, have taken steps to protect consumers from robocalls and spoofing. Both the FTC and FCC operate consumer complaint websites and hotlines where consumers can report illegal telemarketing calls. Reporting can help the agencies crack down on illegal callers and improve the data they share with industry players and telecommunications companies, who then develop solutions. The FTC also manages the National Do Not Call Registry, where anyone can register their home or mobile phone for free.

Here at the Committee, we recently passed the RAY BAUM'S Act, which includes provisions directing the FCC to expand and clarify the prohibition on misleading or spoofed caller ID information. It also requires that they, in consultation with the FTC, create consumer education materials on how to avoid this type of spoofing. These provisions were signed into law by the president in March.

This is just one of many steps in the right direction, but as communication technology continues to advance, so do the tools and tactics illegal telemarketers use to evade existing protections. So-called "neighbor spoofing" is one of the most effective new tactics, and it is particularly hard to detect. Scammers use phone numbers with your area code or an area code nearby to engender trust. Many consumers are likely to answer when it looks like the call could be coming from their child's school, their local church, or their dentist's office.

We also finished up another tax season last week. IRS schemes are on the rise as scammers deceive individuals into giving up their personal or financial information. Using the internet and social media, fraudsters can convincingly portray IRS employees by naming a few identifying facts, like your home address or current city of residence. To avoid falling prey to these calls and others, never give personally identifiable information over the phone. Government officials will never ask for your bank account information or social security number over the phone. Consumers should hang up and call their local IRS office to check if the call they received was legitimate.

The bad actors clearly keep evolving, and we need to make sure consumers stay one step ahead. There are a wide array of technical and marketplace solutions consumers can use to block, avoid, or otherwise protect themselves from robocalls and caller ID spoofing. There are now over 500 call blocking apps for Android, Apple, and other devices. Many home phone providers offer the option to add robocall blocking functions to their service for free. Today, we'll hear from a few of the innovators in robocall blocking and advanced caller ID technology on how to implement these strategies for both landline and mobile phones.

There is no silver bullet to solve the problem of unwanted calls, but we owe it to our constituents to present all the options available. Improving education and awareness will be key to preventing consumer harm. I want to thank our witnesses again for being here today, and I look forward to this important discussion.

Mr. LATTA. Thank you very much. The gentleman yields back.

The chair now recognizes the gentleman from Texas for 5 minutes.

OPENING STATEMENT OF HON. GENE GREEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. GREEN. Thank you, Mr. Chairman. I will be brief. I just want to thank you and the ranking member for holding this hearing.

This is one of the biggest complaints I get from senior citizens. And actually at my house, when I go back home after a week, I get calls saying the IRS is going to come over and I owe taxes. And I hear constituents complain about that, and I explain to them the IRS doesn't call you and tell you by phone. You will get a letter and keep in touch with us.

The other frustration is that on my cell phone, I haven't applied for a loan for many years, but I keep getting texts saying: Your $250,000 loan has been approved. I thought about saying: Send it to me and I will go to Costa Rica or someplace.

But it is frustrating to seniors, particularly if you are home all day, or young mothers who have children that they are worried about with all these kind of calls. So we need both the two agencies, the FCC and FTC, see what we can do. If they don't have the tools for it we need to do it.

And I thank you for having the hearing.

Mr. LATTA. Well, thank you very much. The gentleman yields back.

And that will conclude the member opening statements. The chair would like to remind members that, pursuant to committee rules, all members' opening statements will be made part of the record.

And again, I want to thank all of our witnesses for being here with us today, taking the time to testify before the subcommittee. Today's witnesses will have the opportunity to give 5-minute opening statements followed by a round of questions from the members.

Our witness panel for today's hearing includes Mr. Ethan Garr, the Chief Product Officer of RoboKiller; Mr. Aaron Foss, Founder of Nomorobo; Ms. Maureen Mahoney, the Policy Analyst at Consumers Union; and also, Mr. Scott Hambuchen, the Executive Vice President of Technology and Solution Development at First Orion.

So again, we want to thank you very much for being here.

And, Mr. Garr, you are recognized for 5 minutes. Thank you.

STATEMENTS OF ETHAN GARR, CHIEF PRODUCT OFFICER, ROBOKILLER; AARON FOSS, FOUNDER, NOMOROBO; MAUREEN MAHONEY, POLICY ANALYST, CONSUMERS UNION; AND SCOTT HAMBUCHEN, EXECUTIVE VICE PRESIDENT—TECHNOLOGY AND SOLUTION DEVELOPMENT, FIRST ORION

STATEMENT OF ETHAN GARR

Mr. GARR. I think we are going to begin with a clip.

[Audio recording played.]

Mr. GARR. Chairman Latta and members of the committee, I am Ethan Garr from RoboKiller, and what you just heard was one of our Answer Bots wasting a telemarketer's time.

Answer Bots are the solution to the robocall epidemic, and on June 19, 2021, RoboKiller and our Answer Bots will have solved this problem. See, on that date, at our current trajectory, we will have 10 million users deploying hundreds of millions of our time-wasting Answer Bots.

This will reduce spammers' revenue by more than 50 percent. That is enough of a disruption to their bottom line to put them out of business. We are attacking spammers where it hurts, in their wallets.

RoboKiller answers the calls it blocks with these Answer Bots, and they are smart. They know how to press 1 to reach the human behind Rachel from Cardholder Services. They know how to turn the tables on spammers and waste their time instead of yours. This is time that they no longer have to scam and steal not just from our users, but from anyone else, as well. This problem has gotten worse despite call-blocking technologies, despite legislation and enforcement.

But we are different. Our call-blocking competitors have approached this problem from the caller ID angle. But spoofing, caller ID blocking, and other tools limit the value of such approaches. It is a cat-and-mouse game that can really never be won. We are not interested in playing the game. We would rather steal the cheese that the spammers are after.

The spammers' business model is based on making billions of calls, knowing that only a small percentage will get answered, and

an even smaller percentage of those will connect human telemarketers with viable targets. They don't have to be surgical in their strikes. Robocalls let the most vulnerable in our society self-select themselves as victims.

So a relatively small pool of humans, often on the other side of the world, are just waiting for their auto-dialed robocall systems to connect, waiting for someone's grandmother to press 1 and say "Hello." But Answer Bots' inanimate identities cannot be stolen. Their invisible wallets can't be infiltrated. They can keep spammers wrapped up on calls for hours. And they are protecting you even if you don't have RoboKiller. Every minute our Answer Bots are engaging telemarketers is a minute they don't have to speak to someone else.

Our competitors are helping their users, but they are also helping scammers. Telemarketers are happy to skip a well-educated executive with a call-blocker app to get to the elderly grandmother who they know is more likely to fall victim to their scams. With Answer Bots our users are helping everyone.

Unfortunately, you can't solve this problem with legislation alone. A three-man IRS scam operation in a seedy, nondescript room in another country isn't worried that the long arm of the American justice system is ever going to knock on their door. As it became cheaper and cheaper to make calls, the incentive to deploy more robocalls has increased exponentially, as did the incentive to ignore the laws.

The Do Not Call Registry did exactly what it was supposed to do, but, unfortunately, not at all what people expected it to do. So stopping the tiny percentage of legal robocalls that fell under the Do Not Call list purview was almost no help to consumers who were expecting a panacea.

Beyond the Do Not Call list the government's efforts have been well intentioned and well executed. They just don't have broad implications on the problem. Despite the FCC and FTC's well-publicized multimillion dollar enforcement actions, with that estimated $9.5 billion in yearly phone scam revenue these efforts are just not a real deterrent.

No, the real solution to this problem is already in the app store, and it is called RoboKiller. And you can take pride in the fact that the government efforts have made this happen. We weren't in this fight until the FTC had the vision to look beyond legislation and enforcement towards innovation.

When the FTC created the Robocalls: Humanity Strikes Back competition in 2015 they got us, TelTech, into this fight. We have been innovating for 14 years, helping consumers use technology to protect their privacy and security on their phones.

From unmasking blocked calls with TrapCall, to recording calls with TapeACall, to helping people keep their numbers secure with SpoofCard, we have always been focused on giving people control of their phones.

The robocall competition ignited our passion and is accomplishing your goals to help Americans end the robocall epidemic.

We have already started to see the impact. When we heard a telemarketer say in an exasperated voice, "Oh, no, everyone has got RoboKiller today," we knew we had turned the tide. When we

heard another angrily yell at one of our Answer Bots, "Oh, which one are you, the guy with the baby, the guy on the movie set?" then we knew we were winning the fight.

From an adorable Southern belle to a guy dealing with a gazelle running around his apartment, our robots are hilarious, but just as important, they are effective.

Earlier this week we were able to showcase RoboKiller and Answer Bots at the FTC and FCC's joint technology expo, and today we have the privilege of testifying in front of this subcommittee. If you want us to help you solve this problem, please do more of this. Help us get more attention so that we can speed up our growth.

We are not worried about putting ourselves out of business by solving the problem. We have built a culture of innovation. So when the scammers start ringing doorbells after we have solved this problem we will have a solution for that, too.

Answer Bots wasted more than 25,000 hours of human telemarketers' time last month. For 150,000 users that represented hundreds of thousands of blocked calls and the peace of mind that when their phone rang it wasn't a harassing call from a scammer. For thousands of other Americans who have yet to purchase RoboKiller, that was 25,000 hours where they, too, were protected from those otherwise engaged telemarketers.

This robocall problem has grown into a true epidemic. Ever since I have been speaking, 2,700 unwanted calls are being made to American citizens every second. But it is over. RoboKiller and our Answer Bots are on the case.

Thank you very much.

[The prepared statement of Mr. Garr follows:]

Digital Commerce and Consumer Protection Subcommittee Hearing
Do Not Call: Combating Robocalls and Caller ID Spoofing

Ethan Garr, RoboKiller
Chief Product Officer, TelTech Systems

Summary of Testimony:

RoboKiller is a unique mobile application that is solving the robocall problem through disruption. The app answers the calls it blocks on behalf of its users, then deploys Answer Bots, our own army of robots designed to talk back to and waste spammers' time.

Spoofing, caller ID blocking, and other tools limit the effectiveness of solutions that simply block numbers. These services protect their users, but make it easier for scammers and spammers to skip over their savvy customer base to more quickly reach the most vulnerable Americans.

Our service turns the tables on telemarketers, engaging them in protracted conversations. Answer Bots cannot be robbed of their wealth or identities, and the time they waste doesn't just protect our users, it protects everyone else as it prevents telemarketers from making additional calls.

RoboKiller leverages several advanced technologies including audio-fingerprinting and machine learning to power an algorithm that blocks more than 200,000 spammer's numbers at any time. But answering the calls we block is what allows us to deploy our Answer Bots to truly combat the problem.

Spammers make billions of robocalls knowing that only a small percentage will get answered, and even fewer will reach their human telemarketers. They don't have to be targeted because robocalls let the most vulnerable in our society self-select themselves as victims. But last month our Answer Bots fought back and stole an estimated 25,000 hours of time from spammers and scammers.

This problem has reached epidemic proportions, and it is not going to be solved through legislation or enforcement, though both of those efforts are important. This is a problem fueled by inexpensive phone calls, and huge margins, so our solution focuses on impacting the economics of spam calls.

We are here because the FTC put innovation to work when it held the Robocalls: Humanity Strikes Back competition, which we were fortunate enough to win. The government can help solve this problem by continuing to support creative solutions. This hearing and the FTC and FCC's technology expo next week will help us spread our message and grow, and ultimately that will help us end the robocall scourge.

RoboKiller Written Statement

Every day we are adding thousands of RoboKiller users to our service, which means we are putting Answer Bots to work, hitting telemarketers where it hurts: in their wallets.

When our mobile application, RoboKiller, reaches 10 million users, we estimate we will have reduced spammer's revenue by more than 50%. We believe this is enough of a disruption to their bottom line to put them out of business.

Robokiller doesn't just block unwanted calls, it answers the calls it blocks with Answer Bots, our army of robots that know how to press one to reach the human behind "Rachel from Cardholder Services." Answer Bots, turn the tables on scammers and spammers by wasting their time. That is time that they no longer have to scam and steal from our users or anyone else.

Our competitors have approached this problem from the Caller ID angle, but spoofing, caller ID blocking, and other tools limit the value of those approaches. It is a cat and mouse game that can never be won. We are not interested in playing that game, we'd rather steal the cheese that the spammer's are after; our approach is about cutting off their revenue.

RoboKiller blocks more than 200,000 spam and telemarketing calls from ever reaching our hundreds of thousands of user's phones, but more importantly we answer the calls we block with these Answer Bots. From an adorable Southern Belle to a guy dealing with a gazelle running around his apartment, our robots are as hilarious as they are effective. But don't mistake entertaining for simplistic.

Our service leverages several advanced technologies including audio-fingerprinting and machine learning to power an algorithm that blocks spammer's calls, then answers those calls with Answer Bots. RoboKiller users can either create their own custom answer bots or choose ones from our library. That means at any given time thousands of unique Answer Bots can be fighting back against spammers.

How effective are they? In a single day, we deployed one of our answer bots more than 1200 times, and it interacted with telemarketers for more than 5000 minutes. Last month we estimate that Answer Bots wasted more than 25,000 hours of human telemarketer's time.

And remember, these robots are protecting you even if you don't have RoboKiller. Every minute our Answer Bots are engaging telemarketers is a minute they don't have to speak to anyone else.

The spammer's business model is based on making billions of calls, knowing that only a small percentage will get answered, and an even smaller percentage will connect their human telemarketers with viable targets. They don't have to be surgical in their strikes, robocalls let the most vulnerable in our society self-select themselves as victims.

So a relatively small pool of humans, often on the other side of the world, are sitting in seedy call centers and back rooms just waiting for their auto-dialed robocall systems to connect. Waiting for someone's grandmother to say "hello".

Answer Bots love to say hello, but their inanimate identities cannot be stolen. Their invisible wallets cannot be infiltrated. They can keep spammers engaged in conversations for several

minutes, and often much longer than that. Answer Bots are great revenge for our customers, but they are great news for all of you on this panel.

You cannot solve this problem with legislation alone. A three-man IRS scam operation in a nondescript room in India isn't worried that the long-arm of the American Justice system will ever knock on their door. And singularly-focused call blockers may even help the scammers. Scammers are happy to skip a well-educated young executive with a call blocker app to more quickly get to a vulnerable elderly grandmother.

The real solution to this problem is already in the app store and it's called RoboKiller, and you can take pride in the fact that government efforts made this happen. We weren't in this fight until the FTC had the vision to look beyond legislation and enforcement towards innovation. When the FTC created the Robocalls: Humanity Strikes Back competition in 2015 they got us, TelTech, into this fight.

We have been innovating for 15 years, helping consumers use technology to protect their privacy and security on their phones. From unmasking blocked calls with TrapCall, to recording calls with TapeACall, to helping people keep their numbers secure with SpoofCard, we have always been focused on giving people control of their phones. The robocall competition ignited our passion, and it is accomplishing your goals to help Americans end the robocall epidemic.

We have seen telemarketers change their tactics because Answer Bots have started to impact their bottom line. When we heard a telemarketer say in an exasperated voice, "Oh no, everyone's got RoboKiller today," we knew we had turned the tide. When we heard another scammer angrily yell, "oh which one are you? The guy with the baby, the guy on the movie set?" we knew we were winning the fight.

Telemarketers have had their way for years. As it became cheaper and cheaper to make calls, the incentive to deploy more robocalls increased exponentially and there was no way to fight back. The Do Not Call Registry did exactly what it was supposed to do, but unfortunately not at all what people expected it to do.

Stopping the tiny percentage of legal robocalls that fell under the Do Not Call list purview was almost no help to consumers who were expecting and counting on the government to deliver a panacea. In-fact, some have theorized that the Do Not Call list may even help spammers by giving consumers a false sense of security when the phone rings.

Beyond the Do Not Call List the government's efforts have been well-intentioned and well executed, they just don't have broad implications on the problem. Despite the FCC and FTC's well-publicized multi-million dollar enforcement actions, with an estimated $9.5 billion dollars in yearly phone scam revenue, these efforts just are not a real deterrent. RoboKiller isn't a deterrent either, it is a solution.

This week, you gave us the chance to testify for this subcommittee, which will help us to promote our efforts further. Next week, the FTC and FCC are hosting a technology expo where we will again present RoboKiller. Do more of this. Help us get more attention so that we can speed up our growth.

At our current growth rate we will hit 10 million users in June of 2021. At that point telemarketers will have seen a 50% decline in revenues and have no other choice but to move their scams elsewhere.

We are not worried about putting ourselves out of business by solving this problem. We have built a culture of innovation, so when the scammers start ringing doorbells, we will have a solution for that too!

Answer Bots wasted more than 25,000 hours of human telemarketer's time last month. For our hundreds of thousands of users that meant millions of blocked calls and the peace of mind that when their phone rang it wasn't a harassing call from a scammer. For thousands of other Americans who have yet to purchase RoboKiller, that was 25,000 hours where they too were protected from those otherwise engaged telemarketers.

The robocall problem has grown into an epidemic. Today, 2700+ unwanted calls are being made every second in the United States, but it's over. RoboKiller is on the case, and we will solve this problem.

Mr. LATTA. Thank you very much for your testimony today.

And, Mr. Foss, you are recognized for 5 minutes. Thank you.

STATEMENT OF AARON FOSS

Mr. FOSS. Chairman Latta, Ranking Member Pallone, and members of the committee, thank you for giving me the opportunity to appear before you today.

My name is Aaron Foss. I am the founder of Nomorobo and the winner of the FTC Robocall Challenge.

And since launching in 2013, Nomorobo has stopped almost 650 million robocalls from reaching American citizens. And while that number is huge, it is a mere drop in the bucket of this problem. According to our data, approximately 40 percent of all calls on a landline network are unwanted robocalls.

So I am here today to give you a view from the trenches. And let me start off by telling you the good news. The same technology that created this problem, low-cost voice-over-IP service, is now being used to successfully stop it.

In its first year Nomorobo stopped 15 million robocalls from reaching American consumers. That was in the entire first year. And we are now stopping double that amount every single month. Thirty million robocalls a month are being stopped by Nomorobo. And this is much better than the old solution of, "Only answer numbers that you recognize."

And when I first started this crusade carriers believed that FCC regulations prohibited them from blocking robocalls. But since the FCC clarified that those regulations do indeed allow robocall blocking, carriers have been quick to act. Today Nomorobo is supported by most of the major VoIP carriers in the United States and directly integrated with some of the largest.

And mobile technology companies, like Apple and Google, have also done a great job in making their smartphone ecosystems robocall-blocker friendly. They now allow developers to create and distribute robocall-blocking apps to hundreds of millions of users. This wasn't always the case, especially when I started.

And there used to be a lot of fear when it came to stopping robocalls. Many people thought that technology couldn't differentiate between good and bad robocalls. And Nomorobo proved this incorrect. The service is 97 percent effective, and our false positive rate is only one-tenth of 1 percent.

So on the one hand I know that for over 1.6 million Nomorobo users we have solved their robocall problem once and for all. Their phones are now peaceful and quiet. And I wish I could stop my testimony right there and we could end the conversation right now.

Unfortunately, I can't. It is a jungle out there, and the robocallers have started to use more advanced tricks and tactics. We have to continually stay one step ahead of the bad guys. Simple blacklists are no longer as effective in stopping robocalls as they once are.

Last summer we noticed an explosion in neighbor spoofed calls. These are the calls where the robocall caller uses a fake number that looks very similar to the recipient's number. Last summer they used to represent less than 2 percent of all robocalls, but be-

ginning in July of 2017 they represented almost 20 percent of all robocalls. That is a 10x increase.

Now, luckily, technology like Nomorobo can quickly detect and stop new robocalling patterns like neighbor spoofing. And while the carriers are also working on a solution, verifying and certifying caller ID, it is still years away.

Robocallers are flexible and quickly and continually change their tactics. The tools to fight them also have to be flexible and adaptable.

We are at a very interesting point in the robocall battle. Technology has proven that it is the safe and effective solution in the fight. Regulators have cleared the path for carriers to roll out robocall-blocking solutions to their customers. Consumers have shown that they want these services, they trust these services, and are even willing to pay for these services.

And robocall blocking is a virtuous cycle. The more people that use robocall blockers, the less effective robocalling becomes. The less effective robocalling becomes, the less robocalls are made. Everyone wins, except for the robocallers.

And to close, I just want to remind everyone why we are solving this problem. This isn't just about stopping a minor annoyance. Robocalls present a significant threat, particularly to some of our most vulnerable citizens.

I was reminded of this the other day when I received the following email. As everybody knows, my testimony is sworn so I am really not making this up.

It said: "My name is Phil. I just wanted you to know how thankful I am for your service. I have a bad brain injury and the calls I was getting fooled me. Thank you for offering the service for free. My income has been tough to manage, and adding an extra cost, even small, can add up each month."

I thank the committee for continuing to do everything in its power to make robocall-blocking solutions, like Nomorobo, available to all Americans.

[The prepared statement of Mr. Foss follows:]

Aaron Foss
Founder, Nomorobo
Testimony before the
United States House of Representatives Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection
"Do Not Call: Combating Robocalls and Caller ID Spoofing"
April 27, 2018

Chairman Latta, Ranking Member Pallone, and members of the Committee, thank you for giving me the opportunity to appear before you today.

My name is Aaron Foss. I'm the founder of Nomorobo and the winner of the FTC Robocall Challenge. Since launching in 2013, Nomorobo has stopped almost 650 million robocalls from reaching American citizens. And while that number is huge, it's a mere drop in the bucket. According to our data, approximately 40% of all calls on the landline network are unwanted robocalls.

I'm here today to give you a view "from the trenches." Let me start off by telling you the good news.

The same technology that created this problem, low cost voice-over-IP, is now being used to successfully stop it. In its first year, Nomorobo stopped 15 million robocalls from reaching American consumers. We're now stopping more than double that amount - 30 million robocalls - every single month. This is much better than the old solution which was to "only answer numbers that you recognize."

When I first started this crusade, carriers believed that FCC regulations prohibited them from blocking robocalls. But, since the FCC clarified that the regulations do indeed allow robocall blocking, carriers have been quick to act. Today, Nomorobo is supported by most of the major VoIP providers in the US and directly integrated with some of the largest.

Mobile technology companies like Apple and Google have also done a great job in making their smartphone ecosystems robocall blocker friendly. They now allow developers to create and distribute robocall blocking apps to hundreds of millions of users.

There used to be a lot of fear when it came to stopping robocalls. Many people thought that technology couldn't differentiate between good and bad robocalls. Nomorobo proved this incorrect. The service is 97% effective with a false positive rate of only .1%.

So, on the one hand, I know that for over 1.6 million Nomorobo users, we've solved their robocall problem once and for all. Their phones are now peaceful and quiet. And I wish I could stop my testimony right there and we could end the conversation right now.

Unfortunately, I can't.

It's a jungle out there and the robocallers have started to use more advanced tricks and tactics. We have to continually stay one step ahead of the bad guys. Simple blacklists are no longer as effective in stopping robocalls as they once were.

Last summer, we noticed an explosion in "neighbor spoofed" calls. These calls, where the robocaller uses a fake number that looks very similar to the recipient's number, used to represent less than 2% of all robocalls. Beginning in July of 2017, neighbor spoofed calls represented almost 20% of all robocalls. That's a 10x increase.

Luckily, technology like Nomorobo can quickly detect and stop new robocalling patterns like neighbor spoofing. And while the carriers are also working on a solution - verifying and certifying Caller ID – it's still years away. Robocallers are flexible and quickly and continually change their tactics. The tools to fight them also have to be flexible and adaptable.

We're at a very interesting point in the robocall battle.

Technology has proven that it's a safe and effective solution in the fight. Regulators have cleared the path for carriers to roll out robocall blocking solutions to their customers. Consumers have shown that they want these services and are even willing to pay for them.

Robocall blocking is a virtuous cycle. The more people that use robocall blockers, the less effective robocalling becomes. The less effective robocalling becomes, the less robocalls are made. Everyone wins.

To close, I just want to remind everyone why we're solving this problem. This isn't just about stopping a minor annoyance. Robocalls present a significant threat, particularly to some of our most vulnerable citizens. I was reminded of this the other day when I received the following email:

> *"My name is Phil. I just wanted you to know how thankful [I am] for your service. I have a bad brain injury and the calls I was getting fooled me. Thank you for offering the service for free. My income has been tough to manage and adding an extra cost even small can add up each month."*

I thank the committee for continuing to do everything in its power to make robocall blocking solutions like Nomorobo available to all Americans.

Mr. LATTA. Well, thank you for your testimony.

And, Ms. Mahoney, you are recognized for 5 minutes.

STATEMENT OF MAUREEN MAHONEY

Ms. MAHONEY. Chairman Latta, members of the subcommittee, thank you for the opportunity to speak today. I work for Consumers Union, the advocacy division of Consumer Reports.

Since 2015, in response to complaints from thousands of consumers who told us that robocalls were their top consumer complaint, we have conducted our End Robocalls campaign, which calls on the major phone companies to offer to all of their customers free, effective tools to block unwanted robocalls.

Nearly three-quarters of a million people have signed this petition, and they have told us that they are overwhelmed by the harmful, abusive, and irritating robocalls that intrude on their privacy, take their money, and allow scams to enter their homes.

Robocalls have reached epidemic proportions. Since 2006 the number of complaints to the FTC about violations of the Do Not Call list has exploded. And the volume of robocalls is on the rise, as well. Last month, 3 billion robocalls were placed to consumers in the United States.

Unwanted calls undermine the quality of the phone service for which consumers pay dealer. For example, sometimes these robocalling campaigns relentlessly target certain consumers. One consumer told us that she received an estimated 100 calls in a single day, which blocked incoming and outgoing calls for significant periods of time. Others have told us that unwanted incoming robocalls have delayed them from calling a medical professional.

And robocalls cost consumers money. Vulnerable consumers, such as the elderly, may be unduly susceptible to telemarketing pitches for products that they don't want or need. Scam calls like Rachel from Card Services also seek to separate consumers from their money fraudulently.

Consumers with prepaid or limited-minute calling plans may end up paying for robocalls. And often consumers have to pay for call-blocking devices or services, which further push the costs of robocalls onto consumers.

We appreciate the progress that the phone companies, the FCC, and the FTC have made thus far in addressing robocalls. For example, AT&T and T-Mobile have begun to offer free robocall-blocking tools to their customers. In addition, the FCC has approved new rules that give phone companies the leeway to immediately block certain clearly illegally spoofed calls that they see coming through their networks. They have also opened an inquiry into the development of caller ID authentication technology to address call spoofing. And the FTC has initiated a series of contests, as my co-panelists well know, to encourage developers to create and innovate antirobocall technology.

But more action is needed to fully address the robocall problem. The blocking under the FCC's new rules will not reach the vast majority of robocalls. Essential legal protections against robocalls under the Telephone Consumer Protection Act, or the TCPA, remain at risk. And enforcement efforts have not been enough to stop

illegal robocalling. Therefore, we support the following additional reforms.

First, the FCC should require providers to offer technology to identify and block spoofed and unwanted calls. Congress can assist by supporting the ROBOCOP Act, which would direct the FCC to develop rules to implement these technologies.

Second, ensure that consumers have strong legal protections against unwanted calls. The D.C. Circuit Court of Appeals recently struck down portions of the FCC's 2015 rules covering the definition of an autodialer and the safe harbor for robocalls made to re-assigned numbers. The FCC will likely open a proceeding to explore open issues related to the definition of an autodialer, and we urge them to implement rules that maintain important protections against unwanted robocalls so that consumers have a means of controlling or stopping them.

Third, increase protections against unwanted debt collection calls. Congress should pass the HANGUP Act to remove the exemption placed in the TCPA for Federal debt collection robocalls. While the exemption should never have been passed in the first place, we urge the FCC to issue rules to implement the provision to provide clarity and to ensure that consumers have a way to limit and stop these calls.

And finally, empower the FTC to counter illegal calls. Congress should allocate to the FTC greater resources for enforcement and the development of antirobocall technology. It should also remove the common carrier exemption in the FTC Act so that the FTC can directly call on phone service providers to be part of the solution.

Thank you for your attention to this important consumer issue, and I look forward to addressing any questions you have.

[The prepared statement of Ms. Mahoney follows:]

Consumers
Union®

THE ADVOCACY DIVISION OF
CONSUMER REPORTS

Statement of

Maureen Mahoney
Policy Analyst
Consumers Union

Before the

Digital Commerce and Consumer Protection Subcommittee

On

"Do Not Call: Combating Robocalls and Caller ID Spoofing"

April 27, 2018

Chairman Latta, Ranking Member Pallone, and members of the Subcommittee, thank you for the opportunity to speak today. I work for Consumers Union, the advocacy division of Consumer Reports.[1] Since 2015, in response to the complaints of thousands of consumers who cited robocalls—unwanted, autodialed calls—as their top consumer concern, Consumers Union has conducted our End Robocalls campaign, which calls on the major phone companies to offer free, effective tools to all of their customers to block these calls.[2] Nearly three-quarters of a million people have signed our petition to the phone companies to provide these tools. These consumers have told us that they are overwhelmed by the harmful, abusive, and irritating robocalls that intrude on their privacy, take their money, and allow scams to enter their homes.

We appreciate the progress that phone companies, the Federal Communications Commission (FCC), and the Federal Trade Commission (FTC) have made thus far in addressing robocalls. For example, AT&T and T-Mobile have begun to offer free robocall-blocking tools.[3] In addition, the FCC has approved new rules that give phone companies the leeway to immediately block certain categories of clearly illegally spoofed calls in their networks: calls spoofed with an invalid number, calls spoofed with an unallocated or unassigned number, or at the request of the owner of the spoofed number.[4] The FCC has also opened an inquiry into developing technology that can confirm the validity of caller ID information.[5] And the FTC has initiated a series of contests to encourage developers to create and innovate anti-robocall technology.[6]

---

[1] Consumers Union is the advocacy division of Consumer Reports. Consumers Union works for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves, focusing on the areas of telecommunications, health care, food and product safety, energy, and financial services, among others. Consumer Reports is the world's largest independent product-testing organization. Using its more than 60 labs, auto test center, and survey research center, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 8 million subscribers to its magazine, website, and other publications.
[2] Tim Marvin, No More Complaining. Let's End Robocalls! ConsumersUnion.org (Feb. 17, 2015), http://consumersunion.org/campaign-updates/no-more-complaining-lets-end-robocalls/.
[3] AT&T Mobile Security & Call Protect (last visited April 24, 2018), https://www.att.com/features/securityapps.html; T-Mobile, Call Protection Solutions (last visited April 24, 2018), https://explore.t-mobile.com/callprotection.
[4] In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, Report and Order and Further Notice of Proposed Rulemaking, CG Docket No. 17-59 (Rel. Nov. 17, 2017), *available at* https://ecfsapi.fcc.gov/file/111717758568/FCC-17-151A1_Rcd.pdf.
[5] Fed. Commc'ns Comm'n, Call Authentication Trust Anchor, Notice of Inquiry (July 14, 2017) at ¶14, *available at* https://ecfsapi.fcc.gov/file/07141096201120/FCC-17-89A1.pdf. The FCC has also proposed a reassigned number database, to help cut down on the number of "wrong number" robocalls. In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, Second Further Notice of Proposed Rulemaking (March 23, 2018), https://ecfsapi.fcc.gov/file/032399073325/FCC-18-31A1.pdf. It has also announced new enforcement efforts. Fed. Commc'ns Comm'n, Robocall Scammer Faces $120 Million Proposed Fine for Massive Caller ID Spoofing Operation (June 22, 2017), https://apps.fcc.gov/edocs_public/attachmatch/DOC-345470A1.pdf.
[6] *Still Ringing off the Hook: An Update on Efforts to Combat Robocalls, Before the United States Senate Special Comm. on Aging*, 114th Cong. at 13-15 (2017) (testimony of the Federal Trade Commission), https://www.ftc.gov/system/files/documents/public_statements/1256863/p034412_commission_testimony_re_roboc alls_senate_10-4-17.pdf. [hereinafter "Still Ringing Off the Hook"].

But more action is needed to fully address the robocall problem. The blocking under the FCC's new rules will not reach the vast majority of robocalls. For example, it will not address the problem of "neighbor spoofed" calls, in which the caller ID is spoofed with a number in the recipient's own area code and exchange, or other calls that are spoofed with numbers that are in circulation. Moreover, scammers will likely simply stop spoofing numbers that they know are more likely to be blocked. Essential legal protections against robocalls under the Telephone Consumer Protection Act (TCPA) and FCC rules remain under attack and at risk. And enforcement efforts have not been enough to stop illegal robocalling.

We support the following additional reforms:

- **Require anti-spoofing, call-blocking technology**: The FCC should require providers to offer technology to identify and block spoofed and unwanted calls. Unblocking requests should be evaluated by a required set of criteria to ensure that consumers' wishes are honored. Congress can assist by supporting the ROBOCOP Act,[7] which would require the FCC to develop rules implementing this technology.

- **Ensure that consumers have strong legal protections against unwanted robocalls:** The DC Circuit Court of Appeals recently struck down portions of the FCC's 2015 rules, covering the definition of an autodialer and the safe harbor for robocalls made to reassigned numbers. The FCC will likely open a proceeding to explore open issues related to the definition of an autodialer. We urge the FCC to implement strong rules that maintain important protections against unwanted robocalls.[8]

- **Increase protections against unwanted debt collection calls:** Congress should pass the HANGUP Act,[9] to remove the exemption in the Telephone Consumer Protection Act (TCPA) for federal debt collection robocalls, and overturn the FCC's Broadnet ruling that effectively exempts robocalls made by federal contractors.[10] We also urge the FCC to implement strong rules limiting federal debt collection calls.

- **Empower the FTC to counter illegal calls:** Congress should strengthen the FTC's ability to stop abusive robocalling by allocating greater resources for enforcement and the

[7] S. 2705, H.R. 5573 (2018)

[8] *Abusive Robocalls and How We Can Stop Them, Before the Senate Committee on Commerce, Science, and Transportation*, 115th Cong. (2018)(testimony of Margot Freeman Saunders), *available at* https://consumerfed.org/wp-content/uploads/2018/04/testimony-on-problem-of-unwanted-robocalls.pdf [hereinafter Saunders testimony].

[9] S. 564 (2017).

[10] In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Petitions for Declaratory Ruling by Broadnet Teleservices LLC, National Employment Network Association, RTI International, Declaratory Ruling, FCC 16-72, CG Docket No. 02-278 (July 5, 2016), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0706/FCC-16-72A1.pdf.

development of anti-robocall technology. It should also remove the common carrier exemption in the FTC Act so that the FTC can directly call on phone service providers to be part of the solution.

We also generally support the recommendations made by the National Consumer Law Center in their testimony before the Senate Commerce, Science, and Technology Committee on April 18, 2018.[11] Below, I will describe how robocalls continue to plague consumers, and expand on each of the recommendations listed above.

Unwanted robocalls continue to harass consumers.

Robocalls have reached epidemic proportions. Since 2006, the number of complaints about violations of the Do Not Call list has exploded.[12] Consumers filed at least seven million complaints about violations of the Do Not Call list in fiscal year 2017, over twice as many complaints as in 2014.[13] This is reflected in FCC complaint data, in which unwanted calls reliably rank as one of the top consumer complaints.[14]

Not only have complaints to the FTC increased, but the volume of robocalls is on the rise as well. Aaron Foss of Nomorobo estimated in 2015 that over a third of all calls are unwanted robocalls.[15] Last month, three billion robocalls were placed to consumers in the United States— fifteen percent higher than in February 2018, and overall, the highest number since the call-blocking company YouMail began tracking that data in 2015.[16] According to YouMail, as of February 2018, the most common type of robocalls (32%) are payment reminders, followed closely by alerts and other reminders (28%). Another 16% are from telemarketers in general. Roughly a quarter of all robocalls—24%—are scam calls.[17]

Unwanted calls are an assault on consumer privacy, and undermine the quality of the phone service for which consumers pay dearly. For example, sometimes, these robocalling

---

[11] Saunders testimony, *supra* note 8.
[12] *National Do Not Call Registry Data Book FY 2016*, FED. TRADE COMM'N at 4 (Dec. 2016), https://www.ftc.gov/system/files/documents/reports/national-do-not-call-registry-data-book-fiscal-year-2016/dnc_data_book_fy_2016_post.pdf.
[13] *National Do Not Call Registry Data Book FY 2017*, FED. TRADE COMM'N at 6 (Dec. 2017), https://www.ftc.gov/sites/default/files/filefield_paths/dnc_data_book_fy2017.pdf.
[14] Fed. Commc'ns Comm'n, Consumer Complaint Center, Unwanted Calls (last visited April 14, 2018), https://consumercomplaints.fcc.gov/hc/en-us/articles/115002234203-Unwanted-Calls
[15] *Rage Against Robocalls*, CONSUMER REPORTS (July 28, 2015), https://www.consumerreports.org/cro/magazine/2015/07/rage-against-robocalls/index.htm.
[16] *National Robocall Volumes Jump 15% in March to Topple Monthly Records*, YOUMAIL (April 10, 2018), https://www.prnewswire.com/news-releases/national-robocall-volumes-jump-15-in-march-to-topple-monthly-records-300627110.html.
[17] *YouMail Releases Detailed Breakdown of U.S. Robocalls in February*, YOUMAIL (March 21, 2018), https://www.prnewswire.com/news-releases/youmail-releases-detailed-breakdown-of-us-robocalls-in-february-300616969.html.

campaigns relentlessly target certain consumers. One consumer told us that she received an estimated one hundred calls in a single day, which blocked incoming and outgoing calls for significant periods throughout the day. Others have told us that unwanted incoming robocalls have delayed them from calling a medical professional.

Moreover, robocalls cost consumers money. Vulnerable consumers such as the elderly may be unduly susceptible to telemarketing pitches for products that they do not want or need. Scam calls like Rachel from Card Services, in which the caller promises to lower interest rates for a flat fee,[18] or the IRS scam, in which the caller threatens arrest if the recipient does not supply immediate payment for a bogus tax debt,[19] also seek to fraudulently separate consumers from their money. These and other telemarketing scams cost consumers an estimated $350 million in 2011, according to the most recent government data.[20] Robocalls cost consumers in other ways, too. Consumers with prepaid or limited-minute calling plans may end up paying for robocalls. And often, consumers have to pay for call-blocking devices or services, which further push the costs of robocalls onto consumers.

Existing robocall protections are not sufficient.

Enforcement, while important, has been inadequate to address the robocall problem. About a quarter of these calls are coming from scammers, sometimes located overseas, and difficult to track down.[21] These callers intend to commit fraud, and they will completely ignore the Do Not Call registry. They take advantage of low rates for calls on Internet-based platforms, and use autodialers to engage in random and sequential dialing that can send out millions of calls in a short amount of time.[22] They also engage in call spoofing, in which they input misleading information in the Caller ID, to circumvent blocks and trick consumers into picking up the phone, further challenging enforcement efforts.[23] The financial incentives for calling are so great that as soon as one robocall scam outfit is shut down, others quickly pop up in their place.

Enforcement has also been insufficient to protect against unwanted robocalls from otherwise legitimate actors. While the TCPA's private right of action serves as an important

---

[18] Andrew Johnson, *The FTC Gets Rachel the Robocaller...Again*, FED. TRADE COMM'N (June 14, 2016), https://www.consumer.ftc.gov/blog/2016/06/ftc-gets-rachel-robocaller-again.
[19] Amy Hebert, *Scammers Continuing to Pose as IRS Agents*, FED. TRADE COMM'N (May 29, 2014), https://www.consumer.ftc.gov/blog/2014/05/scammers-continuing-pose-irs-agents.
[20] Keith B. Anderson, Staff Report of the Bureau of Economics, Fed. Trade Comm'n, *Consumer Fraud in the United States, 2011: The Third FTC Survey* (April 2013), https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey_0.pdf. There were an estimated 3.5 million telemarketing fraud cases in 2011 (p. 38). The median loss per case was $100 (p. 39). Therefore, an estimated $350 million was lost to telemarketing fraud in 2011.
[21] Still Ringing off the Hook, *supra* note 6, at 7. For a description of the different categories of robocalls received by consumers, see YouMail, *supra* note 17.
[22] *Id.* at 11-12.
[23] *Id.* at 8.

deterrent to unwanted calls,[24] and the FTC, for example, has properly engaged in major enforcement actions against companies such as Dish Network for illegal robocalls made by their contractors to consumers on the Do Not Call registry,[25] many consumers still receive unwanted calls, potentially in violation of the law. For example, national consumer groups have called on the FCC to take action against Navient for debt collection robocalls made without consumers' consent.[26]

Consumers also need tools to protect themselves from calls that may be legal but are nonetheless unwanted. Most non-emergency autodialed calls to cell phones are illegal, unless the caller has the consumer's consent.[27] However, exemptions threaten to chip away at these protections. For example, an exemption was slipped into the Budget Act of 2015 for debt collection calls made on behalf of the federal government, which could lead to more unwanted calls to cell phones, even to consumers who do not owe any debt.[28] And consumers do not have as many legal protections for their home phones, even if the consumer is on the Do Not Call registry. For example, political, charity, and debt collection calls are exempt from the Do Not Call list,[29] and are legal to home phones even without the consumer's consent as long as the call does not feature a pre-recorded message.[30]

Providers must be required to offer anti-spoofing and call-blocking technology.

Consumers need effective relief from this onslaught of robocalling. Several phone companies have begun to offer call-blocking tools to at least some of their customers, but most consumers still lack access to these tools. Traditional landline users, in particular, lack effective options to block unwanted robocalls. Furthermore, caller ID spoofing poses a challenge to blacklist-based call-blocking. The FCC should require companies to move quickly to provide technology that identifies and blocks spoofed and unwanted calls.

Robocall-blocking technology can be offered immediately to serve as an important line of defense against unwanted calls. Advanced call-blocking technology has been available for years. It has been offered in Canada, for both traditional landline and Voice over Internet Protocol

---

[24] 47 U.S.C. § 227(a)(3).
[25] *FTC and DOJ Case Results in Historic Decision Awarding $280 Million in Civil Penalties Against Dish Network and Strong Injunctive Relief for Do Not Call Violations*, FED. TRADE COMM'N (Jun. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/06/ftc-doj-case-results-historic-decision-awarding-280-million-civil.
[26] Letter from National Consumer Law Center et al. to Michael Carowitz, Chief of the Enforcement Bureau, FCC (June 12, 2017), https://www.nclc.org/images/pdf/robocalls/enforcement-letter-tcpa-fcc.pdf. [hereinafter NCLC Letter]
[27] 47 U.S.C. § 227(b)(1)(A)(iii).
[28] Bipartisan Budget Act of 2015, Pub. L. No. 114-74, 129 Stat. 588 [hereinafter "Budget Act"].
[29] *National Do Not Call Registry*, FED. TRADE COMM'N (March 2015), https://www.consumer.ftc.gov/articles/0108-national-do-not-call-registry.
[30] 47 U.S.C. § 227 (b)(1)(B).

(VoIP) phones, since 2007, for free.[31] The Canadian technology is said to be adaptable to United States networks.[32] Another call-blocking technology became widely available as a third-party service for VoIP phones in the U.S. in 2013.[33] And app technology has proliferated. Robocall-blocking apps had long been available for Android phones, and an iOS update in 2015 allowed third-party apps to block calls on iPhones.[34] These technologies typically use information reported to them by consumers and other sources to block calls identified as spam or scam calls.[35]

Consumers Union has long called for the phone companies to provide free robocall-blocking tools to consumers, bolstered by an FCC decision in July 2015 that clarified that phone companies can offer optional, advanced robocall-blocking tools to their customers without violating their responsibilities to connect calls placed to them.[36] Progress accelerated in 2016, when then-FCC Chairman Wheeler called on the top phone companies and gateway providers to offer robocall-blocking tools to consumers and to move forward with caller ID authentication technology to address spoofing.[37] In response, the major phone companies joined the Robocall Strike Force, the industry-led group conducted under the auspices of the FCC, which worked toward those goals, as well as consumer education and a traceback initiative to more easily track down robocalls through multiple carriers to their sources.[38]

Still, most consumers still do not have effective robocall-blocking tools. The FCC should require the phone companies to offer robocall-blocking technology to all of their customers. AT&T and T-Mobile began offering free robocall-blocking tools to at least some of their customers, and Verizon and Sprint have rolled out paid products for smartphones.[39] But

---

[31] *Robocalls: All the Rage, An FTC Summit*, FED. TRADE COMM'N at 219 (Oct. 18, 2012), https://www.ftc.gov/sites/default/files/documents/public_events/robocalls-all-rageftcsummit/robocallsummittranscript.pdf.

[32] Brad Fisher, Senior Vice President of Marketing and Product, Primus Canada, cited in Maureen Mahoney, *Dialing Back: How Phone Companies Can End Unwanted Robocalls*, CONSUMERS UNION at 7 (Nov. 2015), http://consumersunion.org/wp-content/uploads/2015/02/Dialing-Back-Complete-Report-11.16.2015.pdf. [hereinafter "Dialing Back"].

[33] Still Ringing Off the Hook, *supra* note 6, at 13.

[34] Glenn Fleischman, *New Call-Blocking Apps in iOS 10 Can Stop Spammers and Scammers Before They Reach You*, MACWORLD (Sept. 16, 2016), https://www.macworld.com/article/3119736/ios/new-call-blocking-apps-in-ios-10-can-stop-spams-and-scams-before-they-reach-you.html.

[35] Dialing Back, *supra* note 32, at 6.

[36] In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act, Declaratory Ruling and Order, CG Docket No. 02-278, at ¶154 (Rel. July 10, 2015), https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-72A1.pdf [hereinafter Declaratory Ruling and Order].

[37] Tom Wheeler, *Cutting Off Robocalls*, FCC Blog (July 22, 2016), https://www.fcc.gov/news-events/blog/2016/07/22/cutting-robocalls.

[38] Robocall Strike Force Report at 2 (Oct. 26, 2016), https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf.

[39] Industry Robocall Strike Force Report at 17-18 (April 28, 2017), https://www.ustelecom.org/sites/default/files/documents/Ex%20Parte-Strike-Force-Report-2017-04-28-FINAL.pdf.

traditional landline users, in particular, have few options for blocking unwanted calls, and options for them can be pricey.[40]

The FCC should also require the phone companies to implement technology that can verify the accuracy of the Caller ID information, by a date certain. This is important because caller ID spoofing poses challenges to blacklist-based call blocking. Callers often cycle through different spoofed numbers in a short amount of time, making it difficult to stay one step ahead of the robocallers.[41] We are not prescriptive about the technology that should be implemented, but it is important that it be able to protect all consumers, be able to block unwanted spoofed calls, offer protection against calls originating from overseas, and be provided at no extra charge.[42] In addition, we recognize that there are legitimate reasons for masking the caller's identity in some circumstances. This technology should not prevent the blocking of caller ID information as allowed under the Communications Act[43] and FCC regulations.[44] Finally, the deadline for implementing this technology should take into account the different financial circumstances of the phone service providers, while expediting implementation as feasible.

As these comprehensive blocking mechanisms are implemented, certain wanted calls may be blocked. Our goal is to ensure that consumers receive the calls they want, while having the ability to protect themselves from the calls they don't. Thus, the FCC should establish a system to manage the unblocking of legitimate calls. It should be guided by a set of principles to ensure that the consumer's wishes are not disregarded. The unblocked calls should be legal; the caller ID information should be verified; and calls blocked by optional call-blocking systems should not be unblocked without the consent of the called party. Finally, to ensure that the costs of implementing this system are not passed along to be borne by consumers, the system should be paid for by those in the calling industry who seek to benefit from it.[45]

Ensure that consumers have strong legal protections against unwanted calls.

We urge the FCC to ensure that the legal protections that currently exist in the Telephone Consumer Protection Act against unwanted calls remain robust. Even with the best robocall-blocking tools, consumers cannot effectively control unwanted calls without privately

---

[40] *Robocall-Blocker Review*, CONSUMER REPORTS (Aug. 14, 2015), https://www.consumerreports.org/cro/magazine/2015/07/robocall-blocker-review/index.htm [hereinafter "Robocall Blocker Review"].
[41] Nomorobo, Background Updates (last visited April 24, 2018), https://nomorobo.zendesk.com/hc/enus/articles/115001498406-Background-Updates.
[42] See, Comments of Consumers Union et al, WC Docket No. 17-97 (August 11, 2017), *available at* http://consumersunion.org/wp-content/uploads/2017/08/Robocalls-FCC-NOI-on-caller-ID-authentication-CUcomments-final.pdf.
[43] 47 U.S.C. § 227(e)(3)(B).
[44] 47 C.F.R. §64.1604(b)
[45] *See*, Comments of Consumers Union, National Consumer Law Center, et al., CG Docket No. 17-59 (Jan. 23, 2018), https://ecfsapi.fcc.gov/file/10124133525388/Consumer%20group%20comments%20FNPRM%201.23.18.pdf

enforceable legal rights. The Court of Appeals for the DC Circuit recently vacated portions of the FCC's 2015 Declaratory Ruling and Order on robocalls.[46] Specifically, the court rejected the FCC's definition of an autodialer, a key element in TCPA for controlling unwanted, automated calls. Under the TCPA, most calls made with an autodialer to a cell phone can only be made with consent. Second, the Court rejected the FCC's rule that established a safe harbor limited to one robocall made to a reassigned number. Finally, the Court upheld the FCC's rule that a consumer may revoke consent to receive robocalls in any reasonable manner.

The FCC will likely open a proceeding to address open questions of how to define an autodialer. The courts have repeatedly found that automated calls from call centers meet the statutory definition under the TCPA, and thus require consent to be placed to cell phones.[47] We are hopeful that the FCC will recognize that the statute has ample room to cover most existing automated dialers, and thus will protect consumers from unwanted calls. If, instead, the FCC narrowly defines autodialer, many telemarketing scam calls and unwanted calls from debt collectors will not be covered by the TCPA, leaving consumers without the means of controlling or stopping these calls.

We call on the FCC to issue rules that 1) maintain a comprehensive definition of an autodialer, so that all automated calls are included, but that exempt equipment that is not typically used to engage in mass calling, such as the personal use of a smartphone; 2) create the reassigned number database as they have proposed,[48] which callers can use to ensure they are contacting consumers who have provided their consent, allowing a safe harbor only for calls made due to errors in the database; and 3) ensure that consumers may revoke consent to receive automated messages, so consumers know exactly how to request that the calls stop.[49]

Increase protections against unwanted debt collection calls.

Debt collectors remain a top source of unwanted automated messages. According to YouMail, 16 of the top 20 robocallers in March 2018 were payment reminders and debt collectors.[50] Consumers often tell us that they receive debt collection robocalls that are intended for someone else, but the callers ignore the pleas to stop calling. Despite these concerns, the Budget Act of 2015 exempted from the TCPA robocalls made for the purpose of collecting

---

[46] *ACA International v. FCC*, 885 F.3d 687 (D.C. Cir. 2018).
[47] *The Effect of ACA International: What Does it Vacate, What Does it Undermine, What Rules Remain?* NATIONAL CONSUMER LAW CENTER 13-15 (April 2, 2018), https://www.nclc.org/images/pdf/robocalls/memo-effect-of-aca-international.pdf.
[48] In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17-59 (April 23, 2018), *available at* https://www.federalregister.gov/documents/2018/04/23/2018-08376/advanced-methods-to-target-and-eliminate-unlawful-robocalls.
[49] Saunders testimony, *supra* note 8, at 17-18.
[50] *National Robocall Volumes Jump 15% in March to Topple Monthly Records*, YOUMAIL, (April 10, 2018), https://www.prnewswire.com/news-releases/national-robocall-volumes-jump-15-in-march-to-topple-monthly-records-300627110.html.

federal debt, such as student loan debt or tax debt.[51] This provision could lead to millions more robocalls not only to consumers, but to their relatives, references, and employers.

We support the HANGUP Act, which not only removes the debt collection provision from the TCPA, but reverses a decision made by the FCC that we are concerned effectively exempts federal contractors from the TCPA as well.[52] The HANGUP Act has garnered bipartisan support, and over 80,000 Consumers Union activists contacted their representatives in Congress to support it when it was first introduced in 2015. We urge Congress to pass it as soon as possible.

In the meantime, rules implementing the Budget Act provision have yet to go into effect. The Budget Act directed the FCC to issue rules to implement the provision.[53] The FCC finalized rules that put strict limits on the debt collection robocalls, limiting them to three per month without the consumer's prior consent, in August 2016.[54] However, those rules have yet to be implemented, as the FCC withdrew them from the OMB in January 2017.

The exception to the TCPA does not go into effect until rules have been issued to implement it, yet Navient has robocalled consumers even after they have asked for the calls to stop.[55] In defense against resulting TCPA suits, Navient has argued that the Budget Act exempts these calls.[56] Though the Budget Act exemption never should have been passed in the first place, it is important that the implementing rules be finalized now so that the guidelines will be clear and consumers will have some protection regarding debt collection robocalls made on behalf of the federal government.

Empower the FTC to counter robocallers.

The Federal Trade Commission has taken a number of steps to address the illegal robocall problem, beginning with its implementation of the Do Not Call Registry in 2003, which has helped consumers to control telemarketing calls from legitimate telemarketers.[57] However, the FTC has faced challenges in effectively enforcing the Do Not Call registry, collecting only about 12% of the civil penalties and equitable relief it has ordered for robocall and Do Not Call violations.[58] Indeed, enforcement efforts have proven inadequate to the problem of robocalls. We

---

[51] Budget Act, *supra* note 28.
[52] S. 564, Congress.gov, (last visited April 15, 2018), https://www.congress.gov/bill/115th-congress/senate-bill/564/cosponsors,
[53] Budget Act, *supra* note 28, § 301(b)
[54] In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02-278, Report and Order, FCC 16-99, (Rel. Aug. 11, 2016) available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-99A1.pdf.
[55] NCLC letter, *supra* note 26, at 12-13.
[56] *Id.*
[57] Still Ringing Off the Hook, *supra* note 6, at 1-2.
[58] "FTC DNC and Robocall Enforcement," (April 3, 2018), provided to the author by Mitchell Katz of the FTC.

recommend that the FTC be given additional funding to pursue cases against more robocallers and to be able to effectively bring them to justice.

In addition, Congress should earmark additional funds for the FTC to further develop anti-robocall technology. The FTC has played an important role in the development of these tools. It created a series of contests in order to spur development of technology to automatically identify and block robocalls.[59] Most notably, Nomorobo was selected the winner of the first contest, and it was made available for consumers to use beginning in 2013.[60] Volunteer testers for Consumer Reports gave Nomorobo's home phone service high marks for its ability to block unwanted calls.[61] The FTC should continue to push to develop robocall-blocking technology, particularly for traditional landline phones, where market incentives may be less compelling for phone companies.

Finally, the FTC currently lacks authority over phone companies that could help ensure that the consumer protection agency uses its expertise and enforcement strength to push the phone service providers to address this issue. This is one more reason why Congress should remove the common carrier exemption in the FTC Act.

Conclusion

There is a long way to go in the fight against robocalls. Consumers Union will continue urging phone companies, the FCC, and Congress to take action on this issue, while also providing consumers with information on steps that they can take to protect themselves.[62] We thank you for your interest in helping to protect consumers from these relentless unwanted calls. I look forward to addressing any questions you may have.

---

[59] Still Ringing Off the Hook, *supra* note 6, at 13-15.
[60] *Id.* at 13.
[61] Robocall-Blocker Review, *supra* note 40.
[62] *See*, e.g., Anthony Giorgianni, *The Newest Ways to Deal with Robocalls*, Consumer Reports (Nov. 13, 2017), https://www.consumerreports.org/robocalls/how-to-deal-with-robocalls/.

Mr. LATTA. Thank you.

And, Mr. Hambuchen, you are recognized for 5 minutes.

STATEMENT OF SCOTT HAMBUCHEN

Mr. HAMBUCHEN. Chairman Latta, members of the subcommittee, thank you for giving me the opportunity to appear today. I am Scott Hambuchen, an executive with First Orion Corporation.

Today consumers are being scammed out of hundreds of millions of dollars and are now conditioned to not answer the phone unless they know who is calling. This lack of trust in the voice channel must change.

First Orion partners with carriers to offer their subscribers protection from scams and unwanted calls. First Orion also offers consumers mobile apps, such as PrivacyStar, to protect their cell phones from these calls. These offerings use sophisticated analytics to identify calls that are highly likely to be scams.

First Orion analyzed over 34 billion calls this past year and labeled 3.5 billion of them Scam Likely, giving consumers a warning before they answer. In addition, consumers can opt in to blocking calls labeled Scam Likely so their phone never rings. In 2017 we blocked over 500 million of these calls for consumers.

Most of the larger carriers have launched some form of scam protection. First Orion is the chosen provider for T-Mobile's groundbreaking offering last year, deploying our Scam Likely solution to over 58 million subscribers for free. We also know there are over 500 apps in the Google Play and Apple App Stores that are free or available for a small month monthly charge.

Despite these efforts, we are still getting fraudulent and unwanted calls. The fraudsters are sophisticated, evolving their practices to avoid being labeled and blocked. They operate like a business and constantly change their tactics to appear legitimate.

Scammers use methods that legitimate callers often use, such as prerecorded messages, automated robocalls, and altering their caller ID, commonly referred to as spoofing.

Some robocalls are legitimate and wanted, such as automated notices from your child's school. And yet some scams are not robocalls. Both are still growing.

Spoofing is no different. Legal spoofing by a national pharmacy chain letting customers know their prescription is ready and spoofing the number for the local pharmacy is helpful. However, neighbor spoofing, inserting a random number with the same area code and prefix as the called number to get a consumer to answer a scam call, is illegal and much harder to detect.

Let me be clear. We are in an arms race, not a marathon with a finish line, at least until we make it unprofitable. Our approach provides consumers the best information available—who is calling and why—allowing consumers to decide if they should answer.

We also allow consumers to block future calls from that number or call category. We offer more information, including a calling number, the company name if available, the call category, and the ability to file complaints that we send to the FTC.

We take great care in applying labels using sophisticated algorithms based on calls we see, input from consumers, and many

36

other sources of intelligence. No one piece of data ever generates a Scam Likely label.

Our labeling methods are constantly evolving to respond to new threats. In response to neighbor spoofing, we have evolved our analytics to soon start identifying individual calls, not just the calling number, as Scam Likely. As a result, we expect the number of identified scam calls to rise from 12 percent today to 15 percent.

Of course, any algorithmic approach has some errors. Reported cases of false positives are a fraction of 1 percent for us. So calling parties can easily fix an incorrect label, we launched CallTransparency.com, a website that provides legitimate callers the opportunity to register their numbers and avoid the Scam Likely tag.

The FCC has wisely established a light touch regulatory regime that allows continued development of call labeling and blocking solutions, with the potential for profound consumer benefits. We also commend the multiyear FTC focus on these issues and their role with complex multiagency enforcement actions.

Finally, we will continue working with call originators to further enhance our solutions, although we do oppose any regulation or industry efforts that may help scammers, such as call block indicator tones.

To conclude, the one area where First Orion believes that industry and government can do more together is expanding consumer education about scam calls and what tools are available to them.

Mr. Chairman, First Orion appreciates the opportunity to appear today. We are available to provide any additional information the committee may request. Thank you.

[The prepared statement of Mr. Hambuchen follows:]

WRITTEN TESTIMONY OF

FIRST ORION
TRANSPARENCY IN COMMUNICATION

SCOTT HAMBUCHEN

EXECUTIVE VICE PRESIDENT, TECHNOLOGY SOLUTION AND DEVELOPMENT

FIRST ORION CORP.

BEFORE THE

CONGRESS OF THE UNITED STATES

HOUSE OF REPRESENTATIVES

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER PROTECTION

Title of Hearing

DO NOT CALL: COMBATTING ROBOCALLS AND CALLER ID SPOOFING

APRIL 27, 2018

Executive Summary

Consumers are being scammed out of hundreds of millions of dollars a year and are now conditioned to not answer the phone unless they know who's calling. They want to be able to trust their phones again and are demanding help.

To that end, First Orion offers protection from scam and unwanted calls. In addition to mobile applications, we work with T-Mobile USA, deploying Scam ID to over 58 million subscribers (free service) and giving them optional call blocking services. Out of over 34 billion calls we analyzed this past year, we identified over 3.5 billion, or about 12%, as scams. In addition, at the request of the consumer, we blocked over 500 million of these calls.

Despite our efforts and those of other key industry stakeholders, scam calls in particular are still a big problem. The fraudsters are very sophisticated, evolving their practices to avoid being labeled or blocked. As a result, we are in an arms race, not a marathon with a finish line, and will be in it until we make it un-profitable.

We provide consumers the best information available about who is calling and why and allow them to decide whether to answer. Consumers can make the decision to block all future calls from particular numbers or call categories.

Reported cases of false positives are a fraction of 1% and calling parties can easily fix an incorrect label.

First Orion applauds consumer education and enforcement efforts but also believes more can be done by industry and government together.

Introduction

Due to advances in calling technology, it is now cheap and easy for legitimate companies and scammers alike to make billions of automated calls known as robocalls. As a result of the sheer volume of scam and unwanted calls, consumers are being swindled out of hundreds of millions of dollars every year and are being conditioned to not answer the phone unless they know exactly who is calling them, and it is increasingly difficult to know. They are frustrated that they can no longer trust their phones. We must better protect consumers, but this utter lack of trust in the voice channel must also change for us all to reap the benefits of a properly functioning voice communications system. Indeed, carriers and consumers aren't the only victims of the vast increase in scams. Legitimate call originators (companies that make outbound calls for themselves or as a service) who "play by the rules" have also been hurt by consumer distrust of any call they don't specifically recognize.

Overview of First Orion

First Orion offers consumers, carriers and call originators a holistic approach to addressing the problems of illegal and unwanted calls. While maintaining a focus on ensuring that legal, wanted calls get delivered and answered, First Orion protects consumers from illegal, fraudulent, and unwanted phone calls to their home, office, and cell phones with our PrivacyStar mobile applications and our First Orion Network Enterprise Solution ("FONES") for carriers.

First Orion is headquartered in Little Rock, Arkansas with offices in Seattle, Washington and London, United Kingdom.

We are proud to have been chosen last year by T-Mobile USA, Inc. ("T-Mobile") to support its groundbreaking Scam ID and Scam Block service, which now protects over 58 million T-Mobile subscribers (free to the consumer). By default, all of these subscribers receive Scam ID, which displays the label "Scam Likely" as part of the caller ID screen for calls we determine are fraudulent in nature. With the Scam Block service, subscribers can also sign up to block calls that are labeled "Scam Likely" (or calls from specific numbers) from ever ringing through to their cell phones.

We offer similar services to protect millions of consumers who have our PrivacyStar and carrier-branded mobile applications installed on their phones. We focus on offering similar functionality for home and office phones as well.

For over 7 years, First Orion has provided complaint data in an automated solution to the Federal Trade Commission ("FTC"). In fact, First Orion subscribers have historically provided as much as 30% of the fraud related complaints compiled by the FTC in its Consumer Sentinel Network.

Background on the "Robocall and Spoofing" Problem

Communications habits have changed drastically with the advent of smart phones and digital communication, but an overarching problem is that consumers have simply become conditioned to NOT answer their voice calls —whether to their landlines or their cell phones. When we get a call from an Unknown Caller or 800 number our everyday experience illustrates

that we just don't answer because, as we all know, many of those Unknown and 800 calls represent the unwanted and illegal calls that are the focus of this hearing.

However, the answer to restoring confidence and transparency in the voice channel can't be simply blocking all robocalls and all spoofed calls. This is because not all robocalls and not all spoofing is bad, and not all scammers use robocalling and spoofing (even though many do).

Robocalls can generally be separated into one of three categories:

1. Illegal: This includes scams, but it also includes calls that may not be designed to defraud a consumer but that violate one or more of the telecommunications laws designed to protect consumers from unwarranted intrusions on their privacy.[1] These calls are also unwanted calls from the consumer's perspective.

2. Legal but Unwanted: These calls are not scams and are basically in compliance with laws and regulations, but the practices of the calling party are offensive or harassing to many consumers.

3. Wanted: These are calls that the consumer wants or needs, such as automated calls from his or her pharmacy or child's school.

---

[1] At the Federal level, the primary relevant laws are the Telephone Consumer Protection Act, 47 U.S.C. § 227 (as amended by the Truth in Caller ID Act of 2009) and the relevant implementing regulations from the FCC, 47 C.F.R. § 64.1200-1202; the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. § 6101 et seq. and the relevant implementing regulations from the FTC, 16 C.F.R. § 310 (commonly known as the Telemarketing Sales Rule); and the Fair Debt Collection Practices Act, 15 U.S.C. § 1692 et seq. Many states also provide additional restrictions on telemarketing calls.

And there are a lot of them. According to one index, over 3 billion robocalls were made to US consumers in March 2018.[2]

While unwanted robocalls are annoying and contribute greatly to the lack of confidence in the ecosystem, scam-related calls are particularly pernicious. There are no official numbers on how many robocalls are fraudulent, but official reports on even just a slice of data show the problem is large. In 2017, the FTC received approximately 348,000 "imposter scam" reports, resulting in reported losses of $328 million to imposter scams alone.[3] Imposter scams include, for example, "people falsely claiming to be with the government, a relative in distress, a well-known business, or a technical support expert, to get a consumer's money," but omit many other types of scams, such as traditional calls offering consumers "not to be missed" business or investment opportunities.[4] Additionally, numbers based on consumers reporting scams to law enforcement don't reflect the actual number because, logically, only a fraction of the actual scams committed are reported.

Our own data suggest the problem is much larger. In the last year, First Orion has analyzed over 34 billion calls with over 3.5 billion (approximately 12%) of those calls being identified as scams. At the request of the consumer, First Orion blocked over 500 million of these scam calls.

The practice of "spoofing" amplifies the impact of unwanted and illegal robocalls. Spoofing is the practice of replacing the CallerID field with a number that is different from the actual calling

---

[2] *Robocall Index*, YouMail, https://www.youmail.com/phone-lookup/robocall-index/2018/March (last visited Apr. 24, 2018).

[3] FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK 2017 (2018).

[4] *Id.*

number.[5] Scammers frequently illegally spoof with the caller ID information from a trusted

party (such as the IRS[6]) or a randomly generated number with the same area code and prefix in

an effort to get the called party to think it is a neighbor and answer (commonly referred to as

"neighbor spoofing" or "neighborhood spoofing").[7] Neighbor spoofing in particular has grown

significantly in the past year.[8] It makes determining what is a wanted call versus an unwanted

call more complicated because they both use the same phone number or a very close match to

the called party's phone number.

However, like with robocalling, not all spoofing is illegal or harmful.[9] For example, a national

pharmacy chain letting the consumer know his or her prescription is ready for pickup from the

local pharmacy may spoof the actual number for the pharmacy where the pickup will occur.

This type of spoofing is legal and helpful.

Efforts to Fix the Problem

The Federal Communications Commission ("FCC") and key industry players jumpstarted the

effort to control unwanted and illegal robocalls when they formed the Robocall Strike Force in

July 2016.[10] Since then, the telecommunications industry has progressed in mitigating the

---

[5] *Consumer & Governmental Affairs Bureau Clarification on Blocking Unwanted Robocalls*, 31 FCC Rcd. 10961 (2016).

[6] *See id.*

[7] FCC, *Consumer Alert: Protect Yourself Against 'Neighbor Spoofing', Scam Callers Placing Phone Calls That Appear to Be Local*, https://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0308/DOC-349632A1.pdf (rel. Mar. 8, 2018).

[8] *Id.*

[9] *Call Authentication Trust Anchor*, 32 FCC Rcd. 5988 (2017).

[10] *FCC to Host First Meeting of Industry-Led Robocall Strike Force*, Public Notice, DA 16-917 (rel. Aug. 12, 2016).

threats of many unwanted and dangerous calls. Industry organizations such as the USTelecom

Association and CTIA actively organize and participate with industry working groups focused on

solutions and best practices.[11] Most of the largest carriers have put some form of scam

protection in place within the last year or so, although their exact form varies from carrier to

carrier.[12] Also, there are reportedly over 500 call blocking or labeling mobile applications

available to consumers that offer various types of call protection, up from approximately 85 in

2016.[13] Some of these are free or have basic features for free, while others are available at a

cost ranging from $.99 to $3.99 per month.[14]

As it relates to spoofing, the industry has converged around an industry standard commonly

referred to as STIR/SHAKEN.[15] This system uses "certificate tokens," which one carrier sends to

another during call transmission, to help identify illegally spoofed calls. While STIR/SHAKEN will

advance the fight against illegal spoofing, even relatively unsophisticated scammers will, in

---

[11] *See* Comments of The USTelecom Association, CG Docket No. 17-59 (filed January 23, 2018) discussing industry efforts to address issues such as false positives and the Industry Traceback Group as examples. Comments of CTIA, CG Docket 17-59 (filed January 23, 2018) discussing examples of industry collaboration.

[12] A description of many such efforts can be found in Strike Force documents. Industry Robocall Strike Force Report, *attached to* Letter from Brian Scarpelli, ACT/The App Association, Thomas Goode, ATIS, Krista Witanowski, CTIA, and Kevin Rupy, USTelecom, to Marlene H. Dortch, FCC, CG Docket No. 17-59 (filed Apr. 28, 2017).

[13] Comment by Krista Witanowski, Assistant Vice President, CTIA, March 23, 2018 FCC-FTC Joint Policy Forum, Fighting the Scourge of Robocalls, March 23, 2018, *available at* https://www.fcc.gov/fcc-ftc-robocalls-forum at 135:30-45.

[14] *See How to Stop Robocalls*, CTIA, https://www.ctia.org/consumer-resources/how-to-stop-robocalls (last visited Apr. 19, 2018).

[15] FCC, Robocall Strike Force Report (2016), https://transition.fcc.gov/cgb/ Robocall-Strike-Force-Final-Report.pdf.

many cases, have ways to circumvent the detection. Moreover, STIR/SHAKEN adoption and implementation is just beginning, and until all carriers (originators and terminators) implement the technology, its benefits are limited.

The FCC also recently began allowing providers to block calls without requiring consumer consent when the blocking will prevent almost-certainly-illegal calls from ever being completed.[16] Provider-initiated call blocking is another important tool for preventing harms associated with unwanted and illegal calls; it complements other tools currently available to consumers, such as the subscriber-initiated call blocking services discussed herein. However, this type of provider-initiated blocking will unfortunately not affect many calls since the scammers have exhibited sophistication to rapidly change and adapt to new rules allowing provider-initiated call blocking.

Starting in 2013, even before the formation of the Robocall Strike Force, the FTC focused attention on the issue with its "Robocall Challenges," designed to incentivize innovation in the effort to curb the growing problem.[17] The FTC has continued to play a pivotal role with consumer education, information sharing, and enforcement actions. Bringing such actions has stopped billions of robocalls and imposed hundreds of millions of dollars in penalties. However, due to the complexities of scams, enforcement is equally complex, frequently involving multiple agencies such as the FCC, the Department of Justice, the Internal Revenue Service, the U.S.

---

[16] *Advanced Methods to Target & Eliminate Unlawful Robocalls*, 32 FCC Rcd. 9706, ¶¶ 9-56 (2017).

[17] Press Release, Fed. Trade Comm'n, FTC Announces Robocall Challenge Winners (Apr. 2, 2013), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-announces-robocall-challenge-winners.

Treasury Inspector General for Tax Administration, the U.S. Postal Inspection Service, and state
and foreign country agencies. We particularly applaud these enforcement efforts and
emphasize the growing need for continued focus on enforcement.

Despite all these efforts, we all are still getting too many fraudulent calls. The fraudsters can be
very sophisticated both technologically and organizationally[18] and are evolving their practices
to avoid being labeled or blocked. Some fraudsters run their operations like legitimate calling
businesses and are constantly changing their tactics to look like they are legitimate and to get
consumers to answer their calls, especially when answer rates drop. To address the problem
on an ongoing basis, solution providers will need to identify and adapt to scammers' ever-
changing tactics, until we make scam robocalling so difficult to do that it is no longer profitable
for the scammers. The best parallel in today's technology-driven world is the issue of

---

[18] One notable recent case involved a "complex scheme in which individuals from call centers
located in Ahmedabad, India, impersonated officials from the IRS and U.S. Citizenship and
Immigration Services (USCIS), and engaged in other telephone call scams, in a ruse designed to
defraud victims located throughout the United States. Using information obtained from data
brokers and other sources, call center operators targeted U.S victims who were threatened
with arrest, imprisonment, fines or deportation if they did not pay alleged monies owed to the
government. Victims who agreed to pay the scammers were instructed how to provide
payment, including by purchasing general purpose reloadable (GPR) cards or wiring money.
Upon payment, the call centers would immediately turn to a network of "runners" based in the
United States to liquidate and launder the fraudulently obtained funds." Guilty pleas have been
secured for all 24 U.S. defendants charged in the case. Press Release, Dep't of Justice, Last
Defendant in the United States Pleads Guilty in Multimillion Dollar India-Based Call Center Scam
Targeting U.S. Victims (Nov. 13, 2017), https://www.justice.gov/opa/pr/last-defendant-united-
states-pleads-guilty-multimillion-dollar-india-based-call-center-scam.

sophisticated hackers and the need for constantly updated virus protection systems to keep up with them. Put differently, we are in an arms race, not a marathon with a finish line.

The problem is further complicated by the fact that fraudsters and legitimate calling parties alike use robocalling and spoofing—and that while most scams are robocalls, some are not. So we need to make sure the "arms" we develop in this race are more akin to precision-guided missiles than to powerful but indiscriminate bombs—and that any "shields" we give to legitimate call originators can't also be used by scammers.[19] First Orion is working hard toward that end.

First Orion Solutions

First Orion's scam solutions label suspected fraudulent calls as "Scam Likely," and potentially unwanted, abusive, or harassing calls as "Nuisance Likely," "Telemarketer," "Survey," or other categories as appropriate. Consumers can choose to block individual calling numbers or to block whole categories of calls, such as "Scam Likely" or "Survey."

First Orion's overwhelming customer satisfaction validates this approach. This solution also maximizes transparency for the called party, and helps isolate labeling errors, both "false

---

[19] Certain obvious suggestions for mitigating the impacts of call labeling and blocking on legitimate calling simultaneously benefit the call originators and the scammers. Call originators for example are asking providers to generate a type of "indicator tone" when calls are blocked. Unfortunately, such a tone would immediately alert the scammers that the number they are using has been identified so they must move on to another number instead of having to measure the effect after the fact. *See* Reply Comments of First Orion, Corp., CG Docket No. 17-59 (filed Feb. 22, 2018).

negatives" (failing to identify a fraudster) and "false positives" (misidentifying a legitimate call as a scam call) so corrections can be made in the labeling algorithms.

We analyze and label calls through sophisticated algorithms, machine learning, and artificial intelligence, which are based on the calls we see, complaints and feedback from consumers about calls, research and verification processes, and dozens of other sources of data and intelligence. For example, no one piece or source of data ever causes a call to be labeled "Scam Likely." It is always a combination of data points. Our approach does not rely solely on using "White Lists" of legitimate callers or "Black Lists" of phone numbers of fraudsters, which scammers could easily circumvent using a variety of evolving methods to trick consumers to answer phone calls.

An upcoming enhancement in the First Orion solution will allow us to identify fraudulently spoofed calls based on individual call interrogation instead of using phone number analysis. Phone call interrogation is better at catching scammers who quickly change the numbers that they spoof. As a result, we expect the number of identified scam calls to rise from an average of 12% to as high as 15% or 16% based on current levels of traffic.

On mobile devices, in addition to labeling, First Orion solutions provide enhanced CallerID information, which includes the number calling, a company name if available, a call category (e.g. telemarketing, survey, etc.), phone number and category blocking and the ability to easily file a complaint. We also have a powerful solution that enhances traditional 15-digit caller ID to alert consumers of fraudulent and unwanted calls.

Of course, any approach will have some errors, even if minimal. For our solutions, reported cases of false positives (calls that are mislabeled as "Scam Likely" or other labels) are a small fraction of 1% of the calls we analyze. Interestingly, our reported error rate for calls where we are notified that we failed to identify a scam is also far below 1%.

Although our error rates are low, we work hard to lower them further still. First Orion collaborates extensively with call originators and consumers to actively engage all groups to improve call labeling accuracy. Consumers who use one of the PrivacyStar apps can provide feedback about whether calls are mislabeled (either as a false positive or false negative), and we use this information to better train our analytics systems. T-Mobile customers can also provide feedback about First Orion's call labeling service through the T-Mobile website. Additionally, First Orion actively solicits feedback from call originators to reduce false positives and negatives by participating in several call originator organizations and working groups.

First Orion also takes other common-sense measures to ensure callers can easily and quickly resolve errors. For example, First Orion buys the ad term "Scam Likely," so consumers and call originators who may have no other context for call labeling and blocking can reach both T-Mobile's feedback page and First Orion with just a few clicks. Consumer feedback is always helpful, so we will continue to investigate ways to maximize the feedback we receive.

We also recognize that we can and should rectify any potential errors or issues that affect legitimate call originators. We've recently launched www.CallTransparency.com, which provides legitimate call originators with the opportunity to register their number-related

information. Once both the call originator and their number information are authenticated, legitimate calls from registered numbers will not be labeled "Scam Likely."

In addition, First Orion's Perception Product, currently in beta testing, allows call originators to harness the power of our data analytics to monitor the performance and status of their outbound calling practices. For example, call originators will learn when a scammer is using one of the company's numbers to place illegally spoofed calls or when the call originator is generating significant numbers of consumer complaints. With these offerings, we strive to balance the interests of consumers and call originators alike, with a goal of helping consumers trust and appreciate their phones again.

What the Future Holds

Any effective solution that addresses scam and unwanted calls will require cooperation from all stakeholders – government, the telecommunications industry, call originators and consumers. Much work remains: even for consumers protected by industry-leading solutions with extremely low error rates, tens of millions of scam and unwanted calls are going through every month without being labeled or blocked. However, much of the groundwork for future progress has been laid.

The industry and regulators have learned a lot in this last year or so about aggressively fighting the fraudsters with new tools. For its part, industry has stepped up to the FCC's challenge to take the lead in call protection solutions and industry will continue refining algorithms and approaches over time.

By allowing providers to block a very limited class of calls, the FCC has wisely established a light-touch regulatory regime with the potential for significant consumer benefits. Providers can now block calls, without informing the subscriber, in certain instances where the call is almost certainly illegal. Providers can also couple provider-initiated blocking with other labeling and subscriber-initiated blocking tools that help consumers better decide how to customize their own handling of incoming calls.

There is one area that First Orion believes needs more focus. Supplementing ongoing efforts of the FCC, FTC and consumer organizations such as Consumers Union, First Orion recommends these parties work together to better educate consumers about the kinds of scams that are being perpetrated, the challenges in fighting scam calls, the options available to help consumers know who is calling and why and the tools available to manage the calls they do receive.

* * *

Mr. Chairman, First Orion appreciates the opportunity to appear today to share with the Committee an overview of our business and perspective on the robocall and spoofing issues. First Orion is available to provide any additional information the Committee may request.

Mr. LATTA. I want to thank all of our witnesses for being with us today. We really appreciate the information.

And that will conclude our witness opening statements, and we will move on to the 5-minute questions from our members, and I will recognize myself for 5 minutes.

Mr. Foss, since you won the FTC Robocall Challenge, what are the challenges your company has experienced in getting Nomorobo developed and installed on landline and mobile phones?

Mr. FOSS. So I think that the major challenge that we had has changed. So when we first started off it was absolutely the carrier integration problem. That seems to be thawing.

What the major problem I think right now is, is on the customer, the consumer confusion side. I even hear this mentioned a lot now where people say to put your landline and your mobile number on the Do Not Call list.

There is actually no point in putting your mobile number on the Do Not Call list. The way the TCPA is written, it is actually illegal to call mobile phones unless you have expressed written permission.

So when I actually even hear things like, "Well, you know, my number is on the Do Not Call list, why do I keep getting calls?" or when people say, "Well, put your mobile and your landline on the Do Not Call list," then what are you going to do there? I feel like it is very, very confusing right now.

I think the biggest problem with the adoption of these things is that consumers don't really understand. If they understood that there were these technologies that are available, if they understood where the government steps in and know what it can do to help, I think that that would go a long way now.

Mr. LATTA. And going along with that then, where have you received support and encouragement in that mission to protect your consumers? Where has that support been?

Mr. FOSS. From the consumers themselves. And maybe it is just like an American trait. We have a great military. We have great police. And people still protect themselves in their own homes through various means. They have firearms. They have security systems. Americans do take protecting themselves as a responsibility.

So I think that the easiest place that we have been able to find it, when consumers understand that they can go and protect themselves, that they don't have to rely on the government, that they don't have to rely on the carriers, that really empowers consumers to protect their lines.

Mr. LATTA. Thank you.

Mr. Garr, as a winner yourself, can you share the challenges and support for the RoboKiller company's experience since the FTC contest?

Mr. GARR. Sure. I also would say that we have gotten incredible support from consumers.

People are really angry about this problem. My uncle calls me up probably once every 2 months and screams about the robocalls and telemarketers he is dealing with.

Consumers are passionate about solving this problem. So we see, especially in ratings and reviews, that customers are really pas-

sionate about what we are doing. They want us to succeed and make their lives better.

Certainly the challenges are that scammers are constantly working at this problem, too. So more randomness, new technologies, that is always a challenge.

We are always getting a lot of support from the FTC and the FCC. Since we won the competition we are really fortunate to be really partnered with these agencies. Again, being invited to speak today, having the chance to go to the technology expo on Monday, these are really important to our growth.

We really feel like we have a solution in RoboKiller and our Answer Bots that scales. The only way it scales is if we get the word out there, and being able to participate in things like this has really been a supportive part of the effort.

Mr. LATTA. Let me ask this, if I could ask everyone real quickly, because I don't have a lot of time. But what can be done to stimulate more technological solutions and marketplace innovations to help consumers fight back against robocalls and spoofing?

Maybe, Mr. Hambuchen, we can start with you and just work back down real quick.

Mr. HAMBUCHEN. Thank you, Mr. Chairman.

Well, we certainly think awareness with consumers is a big part of that. The more complaints they file, the more data we have, the more we will be able to combat this.

As you know, our business, we look at labeling and giving consumers choice in blocking these calls, and so the more information we have, the more we can fight the scammers.

Because what you have to realize is these scammers are very sophisticated. They are using data and technology today much like a marketer, a direct marketer would to target these individuals. And so to combat that we need more data, more sophistication, and more analytics deployed in the carrier networks to detect that.

Mr. LATTA. Ms. Mahoney, I have got about 40 seconds left.

Ms. MAHONEY. Thank you.

We think the FCC should require the phone companies to implement advanced call-blocking technology. I think that will provide important incentives for perfecting and improving it. And we also commend the FTC for its efforts so far to spread this technology, and we think they should be allocated more funds to be able to continue these efforts.

Mr. LATTA. Thank you.

Mr. Foss, I have 17 seconds.

Mr. FOSS. I will go with educate, education, making consumers aware of what is out there and showing them that it is a real solution.

Mr. LATTA. Thank you.

Mr. Garr.

Mr. GARR. In my very short time here, real time information is always useful. We can always use that to be more effective in deploying our Answer Bots for the consumers.

Mr. LATTA. Thank you very much.

My time has expired, and I recognize the gentlelady from Michigan for 5 minutes.

Mrs. DINGELL. Thank you, Mr. Chairman.

Ms. Mahoney, I would like to explore some of your testimony regarding the FTC's authority under the Telemarketing Sales Rule to stop these illegal robocalls.

I am concerned by reports that there are a handful of small Voice over Internet Protocol, VoIP, services that are enabling these calls.

During the Senate hearing on this same topic last week we learned that these small VoIP carriers openly advertise short-duration calls, which is code for robocalls. They even offered to blend robocall traffic in with normal calls to avoid detection.

Ms. Mahoney, are these VoIP services contributing to the proliferation of robocalls?

Ms. MAHONEY. Thank you for your question.

Again, we commend the FTC for its work so far on the robocall issue, their enforcement efforts in particular. But we did learn last week from the Senate hearing that there are carriers wherein their primary line of business is to carry this fraudulent traffic.

I think if the FTC had more authority to go after them, they could use their enforcement muscle to really help crack down on this illegal activity.

Mrs. DINGELL. Thank you.

Do you think that going after the carriers that aid and abet illegal robocallers would help reduce the number of unwanted callers?

Ms. MAHONEY. I do.

Mrs. DINGELL. I certainly think that shutting these operations down would be an effective enforcement tactic, but when it comes to these unscrupulous VoIP carriers the FTC says its hands are tied because common carrier activities are exempt from the FTC Act.

Today we are releasing a draft bill that would lift that exemption for FTC enforcement against illegal telemarketing and robocalls, something that the FTC has testified that they support in the past.

Does Consumer Union support expanding the FTC's authority under the Telemarketing Sales Rule to reach common carriers?

Ms. MAHONEY. We do. We think this is a good idea and will help the FTC crack down on this illegal activity.

Mrs. DINGELL. In 1990 Congress passed the Do Not Call Registry after hearing numerous complaints about unwanted calls. That law worked for a while, but one quick glance at your call history shows it is clearly not working anymore, and all of you have testified making that clear, too, that we need to do something.

Ms. Mahoney, do you agree that existing law is insufficient and more can be done here in Congress to help consumers rid themselves of these unwanted calls?

Ms. MAHONEY. Yes. We have long been calling on the phone companies to offer free, effective antirobocall blocking technology. We do think the FCC should require the phone companies to offer this technology so that all consumers are covered. For example, consumers with traditional landline phones do not have effective, free protections against these robocalls.

So those are the important reforms that we would support.

Mrs. DINGELL. Thank you.

And I yield back the remainder of my time, Mr. Chairman.

Mr. LATTA. Thank you very much. The gentlelady yields back.

And the chair now recognizes the gentleman from Oregon, the chairman of the full committee, for 5 minutes.

Mr. WALDEN. Thank you very much, Mr. Chairman.

I was actually just trying to download one of your apps here. I am real ready to do this.

Look, I think we are all really frustrated. We now know that the Do Not Call Registry isn't that effective because these people are operating illegally to begin with. We have been through TCPA issues. It is already illegal to robocall a cell phone.

And it seems to me that technology holds the best promise here, because we can make some changes in statute probably, but at the end of the day isn't it really you all and your brain trust that are going to come up with the technology every day to try and stay ahead of the spoofers every day because they got people doing this, right?

Do you want to address that? What is the best thing a consumer can do? And what should we do to get at this?

Mr. GARR. We passionately believe that disruption of the telemarketers' business is the key to solving this problem. We believe that our Answer Bots, which wastes scammers time——

Mr. WALDEN. Love it.

Mr. GARR [continuing]. Can solve this problem.

Yes, they are entertaining, yes, they are fun, yes, you can create your own. These are great things for consumers. But they serve a really important, valuable purpose. That, again, is time.

Not just that our user is protected. If you are downloading RoboKiller right now, yes, you will be protected from that call, but the great thing is that somebody else is being protected at the same time because the calls that we are blocking and answering with our Answer Bots are wasting those spammers' time. And I am telling you, sometimes it is for 47 minutes at a time.

Mr. WALDEN. See, I really like that, because I want to get even with these people.

I remember a decade or so ago when pop-up ads were the rage on the internet. Every time I would work on a Word document or something, you have these pop-up ads. I threatened to do a death penalty for pop-up ad people, because you couldn't get anything done. And now we are all getting interrupted with these calls.

By the way, I have just downloaded your app. I may move down the table here. But I am going to be in the "get even" mode here real soon with these scammers.

Mr. GARR. We are the "get even" guys.

Mr. WALDEN. I like that a lot, because I think that is what you have to do, is create economic harm on them. Because it is hard to chase them around the globe, right?

So when I get one of these calls, I have tried to like talk to them, and they are really sweet except they don't answer, it is a robovoice for a while. So what happens? Does somebody actually answer? And what are they really after, just my financial information?

Mr. GARR. It really depends on the nature of the call. And, again, like what is really incredible is how effective they can be at reaching their victims.

That IRS scam that was played at the beginning of this testimony, that particular robocall asks you to call back a specific phone

number. That means when you call them back you are self-selecting yourself as a victim.

They don't want people who have RoboKiller. They don't want people who have another product. They want to get past them and get to the human being.

Mr. WALDEN. So they have a sweatshop caller center overseas most likely. Most of this is going on overseas, right?

Mr. GARR. They are not a monolith. I speak to a lot of scammers. You would think it is full-time job for me.

Mr. WALDEN. Is this your voice on one of these?

Mr. GARR. The one we played was my voice, yes.

We talk to a lot of these scammers. It is not one, there is not one image of them. It is three guys working together in disparate locations. It is a bullpen of 100 people.

I ask them, "How many people are in your room?" And sometimes you get, "Oh, there is just me. It is just me." And sometimes you can hear people in the background. Sometimes you can tell it is a big bullpen.

Mr. WALDEN. Stunning they are not truthful to you.

Mr. GARR. Yes, exactly. We really encourage consumers not to trust anything the spammers say or do. Don't press 1 to get off their list because why would you trust someone who is out to get you in the first place?

Mr. WALDEN. Right. I was going to ask you that, because they do have, like, press 1 if you want off, you do this or that. Bottom line is you should just hang up, right, or, no, do your deal.

Mr. GARR. Yes. If you have RoboKiller we will take care of it for you. But, yes, I think if you are going to engage never give out personal identifying information.

Mr. WALDEN. And so when somebody is using, let's just say, your app, I am trying not to hawk one service over another here, but let's say they use your app. Is that counting against their phone minutes or anything like that? Our phone minutes, I mean the consumers.

Mr. GARR. For our users? No.

Mr. WALDEN. So it is not tying up my phone line?

Mr. GARR. No, no, no. The call is being forwarded to us, and then we are answering that call. So the user is just getting a notification on their phone saying RoboKiller has blocked this call, that it is a spam call.

Mr. WALDEN. And how do you know that it is not a real call?

Mr. GARR. That is our special sauce. We are using a lot of tools. When we won the FTC's competition, we demonstrated how audio fingerprinting could be used to attack this problem. That is one of the tools we use, along with machine learning, lists that we find and build, using our own consumer's consumer information. As we grow we are building a larger and larger ecosystem to learn from.

Mr. WALDEN. OK. My time has expired. But thank you all for the good work you are doing. This is what it is going to take. And I am all about getting even with these people.

Thank you.

Mr. LATTA. Thank you very much. The gentleman's time has expired.

And the chair now recognizes the gentleman from Texas for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman, again, for holding this hearing.

Ms. Mahoney, I appreciate the work Consumers Union does trying to make America aware of options they do have to protect. I am especially concerned about protecting those more vulnerable to fraud.

Do you think the elderly specifically are likely to know about the apps and the technologies that exist to protect them from robocalls?

Ms. MAHONEY. We think more consumers should be made aware of some of the options that are out there. We would like to see consumers taking more advantage of them.

Oftentimes elderly consumers do have traditional landline phones, and existing call-blocking solutions are not adequate for those types of phone service.

So we would like to see more technologies that are available to them, as well as more education and awareness for these consumers to be able to take advantage of existing tools.

Mr. GREEN. Several witnesses have mentioned that AT&T and T-Mobile have begun offering free robocall-blocking tools to at least to some of their customers, and I am glad to hear, especially since you also mentioned that some of the competitors only provide products that consumers have to pay for.

How can we explain why only some of their customers have access to these tools and not all their customers?

Ms. MAHONEY. Thank you for your question.

Again, we think that all consumers should have access to these tools, and we do think the FCC should require the phone companies to offer to all of their customers these tools.

I think it is possible that phone companies in the short-term do not see market incentives for providing these solutions to all of their customers. So that is why we would like to see more pressure on them to take action.

Mr. GREEN. Mr. Hambuchen, in your testimony you mentioned there are over 400 apps available to consumers that offer robocall and spoofing protection. Since these apps are so widely available, what do you think are the biggest obstacles to better protection from robocalls for these consumers that are particularly vulnerable to scammers?

Mr. HAMBUCHEN. Thank you for your question, Congressman.

One of the largest issues is that the scammers are very savvy, very technologically savvy, and so a lot of these apps work based off of just a list of numbers that are going to be blocked or identified. And so that takes time to compile that information.

What the scammers have learned is that rotating that number or these neighbor spoofing-type solutions they can avoid those simple lists of numbers that should be blocked.

And so part of what First Orion is doing is developing technology that allows us to rapidly look at all that information and instead of just looking at the number, looking at the characteristics of the incoming call and identifying that information so that, regardless of what number that scammer may call from, we can identify that information and block that call or label it as a scam.

Mr. GREEN. Of these 500 apps that are available, what kinds of options are available to customers that don't have a smartphone?

Mr. HAMBUCHEN. Well, that is a tough one. Most of the apps are really for the Google Play Store for Android devices, the Apple App Store, which are iOS devices, maybe a handful for Windows smartphones. But for the feature phone you really have to rely on the carriers' in-network solution for any of that scam protection.

Mr. GREEN. Thank you, Mr. Chairman. I yield back.

Mr. LATTA. Thank you. The gentleman yields back.

The chair now recognizes the gentleman from Illinois, the vice chairman of the subcommittee.

Mr. KINZINGER. Thank you, Mr. Chairman.

And thank you all for being here. It is good to have you here on this really important issue.

I just downloaded one of your apps, as well. And I have been getting calls all the time, and I just don't even answer my phone anymore. So I am eager to get a call and listen to the exchange if it happens.

But all of you, I appreciate you being here, and we will start out with Mr. Hambuchen.

What is it about the distributed—you answered a little bit of this, but I want to see if there is anything you missed out on that— what is it about the distributed interconnected nature of the internet that allows bad actors to provision cheap and easy robocalls over VoIP? What is it just about the nature of it, I guess.

Mr. HAMBUCHEN. Well, I think the distributed nature, what you just described, the internet is connected, right, all of it is connected.

So what has happened is the cost for any company to be able to create and launch call campaigns off the internet connected to the carrier networks, the cost of that has come down so dramatically over the last couple of years it makes it very easy for scammers to launch millions of calls at very low cost. And it has also helped the legitimate businesses also reach their customers with legitimate services.

So again, I think what we have got to do is find ways to look at that data, analyze that information, and apply it back into the carrier network.

Mr. KINZINGER. Let me ask, so the internet itself obviously is old relatively, but it seems like these calls have been increasing really in the last few months, maybe the last year, exponentially. Did something change or did they just figure something out?

Mr. HAMBUCHEN. I think as the solutions are deployed and starting to stop some of the calls, so you have heard from all of us the number of calls that we have been able to block or deter, again, the scammers are able to increase their volume. So they are going to get their number of calls out there whatever it takes to hit their number of scams.

Mr. KINZINGER. And to all the industry representatives, when a customer downloads your app, has your service added to their landline, what is their typical experience in the next few days and weeks, zero robocalls, 90 percent reduction?

Mr. Garr, if you want to start.

Mr. GARR. We expect our customers to see more than 90 percent reduction in standard telemarketing calls.

Mr. KINZINGER. That is awesome.

Mr. FOSS. We don't get any of the data back on the mobile side, there is a privacy issue over there, so I can't tell you the exact number.

But what I will tell you is from the very moment that you install Nomorobo and if you go back to your recent call lists and we start labeling all those as robocallers, people will be like: Wow, I knew that that is what that was. So from the very, very moment they get a visceral feedback that it is working.

Mr. HAMBUCHEN. About 12 percent of the calls that come to our consumers are labeled Scam Likely.

Mr. KINZINGER. OK.

Mr. Foss, are you aware of robocallers spoofing the telephone numbers of fire department, EMS, police, sheriff, anything like that?

Mr. FOSS. Yes. So the spoofing known and good robocallers, even on our—like if there is something on a white list or something, does happen.

According to our data it is very, very small, and that attack is actually relatively easy to prevent. So, for instance, with our blacklist solution, when an attack is actually going on, that number is on our blacklist. When the attack stops it can be rolled off.

And as we get integrated with more and more carriers and things we can give those analytics back, and we can tell those public safety organizations: Hey, your numbers are being spoofed, switch on over to see it, something like that.

One of the new techniques that literally just started this week, though, it actually happened, it was attacking some people in Texas and California and New York, and it was aimed at Chinese Americans.

And they were using a variation on neighbor spoofing. They would call from a 212 09244 number, which is where the Chinese consulate was. The message was in Mandarin. And when we started detecting this we couldn't understand—because the messages, again, were all in Mandarin—we couldn't understand what was going on.

When we looked at the analytics and we looked at the area codes and the exchanges that this robocaller was targeting, it was absolutely places with high Asian populations.

One of the ones that popped up was Webster, Texas. Like, I don't understand. It was San Francisco, New York, those kinds of things, and then Webster, Texas. When you go and look at the demographic makeup of Webster, Texas, it is predominantly Asian.

So these spoofing issues, yes, can they go and spoof real numbers like the Chinese consulate, like the public safety organizations? Yes.

But more importantly, it is much more important to stop them as they are happening in real time, report that back. That is a solvable problem.

Mr. KINZINGER. Thank you.

Mr. Garr, in 10 seconds do you have anything to add to that?

Mr. GARR. I would just say that generally the bigger spammers, the cruise scams and things like that, are not using these highly targeted attacks. It is less surgical. They don't need to do that.

What they want to do is, again, they want to get past the people who are savvy enough to have call-blocking apps and services and get to the people who are vulnerable. So they just want to make more and more calls.

And that is why we feel that time is such an important factor here. We have to be hitting them where it hurts, which is in their wallet, and their wallet is connected directly to time. And that is how Answer Bots fight that problem.

Mr. KINZINGER. All right. Thank you all for being here.

Mr. Chairman, I yield back.

Mr. LATTA. Thank you very much.

The chair now recognizes the gentlelady from Illinois, the ranking member of the subcommittee, for 5 minutes.

Ms. SCHAKOWSKY. Thank you.

First, let me apologize. I had another meeting I had to be at, and so I am sorry that I didn't hear your testimony. I appreciate the written testimony that I have, though.

And I have heard horror stories about debt collectors taking advantage of robocall technology, harassing consumers, often several calls a day to a single recipient, hundreds of calls a month, even after the recipient has asked that the calls stop.

And, unfortunately, in 2015 Congress actually made it even easier for some debt collectors to harass consumers by allowing calls to be placed to a person's cell phone without the prior consent required for other robocalls.

So let me ask Ms. Mahoney, can you elaborate for us on what you are hearing from consumers about harassment by debt collectors? And does debt collection make up a substantial portion of all robocalls?

Ms. MAHONEY. Thank you for your question.

We have had a similar experience. We have heard from many consumers about unrelenting, harassing debt collection robocalls. And oftentimes they are intended for another person. It is very difficult to get these calls to stop because the caller does not believe that the consumer doesn't owe the debt.

We heard from one consumer who is on a fixed income, has a limited-minute cell phone plan. She is constantly receiving unwanted debt collection robocalls that are intended for someone else and can't get them to stop. So she is very frustrated that she is essentially paying for these robocalls.

And there are a couple of reasons why there are so many of these debt collection robocalls. I think there are strong incentives because of the inexpensive cost of sending out these messages for debt collectors to reach out to consumers.

Also, as you note, exemption to the TCPA was slipped into the budget bill of 2015 that exempted debt collection robocalls made on behalf of the Federal Government. For example, to collect Federal student loan debt or tax debt.

This was very unpopular when it passed. Nearly 200,000 Consumers Union activists reached out to the FCC to ask them to implement strong rules in order to limit them.

So we don't think this provision should have been passed in the first place. We do think it should be removed, for example, through the HANGUP Act.

But in the meantime, the FCC has yet to finalize rules implementing this provision, and we do urge them to do so, so that there is some clarity around the issue and that consumers know how to stop these calls.

Ms. SCHAKOWSKY. Thank you. I would agree with that. I don't see why any debt collector, even for a Federal-backed loan, should be given free rein to harass consumers.

In 2016 the Federal Communications Commission voted to adopt protections that would have established guardrails on these calls to limit their abuse, but those rules never went into effect.

So, Ms. Mahoney, can you explain the status of those rules? And do you support them being allowed to go into effect? Is that what you were referring to earlier? The FCC. OK.

Ms. MAHONEY. Right. Exactly.

So in the summer of 2016, the FCC did issue strong rules that would limit the amount of these debt collection robocalls that would be allowed to be sent to consumers without their consent, and also provided them the opportunity to stop these calls if they wanted to. Without these rules, consumers wouldn't have the ability to do so.

However, those rules went to the OMB before they could go into effect, and in January 2017 they were withdrawn from consideration by the FCC.

Ms. SCHAKOWSKY. They were what?

Ms. MAHONEY. Withdrawn.

Ms. SCHAKOWSKY. What did you say about consideration? They were dropped from?

Ms. MAHONEY. I believe they were withdrawn by the FCC.

Ms. SCHAKOWSKY. Withdrawn. Oh, OK.

So you testified the Consumers Union supports a bill that would once again require Federal debt collectors to comply with the same rules as any other robocaller. Congresswoman Anna Eshoo is reintroducing the HANGUP Act, which you referred to, here in the House.

Until we pass legislation like the HANGUP Act, what are the minimum protections that you would want to see in place to stop abusive practices?

Ms. MAHONEY. Right. So until these rules are implemented, actually that provision does not go into effect. However, there is a lack of clarity around the issue, so we are concerned that consumers will still get these unwanted robocalls from Federal debt collectors.

We would like to see rules issued in the meantime so that consumers have additional protections against them. We would like to see that provision reversed. And we would like consumers to have the opportunity to block all unwanted calls through the expansion of technology that is available to them to do so.

Ms. SCHAKOWSKY. All right. Thank you. And I yield back.

Mr. LATTA. Thank you. The gentlelady yields back.

The chair now recognizes the gentleman from Florida for 5 minutes.

Mr. BILIRAKIS. Thank you, Mr. Chair. Thank you for holding this hearing as well.

And I thank the panel for their testimony. This is a very important issue. It affects our constituents.

Mr. Garr, you mentioned that your technology does not—the constituent or the customer, the person does not have to answer the phone. In other words, it does not affect them, it doesn't interrupt them at all. In other words, they just see on the caller ID that a call was made and you interrupt the call. Is that correct?

Mr. GARR. Yes, we block the call.

Mr. BILIRAKIS. You block the call.

Mr. GARR. And then answer it with our Answer Bots.

Mr. BILIRAKIS. So no inconvenience for the constituent?

Mr. GARR. No. And all we do is we show them a notification on their phone so that they know that a call was received and that we blocked it.

Our job is to give users control of their phone. I think what you are all talking about when you say, "I don't even pick up my phone anymore, you know, we unplugged our landline," when you hear those stories, people are saying they have lost control of their phone.

Our job, what we are passionate about at TelTech with RoboKiller, is making sure people have control of their phone once again.

Mr. BILIRAKIS. And that is so very important because a lot of times when you have an elderly parent you want to make sure you pick up the phone. You never know, it is an emergency, it could be. Even with a mobile phone, I see robocall, but I identify, I see the number, and I know it is somebody that I know. So a lot of times I will pick up the phone.

Mr. GARR. Absolutely. One of our pioneering technologies is a product called TrapCall, which unmasks blocked calls, which is a problem that is still prevalent today, but was a huge deal 8, 9 years ago, it was all over the news. When people were getting blocked calls, it was really important for them to know who was calling from behind those blocked calls.

We wanted to find a way to give people back that control of their phone without disrupting their whole life, without changing the way they interact with their phones.

Mr. BILIRAKIS. Yes. And for the rest of the panel, is that correct? All this other technology, which is great, and thank you for continuing to innovate until we solve this terrible problem. You are not interrupting the consumer in any way? In other words, the phone doesn't ring during dinner or during your favorite program, is that correct, as well?

Mr. FOSS. Correct. So on our landline product, the phone will ring once and then we answer it. It stops ringing, they will see the caller ID, so people can make sure that they know that it is working.

On our mobile product, we give consumers the option, do they want to identify it as a robocall or just send it directly to voicemail. In that case, it is even one better. The only calls that come through are from people that you know or the calls that should happen.

This is a story that literally just happened last month. My uncle wound up in the hospital unexpectedly. The ambulance had to come pick him up. And he called, and I didn't recognize the number. But I trust my product. I answered it. It turns out that he was in the hospital, and he told me what room he was. I had to go and pick up some stuff from his house for him.

If I didn't answer unknown calls, I don't know what would have happened. And, ironically, when I went to pick up his——

Mr. BILIRAKIS. That is a good example. That is my greatest fear.

Mr. FOSS. That is exactly right and it is really important. And, again, this is not a made-up story. And, no joke, when I went to pick up his stuff, he has an old flip phone, feature phone, it rang. And I figured it was one of his friends who was calling to find out what is going on. I answered it, and no exaggeration, it is, "You have won a free cruise."

So on that point I was laughing because of all that was going on. But I am like, even I can't protect my uncle because he doesn't have the latest technology.

So in one case the robocall blocking apps actually—I was immediately able to get in touch with the people that I care about that are having issues, and on the other hand, it was, wait, this same call, the same technology could have taken advantage of my uncle.

Mr. BILIRAKIS. Anyone else want to comment on that?

Mr. HAMBUCHEN. Yes, Congressman, I will just add that at First Orion consumer choice is paramount. For our default solutions and carrier networks the labeling is what takes place.

So you see the call with a label of Scam Likely or some other label, and then the consumer has the option to actually block any of these calls in the future so that their phone won't ring. And for non-Scam Likely tags, those things can actually be forwarded over to their voicemail so they don't miss a call if something did get blocked.

Mr. BILIRAKIS. I have a question here. I know I am running out of time. Mr. Chairman, would you allow me to ask a question?

Mr. LATTA. Sure.

Mr. BILIRAKIS. Why don't I submit it for the record.

But I just want to make a statement. Our constituents should not have to deal with this. They should have the right to enjoy the privacy in their own home. They shouldn't even have to play defense, in my opinion. So we have to do something about this.

But I appreciate what you are doing to protect our constituents.

But this is an issue we hear about on a daily basis from family members. My dad was a member of this committee. He complains to me all the time about these robocalls, and he is right.

So thank you very much for what you do.

Thank you for holding the hearing, Mr. Chairman. And I will yield back and submit the question.

Mr. LATTA. Thank you. The gentlemen yields back.

The chair now recognizes the gentleman from New Jersey, the ranking member of the full committee for 5 minutes.

Mr. PALLONE. Thank you, Mr. Chairman.

I am glad to hear that industry groups have been working on technology to root out caller ID spoofing with a system that can

verify a call's true origin, and the call authentication trust anchor has been in development for some time now.

My questions are for Ms. Mahoney.

Do you support creating a call authentication trust anchor so that consumers know who is really calling them?

Ms. MAHONEY. Thanks for your question.

There is broad consensus that caller ID authentication can be an important step in order to address the problem of call spoofing.

And as my copanelists have mentioned, call spoofing and neighbor spoofing have become increasingly concerning. They do make it difficult for many call-blocking technologies to function. They allow spoofers to hide detection, which makes enforcement difficult, and generally just makes the robocall problem worse.

So caller ID authentication has been in development for many years. This is a technology that would allow the originating provider to confirm or validate the accuracy of the caller ID information so that that can be traced all along the call path.

And we would like to see the phone companies be required to implement some form of caller ID authentication with a certain set of consumer-friendly standards. For example, it should be free. It should have the capability to block spoofed calls as well.

Mr. PALLONE. Well, in July of last year the FCC started a process to explore the creation of a call authentication trust anchor, but the effort seems to have stalled out.

So today I am releasing a discussion draft of the Stopping Bad Robocalls Act, and one provision in my draft bill would set a 1-year deadline for the FCC to adopt rules to create such a trust anchor to ensure consumers know who is calling when they answer the phone.

So, again, Ms. Mahoney, do I understand correctly that Consumers Union supports a deadline to get this call authentication program in place?

Ms. MAHONEY. Again, thank you for your efforts to help spur this technology. We would like to see the FCC issue rules and require the phone companies to implement this technology by a certain deadline.

Mr. PALLONE. Now, how would creating a call authentication system help put an end to bad actors masking their caller ID information or spoofing and preying on unsuspecting consumers, and seniors in particular?

Ms. MAHONEY. Well, since call spoofing has made it so difficult for call blocking, again, from enforcement efforts, and it tricks consumers into picking up their phone, cracking down on call spoofing would improve the functioning of call-blocking tools and it would allow consumers to trust their caller identification information again.

Mr. PALLONE. Now, would an authentication system also make enforcement easier by helping track the source of illegal robocalls?

Ms. MAHONEY. Yes. That has been a focus of the phone companies in order to speed up this process. Since calls are routed through multiple carriers, it can be time consuming to track them down to their original location.

The phone companies have been exploring things like trace back to speed this process. But caller ID authentication would overall speed up this process and make it much more effective.

Mr. PALLONE. Well, you mentioned in your testimony that because of a court ruling, the definition of autodialer is unclear. In the wake of that court case, do you generally support a clarification of that definition?

Ms. MAHONEY. Yes. The ball is in the FCC's court in order to clarify a definition of an autodialer that protects all consumers and the existing autodialers that are in use. But we appreciate any assistance in that.

Mr. PALLONE. And I have also heard that many consumers are plagued by robocalls they receive as a result of reassigned phone numbers.

Do you support requiring the FCC to establish a nationwide database of consumer telephone numbers that have been reassigned to other consumers so we can help stop these annoying calls?

Ms. MAHONEY. Yes. We urge the FCC to implement regulations to create the reassigned number database, as proposed, in order to cut down on this problem of wrong number robocalls.

Mr. PALLONE. And the bill I released, I mentioned, addresses the issue with the definition of an autodialer and would require the FCC to establish a database of reassigned numbers.

I know we have heard a lot about neighbor spoofing, but I recently heard from a constituent about something perhaps even more alarming. Instead of the first six digits looking like her phone number, so she would think it was a neighbor calling, the first six digits looked like a phone number of a relative that frequently calls.

I don't know how the spoofing companies would know what calls are coming in, but if there is some sort of access to caller information, I think we should stop it.

Do you have any thoughts on this report that I am mentioning?

Ms. MAHONEY. I have not personally heard from any consumers about this happening, but scammers are smart and they are constantly thinking of ways in order to trick consumers into handing over their money or personal information, so I wouldn't put it past them. And certainly we hear often about neighbor spoofing, in which the first six digits are spoofed.

Mr. PALLONE. All right. Thank you so much.

Thank you, Mr. Chairman.

Mr. LATTA. Thank you. The gentleman yields back.

The chair now recognizes the gentleman from South Carolina for 5 minutes.

Mr. DUNCAN. Thank you, Mr. Chairman. Thanks for this timely hearing.

I got a Facebook post on my feed the other day from a constituent. She said this:

"I realize we deregulated cell phone marketing awhile back. Woohoo. But the Do Not Call options don't work.

"I am on a Do Not Call list," she said. "I punched the number to take me off the list and they just call from another number, a

number that, by the way, you can't call back. Yes, you can block, and I do, but the bots just call from another number.

"What kind of scam business thinks this works? I wouldn't in a million years get their extended warranty, health insurance, et cetera."

I, too, have been called just recently by the IRS. Apparently I was involved in some tax fraud, and if I didn't call them right away, I face jail time.

I called them back, or I answered one of their calls, it came right in, I can't remember if I called back, whatever, because I wanted to know. I told them who I was. I told them that I was going to investigate whether they were legitimate. And I said, "If you are a fraud, we will find out, and the authorities will knock on your door."

The guy offered to give me his badge number and to spell his name. He didn't do a very good job pronouncing his name and definitely couldn't spell it. He had to spell it per letter, A as in apple, that sort of thing. I never did get his name right because he didn't speak English very well.

Then just this week I was called by the Social Security. They were out of Texas. But they called me and said that I was involved in Social Security fraud.

For the people that are watching, the IRS does not call you and the Social Security Administration does not call your phone. They send you something in the mail and you call them.

So I want all the people across America not to fall for this scam. But it raises an important issue that we are talking about today.

And I want to ask you guys. Let's take a hypothetical scenario that a robocaller would get hold of a home security company that a consumer uses or a bank number even, a number that they would recognize, and they started using that.

How would it work in your system if that happened, if they spoofed a legitimate number, not one of the cell phone exchanges from my area that I would recognize? "Well, maybe that is somebody that I know and I don't have them in my contacts." They use a legitimate number that might be your local bank, and the consumer wouldn't complain about that number because they don't want to not have their bank call them, right? What would happen and how would that work?

Mr. GARR. That is a great question. And I think it is really important when you think about call-blocking technology that it is just as important that you are removing numbers from the list as adding numbers to the list, and that is what we think we do really well.

Our algorithms are working in real-time to understand patterns of calls. So what you are describing, if it happens, it is very unlikely that it is a single call coming from that number. It is multiple calls coming from the same number, even if they are spoofing a legitimate number.

We see that spike because we have a large ecosystem of users, we have just on RoboKiller 164,000 users now, a large ecosystem of users potentially seeing that call. If we are seeing that call in real-time come in, we know that it is likely a scam, and we are able

to prevent, block against that. So we are an able to adapt really quickly.

And I think, going back to what you are saying, consumers should always remember when the phone rings, my grandfather's principle, which is honest people are always willing to put things in writing. So if you get a call and someone is asking you for personally identifying information, even a company you work with, ask yourself why, and say, "You know what, if you want to ask me that question, send me a certified letter."

Scammers aren't going to take the time. Again, this is all about time. Scammers want to get past you, as a skeptic, and get to somebody they can target. They want to get to the vulnerability people.

Mr. DUNCAN. And it is the seniors that are the most vulnerable in this. I really think there ought to be a public service commercial that runs on the TV during the time that seniors are watching to warn them that the IRS will never call you, don't give any of your personal information.

We have done a lot. All of us have done messaging within our ability.

Let me ask you this. Could they theoretically spoof the House of Representatives' number and put that in?

Mr. GARR. Sure. Caller ID is not something that you should automatically trust or can automatically trust.

But spoofing is a complicated issue. I don't know what phone system you use, but there is a very good chance that the phone system in this building spoofs calls. Spoofing is not a monolith. Spoofing is used for legitimate purposes all the time.

Mr. DUNCAN. Spoofing is used for legitimate purposes all the time?

Mr. GARR. Absolutely.

Mr. DUNCAN. Give me an example. Give the committee an example of that.

Mr. GARR. Sure. My stepfather is a veterinarian. When he has to call a client back at night for an emergency he spoofs his office number so that he is not giving away his personal home number or mobile number, and also so that his customer knows that it is him calling, it is his animal hospital calling.

Lots of people use spoofing for legitimate purposes all the time. Again, it is not just a monolith, you can't look at it and say all spoofing is bad.

Mr. DUNCAN. Just by the use of the word "spoof" tells me it is bad, that you have got to use that terminology.

Mr. GARR. Yes, it has a terrible connotation.

Look, I am not saying that robocallers aren't using it for illegitimate purposes and that is not a problem we need to work on. What I am saying is that spoofing is a tool, and people are using it for legitimate purposes all the time.

Somebody used the example of your pharmacy calling you. When you see CVS calling you, it is always CVS. How do they do that calling from multiple CVSs? Probably using spoofing. I can't say that for 100 percent sure. But spoofing is used all the time to maintain a consistent——

Mr. DUNCAN. Just that phrase, Mr. Chairman, that spoofing is used for legitimate purposes strikes me as odd.

I know I am out of time. Thank you so much. I yield back.

Mr. LATTA. Thank you very much. The gentleman's time has expired.

The chair recognizes the gentleman from Kentucky for 5 minutes.

Mr. GUTHRIE. So to follow on that point he just made. So if one of us uses our personal cell and calls a constituent back and it shows up U.S. House of Representatives, our office number, that is spoofing, by definition?

Mr. GARR. I think you are saying using your mobile number?

Mr. GUTHRIE. Yes, using my own personal number and the office number shows up on their caller ID.

Mr. GARR. What I was more saying is that if you are calling from an office number here and it says U.S. House of Representatives, there is probably, in a building this size, hundreds of different phone numbers, hundreds of different phone lines. The system, I think it is called the PBX, is using spoofing so that you maintain that unique number that the person on the outside sees on their caller ID.

Mr. GUTHRIE. OK. I see what you are saying. All right. Thanks. I was just asking if that was an example.

So I have a question for the technology companies addressing the issue head on. Mr. Foss and Mr. Garr and Mr. Hambuchen, do any of your companies approach the robocall problem by diverting calls to voicemail directly? And have provider's legitimate call originators or any regulators expressed concerns about that?

Mr. FOSS. I think you have touched on something very important. And the wording that we all use, again the spoof, the setting of the caller ID, when we say blocking or stopping, labeling those, I think it is really important, you have touched on something really important.

On our product, on mobile, when we say block the call, that is shorthand for it goes directly to voicemail. One of the other representatives said, like, if you don't answer it, it is just like declining it and then they don't leave a message.

That is incredibly safe because everybody misses calls all the time. Everybody is always kind of worried, "Oh, are we going to miss it." Like, we just dump it to voicemail.

On our mobile product, when we say that we block a call or stop a call, we actually prompt the user to type in a captcha. So it says, "This phone is protected by Nomorobo, please type the number 3286." It picks a random number. And if they type it in, proving they are human, we let the call through.

So it is really important to understand that blocking the call and making it disappear into the ether is not the right way to do it.

But putting up a challenge, getting them over to voicemail and then allowing the user to go and check that or to add that to their contacts, that is really what we are talking about when we are talking about stopping the call. It is really important.

Mr. GUTHRIE. OK. Any other answers from the other two of you?

Mr. HAMBUCHEN. Sure. At First Orion the approach we take is we are labeling calls with Scam Likely when we know it is a scam.

We also have other labels, such as Telemarketer or Nuisance Likely, based on what we know about that number.

As I mentioned, we think consumers should have choice. And so consumers can see the label for any of these calls, but can also have those calls what we would call blocked.

Scam Likely calls, when we say blocked, they go away, they don't go to voicemail. All the other types of calls would go to voicemail. So if it was a telemarketer, a survey, account service, or some other type of label, those would go to your voicemail.

Mr. GUTHRIE. OK.

Mr. GARR. Yes, if I can just say, some originators have complained. But, again, our users are looking for control of their phones. It is their phones, not the originator's, not anyone else's.

There is a difference between legal and illegal versus wanted and unwanted and our users are asking us to prevent unwanted calls. Just because a debt collector may be a legal telemarketer and just because a political robocall—and I understand why you guys may use them at times—may be a legal call, that doesn't mean that the consumers want to receive them. So it is really important that we give them the control to do that.

But, again, we are forwarding the calls—we are answering the calls that we are blocking. That gives the users control over those calls to decide what to do with those calls after the fact. They can hear these Answer Bots.

Mr. GUTHRIE. OK. Thank you, Mr. Garr. I will continue with you.

What can be done to enhance consumer education from a parent's child who might be getting their very first smartphone, for a senior citizen with a traditional landline, and a mobile phone?

Mr. GARR. Again, I think there are a couple things that you should always be teaching people about the use of their phones. One is that caller ID is not something you can trust out of hand. And when someone calls you, unless it is someone directly that you know, a really trusted source, there is no reason ever to give them your personally identifying information.

Especially when they are using time to put pressure on you, that is the time to push back and say, "If this is a legitimate call, if this is a legitimate request, put it in writing, I will be happy to answer you."

Like I said, my grandfather always said, honest people will always put things the writing, and I think that is a principle that we should always adhere to when we are thinking about this these calls.

But, again, if you put something like RoboKiller on your phone and you get Answer Bots working for you, you are preventing these calls from ever even reaching you and you are protecting yourself and the people around you.

Mr. GUTHRIE. OK. Thank you.

And I am about out of time so I will yield back.

Mr. LATTA. Thank you very much. The gentleman yields back.

The chair recognizes the gentleman from Oklahoma for 5 minutes.

Mr. MULLIN. Thank you, Mr. Chairman.

And thank you guys for taking the time on this day to just come and visit with us. We all know it is a problem. It is just unique to find individuals that are putting so much time to it.

Used to be you could just get rid of your landline and that solved the issue. Now even my cell phone, as my colleagues have stated up here, their cell phones are being called now.

So can you guys just elaborate, how effective are the Do Not Call lists from State to national? Are they even worth the time that we put them in place?

Go ahead, Mr. Foss.

Mr. FOSS. So the Do No Call Registry was created back in the early 1990s with the TCPA, it was implemented in the early 2000s. Think of the world back then. We didn't have cell phones. The Internet didn't exist.

Mr. MULLIN. We did, but they were bag phones.

Mr. FOSS. Exactly. Car phones, right.

The world has changed. So at that time it was legitimate telemarketers and there was no way to tell them to stop. That made sense then as an opt-out mechanism. Legal robocallers, they will go and follow the rules.

Today the robocallers don't follow the rules. Nobody is downloading the Do Not Call list. It is like having a Don't Rob Me list and that all the criminals have to go in. And, look, it hasn't kept up with the time.

I personally think that we should clarify that everything is just opt-in. If you are calling somebody to sell them something, anything with money, to collect a debt or something, I just think you need to have express written permission. It would save a lot of this whole, the patchwork of regulations and rules and clarifications, and this law came in and this was taken and that, if you have to opt in.

Mr. MULLIN. But how could you opt-in, because I don't think anybody gave them their phone numbers to begin with.

Mr. FOSS. Correct.

Mr. MULLIN. So how would that system work? Because it is not enforceable the way that it is now. I don't think anybody opted in to begin with.

Mr. FOSS. Correct. If it was opt-in, and we could basically say, which is pretty much what we are trying to say right now, is that any of those types of calls are illegal, right, and therefore the——

Mr. MULLIN. My point is, is that if you are already on the Do Not Call list, it already is illegal, but it is not being enforced.

Mr. FOSS. If you are on the Do Not Call list and they call a landline, there are all these different kind of—the truth in this lies in the gray area, right?

And then when the carriers, the different regulations and things, when it gets that one bad actor, and they say, well, common carrier, we don't have to—these criminals are always going to look for that one little sliver and go and run through there. And at best, it is going to take years to go and litigate.

If those things were more, "Did you have express written permission to call that person?" OK, show it to me.

Mr. MULLIN. Even what you said earlier, though, you don't need more regulations, just what is put in place, you actually would. If

you put in opt-in, you would have to have regulations that stated that you have to opt-in, but then the enforcement arm is still there. Well, the enforcement arm isn't working on the Do Not Call list.

So explain to me how that would work, because we are all in. We would be all in on that. Do we need to give the FTC or the FCC more broad powers, more teeth? Is that how that works? Because you have got to have it—regulations have got to take place for even the opt-in process.

Mr. FOSS. So let me give you an exact example of this. They are always skirting around this.

Mr. MULLIN. We know they are skirting around.

Ms. FOSS. Right. What is an ATDS, what is an automated telephone dialing system? Now there are a lot of the debt collection companies, HCI, they will manually push a button, they will have somebody, which gets around all the TCPA laws.

I don't even care if those calls are made with an automated dialer, I don't care if it is made from a computer, I don't care if it is somebody that is pushing that button, if you are trying to sell somebody, to scam somebody, to take some money, do something like that, yes, you should not be able to do that.

And then I would think it would give more teeth to the FTC to go after these and the FCC would be able to give a lot less cover.

Mr. MULLIN. All that is great, but it still goes back to the same thing. It doesn't make any difference if it is not enforceable.

Mr. FOSS. Correct.

Mr. MULLIN. If someone else wants to jump in this. How would you enforce it?

Ms. MAHONEY. I do think it is important that consumers have legal protections against unwanted robocalls. Phone companies are reluctant to block so-called legal robocalls. So if consumers don't have these protections, they won't be able to take advantage of some of the blocking.

Mr. MULLIN. How would it be enforced? That is what I am trying to get to. Does anybody have an idea how this thing could be enforced, how Congress could help push that to the next level?

Mr. GARR. Truthfully, I don't think a Do Not Call list is the solution.

Mr. MULLIN. I agree. Well, it is not working, obviously.

Mr. GARR. I don't think it can. There is even a theory that the Do Not Call list actually empowers telemarketers, because if people get a call who are on the Do No Call list, they automatically by default think, "Well, it must be legitimate, I am on the Do Not Call list. So I will answer this question."

So the telemarketers have this thought that, "Hey, if I get someone on the Do Not Call list, they are an even better target." I don't think legislation alone is the solution.

Mr. MULLIN. Just technology.

Mr. GARR. I think technology is the solution.

Mr. MULLIN. So that leads to my question, where I was trying to get to. So it is not regulation in your opinion, it is the private industry that is going to drive the end to robocalls essentially.

Mr. GARR. We believe we are already doing it.

Mr. MULLIN. Do you agree?

Mr. HAMBUCHEN. Sure. I would just add one thing. I think you are right in terms of technology and innovation are what is going to solve the problem. And recently, over the last couple of months, the rules were clarified on enabling carriers to start blocking scam calls, unwanted nuisance calls for consumers.

So allowing industry to start spurring innovation on top of that, I think you are going to see an explosion over the next couple of years of solutions to combat the problem.

Mr. MULLIN. Thank you. And I am out of time. Thank you so much, once again, for being here and taking the time.

This is something, I feel like, that we are going to be relying more and more on private industry to drive and help solve this problem, which is typically what happens in our country to begin, which is great. The government's responsibility is to help you guys, you entrepreneurs, go out and thrive and create and solve problems or create opportunity.

So thank you for doing what you are doing. Appreciate it.

Mr. LATTA. Thank you very much. And the gentleman's time has expired, and seeing no other members wishing to ask questions.

I also want to thank our witnesses for today's hearing. It has been very, very informative. Because, again, it is an issue out there that we all hear about, and I tell you, as the gentleman from South Carolina that not only heard from the IRS, but the Social Security. But it is an issue and we hear it. And people say, "What are we supposed to do?"

And some people, I have heard, in our districts, they actually fall for it and they send the money in. And all of a sudden they find out they are $5,000, $10,000 out, and they don't have $5,000 or $10,000 to be out. So it is really important that the public is protected out there, and that is what we are here to do.

So again, I want to thank you all for being here.

But before we do conclude today, I want to also include the following documents to be submitted for the record by unanimous consent: a joint letter from multiple trade associations; a letter from the Electronic Privacy Information Center; a letter from CTIA; a letter from USTelecom; and a letter from the U.S. Chamber Institute for Legal Reform.

[The information appears at the conclusion of the hearing.]

Mr. LATTA. Pursuant to committee rules, I remind members that they have 10 business days to submit additional questions for the record. And I ask that witnesses submit the response within 10 business days upon receipt of the questions.

And without objection, the subcommittee will stand adjourned. Thank you very much for being here.

[Whereupon, at 10:38 a.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

Even in today's divisive climate, certain things still unite us as Americans. High on that list is our universal frustration with robocalls. They interrupt family dinners, evenings out, and even an occasional Congressional hearing. We might be tempted to ignore them, but when we check the caller ID, the number looks familiar. Is it our child's school, or the doctor's office, or a neighbor? Reluctantly, we pick up only to hear that we have won a free cruise, that Rachel from cardholder services can get us a better interest rate, or that a virus has been detected on our computer.

An estimated 18 billion unwanted calls were placed in the U.S. last year. That is a 76 percent increase over the previous year. The nuisance is so great that people are disconnecting their landlines altogether. But these calls are much more than a nuisance. They cause enormous economic harm. In 2016, more than 22 million Americans lost a total of $9.5 billion in robocall scams-an average $430 per person. Some victims have been conned out of their entire life-savings.

It is no surprise that unwanted telemarketing and robocalls top the consumer complaint list at both the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC). Both agencies are taking action to stop them. But unfortunately, illegal robocalls are proliferating. Staggering profit margins mean that even large fines won't deter bad actors. For every dollar robocallers spend, they make as much as 20 dollars profit. That's a 2,000 percent profit margin.

Moreover, we are caught in an escalating technology arms race. Voice Over Internet Protocol (VoIP) technology and autodialing enable law-breakers to place more calls at just a fraction of a cent per call from anywhere in the world. And sophisticated Caller ID spoofing tools have led to a dramatic rise in robocalls appearing to come from your area code and even similar phone number to yours. As law enforcement gets better at tracing robocalls back to their true point of origin, the scammers find new ways to mask their identity.

Given this reality, it is clear that reactive policing, no matter how aggressive, is not enough. Consumers need better proactive tools to block robocalls.

I understand the FTC and FCC are promoting the development of new tools, including at a joint technology expo earlier this week. And two of our witness are winners of past FTC contests to spur the creation of call-blocking apps. I look forward to hearing about those tools from our witnesses and from Consumers Union on any regulatory gaps we need to close or enforcement tools we should add to the federal arsenal.

As a start, today I'm releasing a discussion draft of my Stopping Bad Robocalls Act. With this discussion draft, we begin the task of crafting serious legislation to address these annoying calls consumers face day in and day out.

This discussion draft includes a number of common sense proposals to help protect consumers, and I'm interested in feedback as to how this draft can be refined and improved before introduction. Among other things, my discussion draft would put the teeth back into the Telephone Consumer Protection Act, enact strong consumer protections for allowed calls, give the FCC tough enforcement tools to use against robocallers, and require the FTC and FCC to work together to reduce unwanted calls by 50 percent annually year over year.

I urge my colleagues to review this draft, and work with me to help stop these unwanted calls. Thank you.

April 25, 2018

The Honorable Bob Latta	The Honorable Jan Schakowsky
Chairman	Ranking Member
Subcommittee on Digital Commerce and	Subcommittee on Digital Commerce and
Consumer Protection	Consumer Protection
Committee on Energy and Commerce	Committee on Energy and Commerce
U.S. House of Representatives	U.S. House of Representatives
2125 Rayburn House Office Building	2322A Rayburn House Office Building
Washington, D.C. 20515	Washington, D.C. 20515

Dear Chairman Latta and Ranking Member Schakowsky,

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 House Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection hearing entitled "Do Not Call: Combating Robocalls and Caller ID Spoofing."

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 Subcommittee 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 Subcommittee 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

epic.org

April 26, 2018

The Honorable Bob Latta, Chairman
The Honorable Jan Schakowsky, Ranking Member
House Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection
2125 Rayburn House Office Building
Washington, D.C. 20515

<div align="center">

RE: "Do Not Call: Combating Robocalls and Caller ID Spoofing"

</div>

Dear Chairman Latta and Ranking Member Schakowsky:

We write to you regarding tomorrow's hearing on "Do Not Call: Combating Robocalls and Caller ID Spoofing."[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,

---

[1] *Do Not Call: Combating Robocalls and Caller ID Spoofing*, H. Comm. on Energy & Commerce, 115th Cong. (April 26, 2018), https://energycommerce.house.gov/hearings/do-not-call-combating-robocalls-and-caller-id-spoofing/.

[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/tcpacomments.html.

[5] *See, e.g*, EPIC, EPIC Administrative Procedure Act (APA) Comments, https://epic.org/apa/comments/; 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

---

<div align="center">

Privacy is a Fundamental Right.

</div>

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 phones[10] 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 everywhere,[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

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/apa/comments/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% of American adults own at least one cell phone and 77% 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.

[11] More than 70% 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.

[12] Federal 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).

[13] Bill 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/.

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 FTC[17] 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 data stored in databases.[18]

---

[14] No. 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.
[17] *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.
[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-Inisder-Threat-Comments.pdf; Comments of EPIC, *Department of Defense (DoD) Insider Threat Management and Analysis*

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/ *Christine Bannan*
Christine Bannan
EPIC Administrative Law and Policy Fellow

/s/ *Alan Butler*
Marc Rotenberg
EPIC Senior Counsel

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).

ctia™

Meredith Attwell Baker

April 27, 2018

The Honorable Bob Latta, Chairman
The Honorable Jan Schakowsky, Ranking Member
Subcommittee on Digital Commerce and Consumer Protection
Committee on Energy and Commerce
United States House of Representatives
Washington, DC

Dear Chairman Latta and Ranking Member Schakowsky:

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 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 <u>495% increase in call blocking</u>, 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 US 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 Cequint, 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 Cequint. 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

USTELECOM
THE BROADBAND ASSOCIATION

April 27, 2018

The Honorable Bob Latta
Chairman
Subcommittee on Digital Commerce
and Consumer Protection
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Digital Commerce
and Consumer Protection
2322A Rayburn House Office Building
Washington, DC 20515

Dear Chairman Latta and Ranking Member Schakowsky:

Over the last several years, USTelecom and our member companies have been tremendously focused on the robocall issue, and we share the Subcommittee'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 reports to the Federal Communications Commission (FCC) on October 26, 2016, and April 28, 2017. These reports, taken together, catalogue industry's substantial efforts to advance the battle against illegal robocalls, and hold significant 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, and a Federal Advisory Committee 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 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. 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. Moreover, at a recent joint FCC and FTC robocall workshop, it was noted that since 2016, there has been a 495% 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 past 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.

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. USTelecom and its industry partners stand ready to further assist in these efforts to bring 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 enable further enforcement actions by federal agencies. While current civil federal 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 activity should be identified, targeted and brought to justice through criminal enforcement efforts. 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.

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.

Sincerely,

Jonathan Spalter
President & CEO

2

April 26, 2018

Scott D. Delacourt
202.719.7459
sdelacourt@wileyrein.com

Chairman Bob Latta & Ranking Member Jan Schakowsky
Subcommittee on Digital Commerce and Consumer Protection
House Energy and Commerce Committee
2125 Rayburn House Office Building
Washington, D.C. 20515

      Re: Hearing on Robocalls and Caller ID Spoofing

Dear Chairman Latta and Ranking Member Schakowsky:

I write on behalf of the U.S. Chamber Institute for Legal Reform[1] ("ILR") to discuss the obstacles abusive robocalls have caused businesses seeking to communicate with their customers. I recently testified on behalf of ILR before the Senate Commerce Committee regarding the Telephone Consumer Protection Act ("TCPA") and robocalls, and this letter contains a number of salient points from that testimony for your consideration during the Digital Commerce and Consumer Protection Subcommittee's hearing on robocalls.

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. 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, businesses need to be 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

---

[1]   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.

Chairman Bob Latta & Ranking Member Schakowsky
April 26, 2018
Page 2

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.[2] 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% between 2015 and 2016.[3] Much of this
litigation targets legitimate companies—many of which are well-known brands—
that have committed marginal or unavoidable violations as they seek to contact their
customers,[4] 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.

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 to be an automated
telephone dialing system ("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 smartphones and tablets, creating

---

[2]   47 U.S.C. § 227(b)(1)(A).

[3]   *See 2016 Year in Review: FDCPA Down, FCRA & TCPA Up*, WebRecon
LLC (2018), https://webrecon.com/2016-year-in-reviewfdcpa-down-fcra-tcpa-up/.

[4]   *See, e.g., Story v. Mammoth Mountain Ski Area, LLC*, No. 2:14-cv-02422-
JAM, 2015 WL 2339437 (E.D. Cal. May 13, 2015); *Gragg v. Orange Cab Co.*, 995
F. Supp. 2d 1189, 1193 (W.D. Wash. 2014); *Emanuel v. Los Angeles Lakers, Inc.*,
2013 WL 1719035 (C.D. Cal. Apr. 18, 2013).

Wiley Rein LLP

Chairman Bob Latta & Ranking Member Schakowsky
April 26, 2018
Page 3

major uncertainty for businesses. Indeed, the FCC's *Omnibus Order* contributed to a 46% increase in TCPA litigation.[5]

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 ATDS, which the court described as "utterly unreasonable."[6] 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.

As Congress and the FCC look for ways to reduce abusive robocalls, reforming the TCPA is an important step. 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 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 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 and shift the focus of enforcement to the actual bad actors who are the root cause of illegal robocalls.

---

[5]   *TCPA Litigation Sprawl: A Study of the Sources and Targets of Recent TCPA Lawsuits*, U.S. Chamber Institute for Legal Reform at 2, 4 (Aug. 2017), http://www.instituteforlegalreform.com/uploads/sites/1/TCPA_Paper_Final.pdf.

[6]   *ACA Int'l v. Fed. Commc'ns Comm'n*, 885 F.3d 687, 699 (D.C. Cir. 2018).

Wiley Rein
LLP

Thank you for your consideration and for holding a hearing on this important issue.

Sincerely,

/s/ Scott Delacourt

Scott D. Delacourt
*Counsel to the U.S. Chamber Institute for
Legal Reform*

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 Rayburn House Office Building
Washington, DC 20515–6115

Majority (202) 225–2927
Minority (202) 225–3641

May 14, 2018

Mr. Ethan Garr
Chief Product Officer
RoboKiller, TelTech Systems
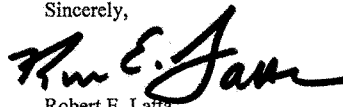101 South Broadway
South Amboy, NJ 08879

Dear Mr. Garr:

Thank you for appearing before the Subcommittee on Digital Commerce and Consumer Protection on Friday, April 27, 2018, to testify at the hearing entitled "Do Not Call: Combating Robocalls and Caller ID Spoofing."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. To facilitate the printing of the hearing record, please respond to these questions by the close of business on Tuesday, May 29, 2018. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to ali.fulling@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Robert E. Latta
Chairman
Subcommittee on Digital Commerce
and Consumer Protection

cc: Jan Schakowsky, Ranking Member, Subcommittee on Digital Commerce and Consumer Protection

Attachment

Response to Additional Questions
Do Not Call: Combating Robocalls and Caller ID Spoofing

Chairman Latta, and Members Burgess and Bilirakis,

Thank you again for the opportunity to present testimony before the Sub-Committee on Digital Commerce and Consumer Protection. It was an honor and privilege to participate, and I appreciate the opportunity to provide feedback to your follow-up questions in this document.

Thank you,
Ethan Garr
RoboKiller.com
Chief Product Officer

Response to questions from: The Honorable Robert E. Latta

1. Today, our RoboKiller mobile app has over 210,000 customers. Following a one-week free trial period, users can either pay $2.99 per month or $24.99 per year.
2. RoboKiller works by putting Answer Bots, which are time wasting robots to work against the invasive spam and telemarketing calls we block for our users. Using an advanced algorithm that blends technologies including machine learning and audio-fingerprinting, we are able to maintain a comprehensive and dynamic global block list of more than 200,000 known spammers. We use Apple's CallKit technology to block these calls from ringing on our customer's phones, but then, using a call forwarding methodology, we are able to answer the calls we block with Answer Bots. These robots, which users either record themselves, or choose from our library, are trained to reach the human telemarketers behind robocalls to waste their time with extended conversations. While these conversations are entertaining and give our users the satisfaction of getting even with telemarketers, they also serve an important purpose: every minute of a telemarketer's time we waste, is a minute they cannot use to scam someone else, whether that is one of our customers, or someone's unsuspecting grandmother. By wasting telemarketers' time, RoboKiller is able to interfere with the spammer's business model, which ultimately will put them out of business.
3. Once a subscriber downloads and successfully sets up RoboKiller, they are immediately protected from more than 200,000 known spammers and from the majority of neighbor-spoofed calls (telemarketing calls that appear to be coming from a local caller ID). These calls will no longer ring on their mobile phones, but the service will answer these calls with Answer Bots. When a telemarketer calls one of our user's phone numbers, our customer only receives a push notification indicating that RoboKiller has protected them from the intrusion. Their phone does not ring. Most users will experience a 90% reduction in spam calls when they use the service. Users are also given the opportunity to provide feedback when we block calls on their behalf, to help our service better protect them and all of the users in our ecosystem. Users can also manually whitelist

and blacklist numbers, and we use data from these interactions to help us train our blocking algorithm.

4. We estimate a false-positive rate of less than 1.5%, and give our users the ability to provide feedback if we incorrectly identify and block a numbers so that we can update the service for them and for other users appropriately.

5. For RoboKiller, if Apple continues to expand the functionality of its CallKit service it will help us improve our call blocking service. If the equipment manufacturers added call blocking without our app it would limit our ability to use Answer Bots on behalf of our users and likely exacerbate the robocall epidemic as a whole. We contend that unless we can impact spammer's bottom line, the problem will only get worse. Blocking calls alone, just means that spammers skip over savvy users who are unlikely to fall victim to scams, to more efficiently reach their more vulnerable, intended targets.

6. We are not currently sharing call complaint data with the FTC, but we are certainly open and willing to do so. We have not discussed this with the FTC in a long time, but when we did (a few years ago), it did not seem like they had an easy way to ingest data that we could provide. We do include data from the FCC in our call blocking algorithm, but this data is not real time, which makes it a less valuable source for us. From our own efforts, we have found that call data that is even a few hours out of date is less useful for the purposes of curating our global block list, so we are only able to use this data as a secondary point of verification. If the FTC can provide a live feed of this data that we can consume it will substantially improve its value and usefulness for our purposes. Also, if the FTC can give us a method of providing large batches of data we collect, we would be happy to do so. We also feel our users would get great benefit and appreciate it if we could give them an option to share complaint data directly from the app or our website to the FTC.

7. Our system is self-correcting in that our users provide feedback about the calls we block for them both directly and indirectly, and then we use that information to correct our global block list. If we see users providing feedback, or blacklisting, or whitelisting numbers in a manner that is inconsistent with how we are marking those callers, our algorithm will consider that and adjust as appropriate. In rare cases we will make manual changes based on feedback we receive through our support channels.

8. Audio-fingerprinting, as we are using it, should not impact privacy as the only calls we are fingerprint are recordings of calls such as voicemails or interactions between our Answer Bots and robocalls, as directed by our users to improve the quality of their service. Audio-fingerprinting only looks at the recordings as audio data and makes comparisons between sets of data, so it should not impact privacy for any party.

Response to questions from: The Honorable Michael C. Burgess

1.
   a. We are not sure if this question is specifically meant for RoboKiller, as we have not been part of, nor have we been asked to comment, on this rulemaking process. Generally speaking, RoboKiller looks to block all

unwanted calls a user might receive, and allow only wanted calls to ring through. Whether or not a call is legal or illegal, is not the question our users are asking RoboKiller to discern, they are looking for the service to block calls they feel are unwanted. We do recognize that different users will have different opinions as to whether a call should or should not be blocked, and therefore, we notify users whenever we block a call so that they can decide if they agree with our system's decision. Users can blacklist or whitelist any number to ensure that the calls we block or do not block are appropriate.

b. Yes, if our users believe calls are legitimate and should not have been blocked, our system is self-correcting. If we see users providing feedback, or blacklisting, or whitelisting, numbers inconsistent with how we are marking callers, our algorithm will consider that and adjust as appropriate. In rare cases we will make manual changes based on feedback we receive through our support channels. However, we feel strongly that our users should determine what is a wanted versus unwanted call.

2. Most companies, like RoboKiller, use their blogs to speak to users about such issues. I think if government entities like the FTC, FCC, and IRS reach out directly to companies like us with specific information about scams and issues, we would be happy to share that content with our users. We are always looking to help consumers better understand the threat and the scope of the problem, but it is difficult for us to know, without a central channel, what information the Government would like us to share with our audience.

3. Because RoboKiller answers the calls it blocks and then allows users to listen to these calls the way they would listen to voicemails, we don't believe our solution threatens legitimate companies ability to conduct business. Consumers should be able to decide what calls they wish to ring through to their phones, and our service provides that ability without risk that important calls will be discarded. Furthermore, our system's self correcting nature ensures that through user feedback, RoboKiller will adjust to allow wanted calls to ring through.

Response to questions from: The Honorable Gus Bilirakis

1. Pre-paid mobile users are more vulnerable to scams. They are no more likely to get robocalls and telemarketing calls than people with unlimited plans, as the spammers have no way to target one over the other, however, most mobile carriers do not provide pre-paid plan subscribers with access to conditional call forwarding, which is a feature we need to provide the RoboKiller service to customers.

2. To be clear, I feel that robocall blocking tools that do not make efforts to engage spammers and consume their time do exacerbate the problem by allowing scammers to quickly skip over savvy consumers to reach more vulnerable targets. RoboKiller's Answer Bots are specifically designed to waste spammers' time, and therefore they do protect consumers in your district (even if they don't have RoboKiller) who are less tech savvy, and are less able to protect themselves. So, encouraging those in your district to

use our service should help protect both the tech savvy and less tech savvy populations. Beyond that I do think it is important to take steps to educate your constituents about the dangers that lurk behind a ringing phone. Encouraging them not to answer unknown calls, to always demand any request for personal information in writing via certified mail, and to report any suspicious calls to government agencies is a useful effort. The best ways to do this is likely through media campaigns, public service campaigns, etc.

Thank you again,
Ethan Garr

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

May 14, 2018

Mr. Aaron Foss
Founder
Nomorobo
5507-10 Nesconet Highway, #201
Mount Sinai, NY 11766

Dear Mr. Foss:

Thank you for appearing before the Subcommittee on Digital Commerce and Consumer Protection on Friday, April 27, 2018, to testify at the hearing entitled "Do Not Call: Combating Robocalls and Caller ID Spoofing."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. To facilitate the printing of the hearing record, please respond to these questions by the close of business on Tuesday, May 29, 2018. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to ali.fulling@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Robert E. Latta
Chairman
Subcommittee on Digital Commerce
and Consumer Protection

cc: Jan Schakowsky, Ranking Member, Subcommittee on Digital Commerce and Consumer Protection

Attachment

Aaron Foss
Founder, Nomorobo
Answers to Additional Questions for the Record for the
United States House of Representatives Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection
"Do Not Call: Combating Robocalls and Caller ID Spoofing"
Hearing held on April 27, 2018

The Honorable Robert E. Latta

1. We have over 1.7 million consumers using Nomorobo on mobile and VoIP landline phones. Landline protection is free and mobile is only $1.99/month or $19.99/year.

2. To the user, after a quick installation, robocalls simply disappear. Behind the scenes, our detection algorithm is analyzing millions of calls per day to determine what phone numbers are sending unwanted robocalls. Over 1,300 new robocaller numbers are detected each day. Our full blacklist contains over 900,000 known robocallers.

3. Robocall protection begins immediately after enabling Nomorobo. On landlines, each time a robocall is intercepted, the user's phone will ring once and then stop. On mobile, after downloading and installing the app, the consumer chooses how the app handles robocalls. If they select "Block," they'll never see or hear them at all. Robocallers are sent straight to voicemail. If they select "Identify," incoming robocalls will be shown as "Nomorobo Caller ID: ● Robocaller" on the lock screen and the consumer can choose whether to answer or decline the call. Our accuracy rate is 98%, meaning that we only miss blocking 2% of all robocalls.

4. In February of 2018, Nomorobo analyzed a total of 70 million calls. 28 million robocalls were stopped, 900,000 robocalls were missed, and only 40,000 good calls were accidentally stopped. This works out to a false positive rate of 0.14%.

5.

    a. To combat robocalls and spoofing, equipment manufacturers and the consumer electronics industry can continue to add features that allow third-party developers to block and analyze robocalls. The app ecosystem, where developers create solutions that fill in missing features of the operating systems, works very well.

    b. I can't speak to any specific conversations that we've had with companies such as Apple or Google.

6.

    a. We don't share call complaint data with the FTC for its call complaint sharing initiative.

    b. We do not input the FTC's call complaint information into our proprietary solution.

    c. The faster the FTC can provide the data, the more actionable it becomes. Any delay, even just a few hours, diminishes the value of the data feed.

    d. Anecdotally, a lot of users tell us that in addition to reporting robocalls in Nomorobo, they also report it to the FTC's call complaint system.

7. There are many ways for a user to report an incorrectly labelled phone number. They can 1. Enter it in their control panel at https://www.nomorobo.com or 2. Call or text it to us at 608-371-6666 or 3. Email us at support@nomorobo.com or 4. Report it in the Nomorobo app. All reports are reviewed and researched by a customer support representative within hours of receipt.

8. We don't audio fingerprint any consumer calls. The only calls that are recorded, transcribed, or "fingerprinted" are ones that come into our company owned honeypot

phone lines. I think there's a huge privacy issue with answering consumer calls and that's why we don't do it. Consumers shouldn't have to give up privacy for protection.

The Honorable Michael C. Burges

1.

    a. I'm not familiar with the status of this Notice of Proposed Rulemaking. I do not know if it will be retroactive.

    b. On landlines, callers are always able to bypass our blocking by completing an audio CAPTCHA ("Please enter the number XX to complete your call"). On mobile, callers can always leave a voicemail if they are incorrectly blocked. In cases where a number is incorrectly blocked/labelled, there are many ways for a user to report it. They can 1. Enter it in their control panel at https://www.nomorobo.com or 2. Call or text it to us at 608-371-6666 or 3. Email us at support@nomorobo.com or 4. Report it in the Nomorobo app. All reports are reviewed and researched by a customer support representative within hours of receipt.

2. The best way to help vulnerable populations would be to have the various government and non-profit organizations encourage the use of robocall blocking services. They're a safe and effective way to stop the robocall problem.

3. Yes. I believe that businesses should be able to know if their numbers are on any robocall blacklists.

The Honorable Gus Bilirakis

1. I'm not sure if consumers that use pre-paid mobile options are any more or less vulnerable to robocalls, spoofing, or scams but I do know that they can use Nomorobo

just the same as post-paid consumers can. As long as they have an Android or iOS

smartphone, they can download and install Nomorobo directly from the applicable app

store.

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

May 14, 2018

Mr. Scott Hambuchen
Executive Vice President
Technology and Solution Development
First Orion Corp.
500 President Clinton Avenue, Suite 215
Little Rock, AR 72201

Dear Mr. Hambuchen:

Thank you for appearing before the Subcommittee on Digital Commerce and Consumer Protection on Friday, April 27, 2018, to testify at the hearing entitled "Do Not Call: Combating Robocalls and Caller ID Spoofing."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. To facilitate the printing of the hearing record, please respond to these questions by the close of business on Tuesday, May 29, 2018. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to ali.fulling@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Robert E. Latta
Chairman
Subcommittee on Digital Commerce
and Consumer Protection

cc: Jan Schakowsky, Ranking Member, Subcommittee on Digital Commerce and Consumer Protection

Attachment

First Orion Corp.

Answer to Additional Questions for the Record

The Honorable Robert E. Latta

1. **How many consumers are using your company's robocall-blocking solution? How much does your company charge for your app or service?**

As a preliminary matter, we want to clarify that call labeling, also known in the industry as "call tagging," is not the same as call blocking. As described in more detail in our written testimony First Orion's scam solutions "label" suspected fraudulent calls as "Scam Likely," and potentially unwanted, abusive, or harassing calls as "Nuisance Likely," "Telemarketer," "Survey," or other categories as appropriate. Consumers can choose to block individual calling numbers or to block whole categories of calls, such as "Scam Likely" or "Survey."

We also want to mention that we look at all calls, not just robocalls, to identify scams. Some legitimate robocalls are wanted by consumers, such as a reminder about an appointment, and some scam calls are not robocalls. We label scam calls based on many factors as described below and in our written testimony.

We have well over 15 million active users of our various mobile applications which offer a number of services described in our written testimony and in our answer to question 2 below. In addition to actual call blocking, consumers use the applications for reverse number look up and for filing complaints many of which we send onto the FTC.

Scam Likely call labeling is free, and these other services range in price from $.99 to $1.99 per month.

For T-Mobile, we label all calls we believe to be fraudulent calls "Scam Likely." This service is provided to over 55 million consumers nationwide. Less than 5% of these T-Mobile consumers have chosen to have the calls labeled Scam Likely blocked. These services are free of charge to the T-Mobile subscribers.

2. Please explain how does your robocall-blocking solution work?

We label calls through sophisticated algorithms, machine learning, and artificial intelligence, which are based on call characteristics (for example, a sudden burst of incoming calls from a previously unknown number, a high failure to ring through rate, very short duration after the call is answered), complaints and feedback from consumers about calls, research and verification processes, and dozens of other sources of data and intelligence. At some point in the future, the "attestation" status of numbers facilitated by the implementation of STIR/SHAKEN will become yet another data point in this process. No one piece or source of data ever causes a call to be labeled "Scam Likely." It is always a combination of data points. Our approach does not rely solely on using "White Lists" of legitimate callers or "Black Lists" of phone numbers of fraudsters, which scammers could easily circumvent using a variety of evolving methods to trick consumers to answer phone calls. Since spoofing allows the same phone number to be used for both legitimate wanted calls and scam calls, we must constantly refine our solution. Soon we will begin labeling individual phone calls rather than phone numbers. This means identifying anomalies in the call itself—allowing us to differentiation "good" calls from "bad" calls from the same phone number.

3. Typically, when a subscriber downloads your company's robocall-blocking app or service, or is accessed via wireline or wireless provider, what is their general experience in the next few days and weeks? How effective is the app or service in eliminating unwanted calls?

For a new T-Mobile subscriber, they will immediately begin to see the "Scam Likely" label displayed on their handsets any time they receive a call we believe is fraudulent. Our experience is that the average consumer sees Scam Likely on approximately 12% of their inbound calls. Once the choice to block such calls is made, the phone does not ring for these T-Mobile subscribers. For Android users, blocked calls appear in the subscriber's call log, but due to limitations on iOS devices, this is not possible on iPhones today.

For users of the various applications, consumers can immediately choose to block an individual phone number they do not wish to receive calls from. For other features some level of subscriber set up is required to block calls. Subscribers select from options like "Basic," "Enhanced," "Maximum" or "Custom," each with different features, before calls are blocked. Once the selection is made, the service goes into effect immediately.

Our experience is that the service is very effective eliminating the calls the consumer has chosen to eliminate.

In addition to labeling and blocking, First Orion solutions also provide enhanced CallerID information, which includes the number calling, a company name if available, a call category (e.g. Telemarketing, Survey, etc.), our scam and nuisance score, and the ability to easily file a complaint.

4. What is the false positive percentage rate of your robocall-blocking service?

Our false positive rate is well below 1%.

5. What help can the equipment manufacturers and the consumer electronics industry lend to combat robocalls and spoofing? Has your company had any conversations about adding a "block robocalls" feature to Google Android or Apple iOS so consumers who want to opt-in could have this service added in their initial settings instead of having to download an app?

While our apps provide effective call labeling and blocking functionality for millions of consumers, we believe the most effective and "future proofed" solutions must be in-network solutions (versus being driving by handsets), as with our T-Mobile services. That said, we constantly confer with industry players about additional approaches to protecting consumers.

6. Does your company share call complaint data and information with the FTC for its call complaint sharing initiative? Does your company also input the FTC's call complaint information that is shared everyday with telecommunications companies into your proprietary systems/solutions? What recommendations do you have to enhance the FTC's call complaint sharing initiative? What percentage of your subscribers have provided fraud related and call complaint information to the FTC in support of their complaint information sharing initiative?

First Orion is one of the very few commercial entities currently providing complaint data (that is information provided by our mobile subscribers via our mobile applications about unwanted and illegal calls they receive) to the FTC for enforcement purposes. We have historically provided as much as 30% of the overall complaint data received by the Consumer Sentinel Complaint Database. We estimate less than 5% of active users contribute complaint data.

We do use the FTC Do Not Call violation data that we contribute to and we also access the FCC complaint file.

We would suggest that the FTC continue to look for additional sources that can provide complaint information. We also believe that consumers should be encouraged to report scams and other illegal practices as soon as they spot them so such intelligence can be quickly included in the systems/solutions of all providers of scam blocking and identification services.

7. How does your company remediate incorrect labeling or tagging of calls and phone numbers?

Although our error rates are very low, we work hard to lower them further still. First Orion collaborates extensively with call originators and consumers to actively engage all groups to improve call labeling accuracy. As described in more detail in our written testimony consumers who use one of our applications can provide feedback about whether calls are mislabeled (either as a false positive or false negative), and we use this information to better train our analytics systems. T-Mobile customers can also provide feedback about First Orion's call labeling service through the T-Mobile website. Additionally, First Orion actively solicits feedback from call originators to reduce false positives and negatives by participating in several call originator organizations and working groups. Any report of a false positive is immediately referred to our research and validation team and any issues are typically resolved within hours if not minutes.

We also recognize that we can and should rectify any potential errors or issues that affect legitimate call originators. We've recently launched www.CallTransparency.com, which provides legitimate call originators with the opportunity to register their number-related information for free. Once both the call originator and their number information are authenticated, legitimate calls from registered numbers will not be labeled "Scam Likely".

In addition, First Orion's Perception Product, currently in beta testing, allows call originators to harness the power of our data analytics to monitor the performance and status of their outbound calling practices. For example, call originators will learn when a scammer is using one of the company's numbers to place illegally spoofed calls or when the call originator is generating significant numbers of consumer complaints. With these offerings, we strive to balance the interests of consumers and call originators alike, with a goal of helping consumers trust and appreciate their phones again.

Finally, First Orion takes other common-sense measures to ensure callers can easily and quickly resolve errors. For example, First Orion buys the ad term "Scam Likely," so consumers and call originators who may have no other context for call labeling and blocking can reach both T-Mobile's feedback page and First Orion with just a few clicks. Consumer feedback is always helpful, so we will continue to investigate ways to maximize the feedback we receive.

8. What are, if any, the privacy issues associated with the audio-fingerprinting of robocalls?

First Orion does not engage in audio fingerprinting and as such has no informed opinion on this question.

The Honorable Michael C. Burgess

1. a. Can you share the status of this Notice of Proposed Rulemaking? Will a future Rulemaking be retroactive?

Reply Comments were due on the FNPRM on February 22, 2018 with no additional action since. Though we contacted the Commission, it is their policy to not provide informal updates before taking official action.

1. b. Is there currently any way for a legitimate caller to become unblocked? If so, how is a caller evaluated for legitimacy?

Please see the answer to The Honorable Robert E. Latta Question 7.

We use various methods to evaluate legitimacy. We typically do not divulge these techniques in public so we won't help the fraudsters circumvent them. We would be happy to discuss them in more detail in a non-public setting. Finally, our systems which monitor the behavior or callers for labeling purposes also provides a good check if a fraudster should be authenticated incorrectly.

2. **How can companies increase the accessibility of resources to educate these vulnerable populations (including the elderly and those with limited English ability) on potential scams?**

Consumer education is a focus for the FTC, FCC (as well as other independent agencies dealing with specific scam activity such as the IRS) and consumer organizations such as AARP, BBB, Consumers Union and the National Consumer Law Center. Perhaps some benefit could come from a coordinated, national campaign (seat-belt campaigns among others come to mind) with these organizations in the lead.

Otherwise, First Orion has recently learned of one very effective consumer education campaign supported by Utilities United Against Scams (UUAS). UUAS is a consortium of more than 100 U.S. and Canadian electric, water, and natural gas utility companies (and their respective trade associations) dedicated to combating impostor utility scams by providing a forum for utilities and trade associations to share data and best practices and work together to implement initiatives to inform and protect customers. This is an innovative, industry-led initiative arming local utilities North America-wide with resources to educate consumers, and it has further been supported the past two years by U.S. Congressional resolutions recognizing a day in November annually as Utility Scam Awareness Day. The next annual campaign will be the week of November 11-17, 2018. UUAS has worked with the communications industry to shut down over 1,500 scammer-used toll-free numbers since March 2017 and is currently working with federal, state, and local law enforcement partners in an effort to help put an end to utility impostor scams.

3. Given the limitations of current call blocking tools and the substantial harm they can cause to businesses and consumers, do you believe that legitimate businesses need to know if their calls are being blocked?

First Orion believes that legitimate call originators should have a way to know when their calls are being blocked, but not in such a way that we alert the scammers that they have been caught. As described in our written testimony, First Orion launched www.calltransparency.com to offer call originators a way to prevent their calls from being labeled as a scam. In addition, First Orion's "Perception" Product, currently in beta testing, allows call originators to continuously monitor the performance and status of all their outbound calling practices, not just scam labeling and blocking. For example, call originators will learn when a scammer is using one of the company's numbers to place illegally spoofed calls or when the call originator is generating significant numbers of consumer complaints. With these offerings, we strive to balance the interests of consumers and call originators alike, with a goal of helping consumers trust and appreciate their phones again and helping call originators not just know when their lines are being spoofed, but when consumers view their practices as problematic.

The Honorable Gus Bilirakis

1. Are consumers who sign up for a pre-paid mobile option more or less vulnerable to robocalls, spoofing or scams? Are they able to access all of the available tools, free or for fee, if they deemed it worth the price?

Given the changes in the pre-pay demographic over the years it is difficult to say whether pre-pay consumers are more vulnerable to scams. All of our applications are available for pre-pay consumers, and pre-pay T-Mobile subscribers receive the Scam Likely service as well.

2. Can you discuss First Orion's CallTransparency.com program? As I understand it, your company created the initiative to allow legitimate callers to register and get their call labeled. Can you explain what that means?

First Orion offers www.calltransparency.com, a free registry for call originators to register their numbers as a legitimate calling party. After an authentication process, the call originators are given a report showing which numbers, if any, are currently being labeled as scams. Once registered, legitimate calls from a registered number will not be labeled as scam by First Orion; individual calls from a registered number will only be labeled as scams in the event we see strong and up-to-date indicia that a scammer has hijacked (spoofed) the number. These services eliminate the requirement for a tone indicating calls are being blocked (which some call originators have asked for) and which alerts the scammers they have been caught as well as the need for call originators to constantly check their numbers to watch for a scam label via an API or a query.

○