S. HRG. 118–606

PROTECTING AMERICANS FROM ROBOCALLS

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMUNICATIONS, MEDIA, AND BROADBAND

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

OCTOBER 24, 2023

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

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

U.S. GOVERNMENT PUBLISHING OFFICE

59–860 PDF WASHINGTON : 2025

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

MARIA CANTWELL, Washington, *Chair*

AMY KLOBUCHAR, Minnesota	TED CRUZ, Texas, *Ranking*
BRIAN SCHATZ, Hawaii	JOHN THUNE, South Dakota
EDWARD MARKEY, Massachusetts	ROGER WICKER, Mississippi
GARY PETERS, Michigan	DEB FISCHER, Nebraska
TAMMY BALDWIN, Wisconsin	JERRY MORAN, Kansas
TAMMY DUCKWORTH, Illinois	DAN SULLIVAN, Alaska
JON TESTER, Montana	MARSHA BLACKBURN, Tennessee
KYRSTEN SINEMA, Arizona	TODD YOUNG, Indiana
JACKY ROSEN, Nevada	TED BUDD, North Carolina
BEN RAY LUJÁN, New Mexico	ERIC SCHMITT, Missouri
JOHN HICKENLOOPER, Colorado	J. D. VANCE, Ohio
RAPHAEL WARNOCK, Georgia	SHELLEY MOORE CAPITO, West Virginia
PETER WELCH, Vermont	CYNTHIA LUMMIS, Wyoming

LILA HARPER HELMS, *Staff Director*
MELISSA PORTER, *Deputy Staff Director*
JONATHAN HALE, *General Counsel*
BRAD GRANTZ, *Republican Staff Director*
NICOLE CHRISTUS, *Republican Deputy Staff Director*
LIAM MCKENNA, *General Counsel*

SUBCOMMITTEE ON COMMUNICATIONS, MEDIA, AND BROADBAND

BEN RAY LUJÁN, New Mexico, *Chair*	JOHN THUNE, South Dakota, *Ranking*
AMY KLOBUCHAR, Minnesota	ROGER WICKER, Mississippi
BRIAN SCHATZ, Hawaii	DEB FISCHER, Nebraska
EDWARD MARKEY, Massachusetts	JERRY MORAN, Kansas
GARY PETERS, Michigan	DAN SULLIVAN, Alaska
TAMMY BALDWIN, Wisconsin	MARSHA BLACKBURN, Tennessee
TAMMY DUCKWORTH, Illinois	TODD YOUNG, Indiana
JON TESTER, Montana	TED BUDD, North Carolina
KYRSTEN SINEMA, Arizona	ERIC SCHMITT, Missouri
JACKY ROSEN, Nevada	J. D. VANCE, Ohio
JOHN HICKENLOOPER, Colorado	SHELLEY MOORE CAPITO, West Virginia
RAPHAEL WARNOCK, Georgia	CYNTHIA LUMMIS, Wyoming
PETER WELCH, Vermont	

CONTENTS

WITNESSES

APPENDIX

PROTECTING AMERICANS FROM ROBOCALLS

TUESDAY, OCTOBER 24, 2023

U.S. SENATE,
SUBCOMMITTEE ON COMMUNICATIONS, MEDIA, AND BROADBAND,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:03 a.m., in room SR–253, Russell Senate Office Building, Hon. Ben Ray Luján, Chairman of the Subcommittee, presiding.

Present: Senators Luján [presiding], Klobuchar, Markey, Peters, Tester, Rosen, Hickenlooper, Welch, Fischer, Budd, and Vance.

OPENING STATEMENT OF HON. BEN RAY LUJÁN, U.S. SENATOR FROM NEW MEXICO

Senator LUJÁN. [Technical problems]—committee to order. I want to thank everyone for being here for a hearing on "Protecting Americans from Robocalls". And first of all, I wanted to thank Ranking Member Thune for working with me and my staff.

I want to thank his team. And I especially wanted to thank Senator Fischer for being here with us, as she always is, but especially to serve in an important role today as well. So, I want to thank you, Senator Fischer, for joining us to preside today.

Thank you so very much. And today, we will hear from expert witnesses on protecting our constituents from the growing number of fraudulent and illegal robocalls and robotexts. Every month, Americans receive roughly 1.5 billion to 3 billion scam calls and likely illegal telemarketing calls.

This is an issue that I am confident everyone in the room has dealt with. For those of you that have your phones on, I am sure you are going to receive robocalls and robotexts that are predatory even during this hearing, and I would not be surprised if we did as well.

Robocalls, they interrupt sleep if you are not putting your phones in some privacy mode or sleep mode or turning them off themselves. They interrupt time with friends and family, and as I said, even during hearings, I won't be surprised if they came up.

So, if they do, feel free to hold your phone up and share with the rest of America what is happening while we are in this room. Robocalls have eroded trust in our Nation's communications networks. I know many in my family, including myself, that you will look at the phone now and you are not sure where it is coming from.

And some of the phone providers are putting scam alerts or maybe it is some other call, and folks will look at their device and they will drop it down as well. Many have become subject to those phishing attacks from those robotexts as well, which are costing the American people billions of dollars.

In 1991, Congress passed the Telephone Consumer Protection Act, the TCPA, and more recently, the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, which—acronym is TRACED. It was back in 2019. These two laws each protect Americans from predatory and unsolicited robocalls and robotexts, giving Federal agencies the tools to fight back.

And in some ways, the TCPA and TRACED, as they were implemented, the number of unsolicited and illegal telemarketing calls has decreased. Do not call complaints at the FCC have reduced as well, not entirely, but by some numbers.

And the Federal Communications Commission has issued 500 million enforcement actions against illegal robocalls over the last 12 months. The FCC has empowered the industry Traceback Group and phone companies to block, by default, illegal or unwanted calls based on reasonable evidence.

And the Federal Communications Commission provided a statement for today's hearing. And without objection, I would like to enter it into the record. We will enter that.

[The information referred to follows:]

FEDERAL COMMUNICATIONS COMMISSION
Washington, DC, October 23, 2023

Hon. BEN RAY LUJÁN,
Chairman,
Subcommittee on Communications,
Media, and Broadband,
Washington, DC.

Hon. JOHN THUNE,
Ranking Member,
Subcommittee on Communications,
Media, and Broadband,
Washington, DC.

Dear Chairman Luján and Ranking Member Thune:

Thank you for the opportunity to submit a statement addressing the ongoing work of the Federal Communications Commission's Enforcement Bureau to combat illegal robocalls and scam texts. Protecting consumers from fraud and unwanted communications is a top consumer protection priority for the Commission and the Enforcement Bureau. The Commission is grateful for the continuing support of the Subcommittee on Communications, Media, and Broadband. Below, I outline the Commission's recent enforcement efforts against illegal robocalls and ways the Commission is modernizing its approach to enforcement. Lastly, I identify where Chairwoman Jessica Rosenworcel has called for new legislation to address statutory gaps that are leaving consumers vulnerable.

Recent Enforcement Activities

In our ongoing effort and commitment to put a stop to illegal robocalls, the Commission has ordered substantial penalties against bad actors, acted swiftly and repeatedly to disrupt illegal traffic, and cracked down on providers who have failed to implement sufficient robocall mitigation plans. This calendar year alone, the Commission has already issued four orders imposing more than $500 million in fines against robocallers. In parallel, the Commission has had significant success blocking illegal robocalls before they ever reach consumers. After identifying a non-compliant gateway or originating provider responsible for facilitating bad traffic, the Commission has permitted or ordered downstream providers to block the traffic from that non-compliant provider—thereby stopping the robocalls immediately. Further, under the Commission's current rules, all providers in the potential path of a call are required to implement a robocall mitigation plan that includes reasonable steps to avoid originating, carrying, or processing illegal robocall traffic, and file that plan in the Robocall Mitigation Database (RMD). The Commission has issued over 20 notices or show cause orders threatening non-compliant providers with removal from the RMD. This is a significant consequence, as downstream providers

may not accept traffic from any provider that is required to file in the RMD and has been removed due to noncompliance with the Commission's rules. Our evolving, multi-pronged approach has resulted in an over 20 percent drop in illegal robocalls since last year, according to one study.[1] But the Commission's work is not done. Going forward we intend to continue the battle against robocalls as well as pioneer enforcement against robotexts.

To strengthen its investigative and enforcement efforts, the Commission has continued to expand its partnerships with state, federal, and international regulatory and law enforcement partners. The Commission now has memoranda of understanding with attorneys general in 47 states, the District of Columbia, and Guam, which allows the Enforcement Bureau and its counterparties to facilitate information sharing and investigative cooperation more easily. The Commission also renewed its memorandum of understanding between international regulatory and law enforcement authorities that are members of the Unsolicited Communications Enforcement Network (UCENet). Collectively, these memoranda aim to promote domestic and cross-border collaboration to combat unsolicited communications, including e-mail and text spam, scams, and illegal telemarketing. These relationships matter. To point to just one example this year, our collaboration with the Ohio Attorney General's Office led to a record-breaking penalty of nearly $300,000,000 ordered against one of the worst robocalling schemes inflicted on U.S. consumers.

The Commission also engages directly with consumers and the general public in a variety of ways to increase consumer and industry awareness. In advance of the Supreme Court's ruling pertaining to student loan debt in June, the Commission worked with multiple attorneys general and the U.S. Department of Education to warn students about potential scams looking to take advantage of any confusion stemming from the ruling. The Commission also now publishes certain traceback data, *i.e.,* information pertaining to calls reported as potentially illegal, including the source of those calls. The Commission also closely monitors and investigates complaints by consumers and small businesses.

Modernizing Enforcement Methods

Many of these successful enforcement efforts would not have been possible without the passage of the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, which led to two key developments. First, the TRACED Act no longer required the Commission to issue citations for the bulk of robocall violations, and instead allowed the Commission to move immediately to forfeiture proceedings. The result was record-breaking fines against the worst bad actors in the industry. Second, the TRACED Act required the FCC to mandate adoption of the STIR/SHAKEN caller identification framework, which enables phone companies to verify that the caller ID information transmitted with a call matches the caller's real phone number. Among other initiatives undertaken to meet this mandate, the FCC launched the RMD to monitor compliance. As discussed above, removal of providers from the RMD who fall short of their obligations to protect consumers is a devastating consequence.

The Commission is currently engaged in discussions with the Treasury Department, including with the Financial Crimes Enforcement Network (FinCEN), to provide the Commission's Enforcement Bureau with access to vital information collected pursuant to the Bank Secrecy Act (BSA). Although our efforts with Treasury are ongoing, we are able to note that these efforts have been collaborative, and our Treasury colleagues have been very constructive in their engagement with us. BSA evidence is critical to identify the financing used to support the entities using U.S. communications networks to commit fraud targeting consumers, as well as the various methods in which bad actors are laundering and exfiltrating their illicit proceeds. Supplementing our current authorities with BSA information will further assist the Enforcement Bureau in identifying and going after the worst actors while limiting their ability to reconfigure and use financial resources to further their schemes.

Proposed Policy Changes

The Chairwoman has identified two additional fronts where Congress can help the Commission's enforcement efforts. First, Congress could help the Commission protect consumers by broadening the definition of "automatic telephone dialing system" in the Telephone Consumer Protection Act (TCPA). The TCPA broadly protects consumers from calls made using an "automatic telephone dialing system or an artifi-

[1] *See* Robokiller, The Robokiller Phone Scam Report 2023 Mid-Year Insights & Analysis at 10 (2023), *https://assets.website-files.com/61f9a8793a878d7f71c5505d/64ca6ccf1f5e962fae3e55e3_Robokiller%20Mid-Year%20Report%202023.pdf.*

cial or prerecorded voice." The TCPA's definition of automatic telephone dialing system has been unaltered since 1991 and needs adjustments to keep pace with the way technology has developed over the last thirty years. Further, in *Facebook v. Duguid,* the Supreme Court narrowly interpreted "automatic telephone dialing system" to mean equipment that stores or generates numbers randomly or sequentially.

Consequently, equipment that simply stores non-random and non-sequential lists of numbers may fall outside the statute. This interpretation makes it harder for the Commission to regulate bad actors manipulating technology to reach massive volumes of consumers, particularly with regards to sending unwanted text messages.

Second, the Chairwoman has explained that Congress could help the Commission protect consumers by giving the Commission the authority to collect the fines it imposes against bad actors responsible for illegal robocalls. The Commission has the authority to issue a Forfeiture Order for violations of the Communications Act and its rules, but it lacks the authority to pursue collection without involvement from the Department of Justice (DOJ). Since 2018, the Commission has referred eight robocalling forfeiture orders to the DOJ for collection, of which the DOJ is currently pursuing collection for two. The result is that significant sums of ill-gotten gains are potentially left in the pockets of bad actors. With its own authority to collect its fines, the Commission would pursue these cases promptly and aggressively.

Thank you for the opportunity to submit written testimony about this important consumer protection matter.

Sincerely,

LOYAAN EGAL,
Chief, Enforcement Bureau,
Federal Communications Commission.

Senator LUJÁN. However, it is important that we recognize that robocalls and robotexts are not just a nuisance. Scammers use our telecom networks to defraud Americans out of an estimated $39 billion.

Now, that was just in 2022 alone. That is roughly enough money to provide affordable broadband to the current 21 million households enrolled in the Affordable Connectivity Program for 8 years. I hope we understand the magnitude of what that $39 billion year to year means.

Scammers and fly by night companies are stealing American families' hard earned dollars using our telecom networks to do so, and they don't face any consequences. The FCC levies fines, but fines go uncollected, and the company dissolves and moves assets elsewhere.

Congress must empower our regulators and enforcement agencies to ensure that when an individual or company breaks the law, they are held to account. Part of the reason these scammers are so effective at tricking consumers and evading enforcement is that the technology is constantly evolving.

We will hear testimony that suggests consumer consent for telemarketing is increasingly falsified. Automated bots and other artificial intelligence systems are using public data to consent on behalf of a consumer for calls they never asked for and do not want.

Automated robocalls and robots are using chat bots and generative artificial intelligence to impersonate a real life person, lulling the recipient into a false sense of security by mimicking voices and mannerisms.

In the most frightening examples, bad actors are playing on our emotions and impersonating loved ones in distress. Earlier this year in the Senate Human Rights subcommittee, Senator Ossoff and Ranking Member Blackburn heard testimony from Jennifer DeStefano of Arizona who was the victim of a scam call impersonating her daughter.

And without objection, I would like to enter her testimony into the record for today's hearing. Hearing none, it is entered.

[The information referred to follows:]

PREPARED STATEMENT OF JENNIFER DESTEFANO

ABUSES OF ARTIFICIAL INTELLIGENCE

JUNE 13, 2023

Good Afternoon Senators, it is my great honor to speak with you today and to share my experience of how artificial intelligence is being weaponized to not only invoke fear and terror in the American public, but in the global community at large as it capitalizes on and redefines what we have known to be as "familiar". I would like to take this moment to thank Senator Ossoff for inviting me to be here today. I would also like to thank Senator Blackburn for your concern on this ever evolving topic and community threat. AI is revolutionizing and unraveling the very foundation of our social fabric by creating doubt and fear in what was once never questioned, the sound of a loved one's voice.

What is "familiar"? How many times have you received a phone call from your child and asked them to verify who is calling? How many times has a loved one reached out to you in despair and you stopped them to validate their identity? Did you hang up on them? Did you require to call them back to make sure you are speaking to the correct person? The answer is more than likely, never. Never have you stopped your loved one and questioned if the voice you are speaking with is really them. The sound of a loved one's voice is often never questioned. It is designed by nature, it is designed by God, as a unique identity, as unique as a fingerprint. This familiar identity is how a mother knows if it's her child crying in a room and it is how a newborn child instantly recognizes their mother.

It was a typical Friday afternoon for our family kicking off a weekend of races and rehearsals that often divide our family across the state. As the parents of four children close in age, we tend to have to "divide and conquer". My husband was with our older daughter Brie and our youngest son in Northern Arizona training for ski races. I was with our older son and youngest daughter Aubrey in the valley as she had rehearsal. Ski racing is a high risk sport and Brie had not raced in years. At age 15, she promised me she would take it easy and not hurt herself by pushing to hard. When I first received a call from an "unknown" number upon exiting my car, I was going to ignore it. On the final ring I chose to answer as "unknown" calls can often be a doctor or a hospital. I answered the phone " Hello", on the other end was our daughter Briana sobbing and crying saying "mom". At first I thought nothing of it, she had run into race gates and bruised herself before, not to worry. I casually asked her what happened as I had her on speaker walking through the parking lot to meet her sister. Briana continued with "mom, I messed up" with more crying and sobbing. Not thinking twice, I asked her again, "ok what happened?" Suddenly a man's voice barked at her to "lay down and put your head back". At that moment I started to panic. My concern escalated and I demanded to know what was going on, but nothing could have prepared me for her response. "MOM THESE BAD MEN HAVE ME, HELP ME, HELP ME!!" She begged and pleaded as the phone was taken from her. A threatening and vulgar man took over the call "Listen here, I have your daughter, you tell anyone, you call the cops, I am going to pump her stomach so full of drugs, I am going to have my way with her, drop her in Mexico and you'll never see her again!" all the while Briana was in the background desperately pleading "mom help me!!!"

With my shaking hand on the door handle to the studio, I put the man on mute, flung open the door and started screaming for help. The next few minutes were a parent's worst nightmare. I was fortunate to have a few moms at the studio who surrounded me, hearing all of the vulgar threats the man was making. One mom ran outside and called 911. Our 13 year old daughter Aubrey stood paralyzed in fear. I needed her help, her sister was in trouble and we had to find her. Another mom ran to her to aid as they started making calls to her dad, her brothers, anyone that could help us figure out what happened to Brie. The kidnapper demanded a million dollars. That was not possible and so the kidnapper decided on $50,000, in cash. At this moment, the mom who called 911 came inside and shared with me that 911 was familiar with an AI scam where they can replicate your loved one's voice. I didn't believe this was a scam. It wasn't just Brie's voice, it was her cries, it was her sobs that were unique to her. It wasn't possible to fake that I protested. She told me that AI can also replicate inflection and emotion. That gave me a little

hope but still was not enough. I proceeded with the negotiations. I asked for wiring instructions and routing numbers for the $50,000 but was refused. "Oh no" the man demanded, "that's traceable, that's not how this is going to go down. We are going to come pick you up!" "What?" I shouted, "You will agree to being picked up in a white van, with a bag over your head so you don't know where we are taking you. You better have all $50k in cash otherwise both you and your daughter are dead! If you don't agree to this, you will never see your daughter again!" he screamed. I had to stall, I asked the mom on the call with 911 to send police, I needed to stall until I had police with me. Then the mom who was making calls with Aubrey was able to get my husband on the phone. He frantically located Brie resting safely in bed.

Brie had no idea what was happening. As I was negotiating the arrangements of the abduction of myself to save my daughter, the mom came to me and told me she found Brie and that she was safe. I didn't believe her. How could she be safe with her father and yet be in the possession of kidnappers? It was not making any sense. I had to speak to Brie. I could not believe she was safe until I heard her voice say she was. I asked her over and over again if it was really her, if she was really safe, again, is this really Brie, are you sure you are really safe?! My mind was whirling. I do not remember how many times I needed reassurance, but when I finally took hold of the fact she was safe, I was furious. I lashed at the men for such a horrible attempt to scam and extort money. To go so far as to fake my daughter's kidnapping was beyond the lowest of the low for money. They continued to threaten to kill Brie. I made a promise that I was going to stop them, that not only were they never going to hurt my daughter, but that they were not going to continue to harm others with their scheme. After I hung up, I collapsed to the floor in tears of relief. When I called the police to pursue the matter, unfortunately I was met with this is a prank call. That it happens often and that I am probably not in harm's way (although not a guarantee). I was offered to have a police officer call me from another "unknown" number if it would make me feel better as law enforcement numbers are also blocked. That certainly did not make me feel better. Bottom line was no actual crime had been committed, no one was physically kidnapped, and no money was transferred, period, the end.

But that wasn't the end, it couldn't be the end. If it was the end, then this nightmare would never stop. I stayed up all night paralyzed in fear. Do they know where I am? Do they know where my daughter is? How did they get her voice? How did they get her crying, her sobs that are unique to her. She is not a very public person. Are we being cyber stalked? Targeted? So many questions that I could not leave unanswered, so I turned to our community and the response was overwhelming!

Friends and neighbors came out of the woodwork with their stories. Kidnapping phone calls coming from their children's phones, bags of money being driven halfway to Mexico, even voices of young children nowhere to be found on social media and who do not have phones, the stories kept pouring in. Even my own mother received a call with my brother's voice claiming to be in an accident and needing money for the hospital bill! My mother is hard of hearing and quite spunky. After having the caller repeat the request multiple times, she realized the language used was not something my brother would say. She told the caller to call their real mother and hung up. The common response the victims received from authorities was that nothing could be done. In fact, one mother I know personally shared with me how she was even mocked by her son's school and security officer. She called his school frantically trying to locate her son when she received a call from him that he had been kidnapped. He even used his unique nickname during the call to self identify. Fortunately he was safe in class and she was told "this happens all the time" as her fear was dismissed. "It's the most frustrating, maddening, scary and invaded I've felt . . . my fear is that it is only a matter of time until someone actually follows through with the threat", she told me as she has been living in fear and concern for her son's safety ever sense.

Money scams have been around for thousands of years. We have all heard of "snake oil" and remember the days of "swap land" sold as paradise in Florida. This is entirely different. This is terrorizing with lasting post traumatic stress. Even months later, sharing the story shakes me to my core. It was my daughter's voice. It was her cries, her sobs. It was the way she spoke. I will never be able to shake that voice out of mind. It's every parents' worst nightmare to hear your child pleading with fear and pain, knowing that they are being harmed and you are helpless and desperate. The longer this form of terror remains unpunishable, the farther and more egregious it will become. The thought crossed my mind before I hung on the "kidnappers" to follow through with the physical abduction of me. Was that what would it take to bring an end to this? Was that what it would take in order to have a pursuable criminal offense?

As our world moves at a lightning fast pace, the human element of familiarity that lays foundation to our social fabric of what is "known" and what is "truth", is being revolutionized with Artificial Intelligence. Some for good, and some for evil. No longer can we trust "seeing is believing", "I heard it with my own ears" nor even the sound of our own child's voice. This concept redefines and rewrites what the very meaning of "familiarity" means. Familiarity is defined as "the quality of being well known or knowledge of something" and further is defined as "relaxed friendliness or intimacy between people." Familiar and family share the root word "Famil" which establishes strength of a relationship between one person and another. I ask you, when your mother calls, are you going to hang up and call her back to make sure it is really her? When your child calls you in need of help, will you disconnect the call and say I don't believe its really you? Is this our new norm? Is this the future we are creating by enabling this abuse of Artificial Intelligence without consequence?

I want to thank you for your time and attention today. Congress has a large and looming task ahead. How do we move forward as a community with this haunting reality that is plaguing us? If left uncontrolled, unguarded and without consequence, it will rewrite our understanding and perception what is and what is not truth. It will erode our sense of "familiar" as it corrodes our confidence in what is real and what is not. This is a non-partisan matter and I have seen the hands reach across the aisle in unified concern. That gives me great hope. How to contain the ever evolving Artificial Intelligence and its unknowns, is not an easy task. My sincere thanks and humble appreciation for your time and attention today. I thank all of you, and especially Senator Ossoff and Congress at large, for tirelessly taking action to keep our community and world safe from the hands of evil. I am one person, one story, but I am not the only one and I certainly will not be the last one unless action is taken. I wish you God's speed.

Senator LUJÁN. Now, she testified, "AI is revolutionizing and unraveling the very foundation of our social fabric by creating doubt and fear in what was once never questioned, the sound of a loved one's voice."

This hearing will examine how robocallers are evading enforcement, consider public, private efforts to combat illegal robocalls, unravel how new and evolving technologies are changing the landscape, and investigate what next steps are needed to protect Americans from fraudulent and illegal text messages and calls.

I am very excited that we have the panel that we have with us today. I will introduce each of you momentarily. But first, I want to recognize a friend and a leader that is with us today, and I want to turn this over to Ranking Member Fischer for her opening comments.

STATEMENT OF HON. DEB FISCHER, U.S. SENATOR FROM NEBRASKA

Senator FISCHER. Good morning, and thank you, Chairman Luján, for holding this hearing. The persistent issue of illegal robocalls has been a longstanding concern of mine. Nationwide, illegal and spoofed robocalls continue to be the number one consumer complaint. I want to ensure that we have the right tools in place to protect consumers from these calls that prey on them.

As we all know, our phones give us connection to the world around us. Whether it is calling family, friends, or colleagues, scheduling appointments, or summoning emergency services, they are integrated into our daily lives. Our phone numbers are a very personal part of our identities as well.

We use them to verify who we are, and we hold on to them for decades, sometimes for a lifetime. But as we know too well, this allows scammers to reach directly into our homes and into our pock-

ets. Bad actors are increasingly savvy in the technologies they use to defraud consumers.

This can result in devastating financial losses. Criminals are engaging in more targeted calls and impersonating businesses like banks to steal personal data or commit financial fraud. Phone scams are still yielding the highest reported fraud losses per person, despite the rapid growth of scammers on social media platforms. In fact, fraud losses due to phone scams are higher than ever.

According to a recent report, over 68 million Americans lost approximately $40 billion to phone scams in 2021 alone. In many ways, it feels like we have had this conversation so many times over so many years. But crucially, in 2019, Congress passed the TRACED Act to put wide ranging solutions in motion that would reduce illegal robocalls.

I commend my colleague, Senator Thune, for leading this legislation, and I was glad to be a co-sponsor of it. Previously, I also led the Spoofing Prevention Act with Senator Bill Nelson, which passed into law in 2018.

This law was a foundational effort to increase penalties and boost enforcement tools that fight illegal spoofing. Deterrence through fines for illegal robocall activities is a key part of cracking down on nuisance calls that endanger consumers.

On this front, Federal agencies, particularly the Justice Department, must improve how they work together to ensure that unpaid fines are collected. There are no silver bullets to eradicate the scourge of illegal scam calls and texts.

Lawmakers have to remain vigilant on and monitor how illegal robocall schemes are evolving. We must be able to empower consumers with the knowledge of who is actually calling them and the ability to block illegal callers. We all share the goal of being able to pick up our phone safely, trusting that we know who is going to be on the other end of the line, but we are not there just yet.

The industry has made commendable efforts to reduce the prevalence of these illegal calls, including through advancements in call author—to authorize them, and trace back technology. New statistics from the federally designated Traceback Consortium, ITC, indicate that certain common robocall scams have started to decline over the last couple of years.

Continuing this trend will take the united cooperation of all voice service providers. As lawmakers, we need to maintain this momentum and ensure that traceback efforts are fully supported. I urge the FCC to spend its time and resources to prevent genuine criminal activity and create meaningful, safe harbors for businesses acting in good faith compliance with the law.

I look forward to hearing from today's witnesses about where we are in this effort and where additional assistance may be needed. Thank you for being here and thank you, Chairman Luján.

Senator LUJÁN. Thank you, Senator Fischer. And I want to thank you again for being with us today. But I want to commend you for your leadership in so many ways, but especially in this case, when it comes to robocalls and robotexts, and what you have been doing to work, to bring support to the American people.

So, thank you so very much for that. As I introduce the panel, we will—after the introduction, we will then hear from Ms. Saunders. But Ms. Saunders, who is the Senior Attorney from the National Consumer Law Center, thank you so much for being with us today.

Ms. Megan Brown, a member of the United States Chamber of Commerce's Cybersecurity Leadership Council. And partner, Wiley Rein, I believe, is with us as well—Wiley. Miss—Mr. Josh Burco—Bercu, like the city.

I appreciate that, Josh. Mr. Josh Bercu, Executive Director, Industry Traceback Group and Vice President of Policy and Advocacy for USTelecom. Thank you so much as well. And Mr. Mike Rudolph, the Chief Technology Officer from YouMail.

Thank you so much for being with us today. Ms. Saunders, the floor is yours for your opening statement for five minutes.

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

Ms. SAUNDERS. [Technical problems]—Senator Fischer, I appreciate the opportunity to testify today on what needs to be done to protect Americans from robocalls. I provide my testimony today on behalf of the low income clients of the National Consumer Law Center and the Consumer Federation of America.

The current regulatory structure allows criminals access to Americans' wallets. As you have cited, billions of dollars are stolen every year through scams executed over this Nation's telephones.

At the same time, the combination of scam calls, along with the onslaught of illegal and unwanted telemarketing calls, have damaged our trust in our phones and made it more difficult for legitimate wanted messages to reach us. The FCC has been trying to solve the problem, but to date its methods have not succeeded.

In my testimony, you can see a graph of the number of robocalls, and telemarketing calls and scam calls over the years, and it looks like that, unfortunately, we are about today where we were in 2019 in terms of the combined number of calls.

But either the FCC does not have sufficient legal tools to stop the calls, or it has not yet determined how to employ those—deploy those tools effectively. The Commission has issued numerous regulations to implement the TRACED Act, brought multiple enforcement actions against scam callers and their complicit voice service providers, yet the numbers of calls and the losses to Americans keep—are continuing.

The problem is that complicit voice service providers responsible for these calls are making money for transmitting them. And as FCC Commissioner Geoffrey Starks said, "illegal robocalls will continue so long as those initiating and facilitating them can get away with it and profit from it."

To eliminate these calls, there must be incentives for compliance, which there are not currently. We believe that the calls can be dramatically reduced, but the resolution requires a shift in emphasis by the FCC.

The primary goal of the FCC's actions should be to protect the Nation's telephone subscribers from the scam calls that are stealing billions of dollars. To do that requires a change, from ensuring

that calls can be completed and protecting voice service providers' access to the telephone numbers, telephone network toward shielding consumers from these illegal calls.

If the FCC were to adopt a system under which it quickly suspends the ability of a voice service provider to participate in the network once that provider is determined to be a repeat offender, we think that would be a magic bullet.

This is along the lines of the temporary restraining order procedure established in the Federal rules of civil procedure. There are procedures that can be used that we think would change the incentive structure and actually cause a reduction in the calls. Additionally, the FCC's current regulations prohibit telemarketers from calling our phones without express written consent.

Telemarketers routinely ignore the specific requirements of these regulations and make about a billion illegal telemarketing calls every month. Then they defend themselves from Government and private enforcement by relying on specious consent agreements that were either completely fabricated or based on supposed consent agreements, sold and resold, and sold again by lead generators.

The FCC could actually eliminate this entire business model by simply reiterating its current regulations. Instead, unfortunately, it has proposed new regulations that are less protective of consumers.

In a nutshell, we believe that the FCC could eliminate most of these illegal calls by changing their current emphasis. In a civilization in which we can take pictures of Saturn's rings, the failure to solve this problem is not a matter of technology. It is a question of whether the people in power actually want to solve it.

Thank you very much.

[The prepared statement of Ms. Saunders follows:]

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

Chairman Luján, Senator Thune, and Members of the Committee, I appreciate the opportunity to testify today on what needs to be done to protect Americans from robocalls. I provide my testimony here today on behalf of the low-income clients of the *National Consumer Law Center (NCLC),* and the *Consumer Federation of America.*[1]

The current regulatory structure allows criminals access to Americans' wallets: billions of dollars are stolen every year through scams executed over this Nation's telephone lines.[2] At the same time, the combination of the scam calls along with the onslaught of unwanted—and mostly illegal—telemarketing calls and texts damages our trust in our phones and makes it more difficult for important messages from health care providers and other legitimate callers to get through.

The Federal Communications Commission (FCC or Commission) has been trying to address the problems, but, to date, its methods have not succeeded in achieving a meaningful reduction in these unwanted and illegal calls. Either the FCC does not have sufficient legal tools to stop these unwanted and illegal calls, or it has not yet determined how to deploy those tools effectively. In *Section I,* we describe the magnitude of the onslaught of the scam and illegal telemarketing calls, and how the

[1] This testimony was written with the substantial assistance of Chris Frascella, Counsel at the Electronic Privacy Information Center, and Carolyn Carter, Deputy Director, National Consumer Law Center.

[2] *See* National Consumer Law Center and Electronic Privacy Information Center, *Scam Robocalls: Telecom Providers Profit* (June 1, 2022), available at *https://www.nclc.org/resources/scam-robocalls-telecom-providers-profit/ [hereinafter Scam Robocalls report].* This report also explains how scam calls are impacting American subscribers, the mechanics of the communications system in the U.S., how the current system facilitates the transmission of illegal calls, and our recommendations to resolve the problem.

problems caused by these calls have not significantly abated. We note that the numbers of these calls have remained high, despite the dozens of new regulations and rulings issued by the Commission to deploy the STIR–SHAKEN caller-ID authentication technology[3] and implement other mandates of the TRACED Act passed by Congress in 2019,[4] and the enforcement actions it has brought against VoIP providers and illegal callers.[5]

In *Section II,* we explain that we believe that these scam and illegal telemarketing calls *can* be dramatically reduced. But the resolution requires a shift in emphasis by the FCC. The primary goal of the FCC's actions should be to protect the Nation's telephone subscribers from the scam calls that are stealing tens of billions of dollars from them. To do that requires a change from ensuring that calls be completed and protecting voice service providers' access to the telephone network toward shielding consumers from these illegal calls. We believe the number of illegal calls would be significantly reduced if *the FCC were to adopt a system of swiftly suspending the ability of complicit providers to transmit illegal calls after they has been notified of previous illegal transmissions.*

In *Section III, we* explain our advocacy before the Commission to encourage it to issue guidance that will radically reduce the number of illegal telemarketing calls.

Finally, *Section IV* describes a methodology that would provide legal callers—such as health care providers, callers with fraud alerts, and those with payment reminders—a way to ensure that their calls are completed and that would also facilitate the blocking of the illegal calls.

I. Illegal and unwanted scam and telemarketing calls persist, despite FCC efforts.

The unrelenting onslaught of unwanted and illegal calls and texts to American telephone lines illustrates that more aggressive measures must be employed to stop them. In recent years, the combined number of scam and likely illegal telemarketing calls made every month to American telephone lines has ranged from *1.5 to 3.3 billion every month,* with little change from year to year.[6]

While the FCC and the private Industry Traceback Group (ITG)[7] have removed hundreds of offending callers from the network—including progress on scam robocalls regarding car warranties and student loan debt relief[8]—the raw number of illegal calls has remained relatively steady. This illustrates that, even as one scam or telemarketing caller or complicit provider is removed from the network, another quickly steps into its place.

Moreover, because of the complete lack of meaningful caller ID used by these callers, it remains effectively impossible for consumers to determine the difference between scam calls and unwanted spam telemarketing calls on the one hand, and legitimate calls on the other hand. Both types of unwanted calls continue to flood the system, and they all purport to be local. As it is highly doubtful that consumers have consented to receive over a billion telemarketing calls every month, most are

---

[3] *See* Federal Commc'ns Comm'n, Combating Spoofed Robocalls with Caller ID Authentication, available at *https://www.fcc.gov/call-authentication*

[4] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, Pub. L. No. 116–105, 133 Stat. 3274 (2019).

[5] *See In re* Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor, Seventh Report and Order, Eighth Further Notice of Proposed Rulemaking and Third Notice of Inquiry, CG Docket No. 17–59, WC Docket No. 17–97, at ¶¶6 to 64. (Rel. May 19, 2023), available at *https://docs.fcc.gov/public/ attachments/FCC-23-37A1.pdf* [hereinafter FNPRM].

[6] *Scam Robocalls report, supra note 2, at 6* (noting annual scam robocall volumes between 20 billion and 25 billion from 2019–2021). *See* Total National Robocalls chart, *infra.*

[7] The ITG, run by USTelcom/The Broadband Association, is designated by the FCC to determine the source of illegal calls. "The origination, delivery, and termination of robocalls involves numerous voice service providers in a complex ecosystem. Using a secure traceback portal developed by the ITG, suspected illegal robocalls are traced systematically back through various networks until the ITG identifies the originator of the suspicious calls, where the calls entered the United States if internationally originated, and often the identity of the calling party. The ITG traces the call back from the recipient to the caller—usually routing through four or more, or sometimes as many as nine or ten service providers (or "hops") across the globe." Industry Traceback Group, How a Traceback Works, available at *https://tracebacks.org/for-government/*

.

[8] *See* Press Release, Federal Commc'ns Comm'n, FCC & State Attorneys General Warn Consumers of Increased Risk of Student Loan Debt Scam Robocalls and Robotexts (June 30, 2023, available at *https://www.fcc.gov/document/fcc-state-ags-warn-student-loan-debt-scam-robocalls-robotexts;* Industry Traceback Group, ITG 2022 Year-In-Review: State of Industry Traceback, available at *https://tracebacks.org/wp-content/uploads/2023/03/ITG-2022-Year-in-Review-State-of-Industry-Traceback.pdf* ("Over 500 offending callers kicked off the network. Terminated callers responsible for approximately 32 million daily illegal robocalls.").

likely illegal. The dark blue area on the chart below shows the combined volume of both scam and telemarketing calls.[9]

Americans continue to lose vast sums to scam calls and texts. The Harris Poll/TrueCaller survey found that the number of Americans who lost money through telephone scams continued to escalate in 2022, increasing from 59 million people suffering these losses in 2021 to *over 68 million in 2022.* As more people were scammed, the total consumer losses also increased to over *$39 billion* last year.[10] The FTC also reported a significant increase in individual reported losses between 2021 and 2022.[11] A March 2023 report issued by Juniper Research predicts that fraudulent robocalls will cost mobile subscribers $*58 billion this year.*[12]

Incessant unwanted calls and texts are degrading the value of the U.S. telephone system. The continued onslaught of unwanted calls from unknown numbers undermines the value of the entire telephone system, and makes it more difficult to reach people in emergencies because they do not answer calls.[13] As the Commission recently noted:

> . . . [T]he evidence reveals that the escalating problem of robocalls has undermined consumers' trust and willingness to rely on their landline telephone, leading consumers in many cases to simply not answer the phone. That communication breakdown can have significant health and safety of life implications for the many consumers who rely on residential landline service.[14]

Government agencies and their contractors (such as ITG and YouMail) typically focus on scam calls, as they are the most damaging to both the recipients and the network. We understand that originating providers have increasingly resisted traceback requests from the ITG regarding telemarketing calls, claiming that these calls are legal because the recipients have provided TCPA-compliant consent for these calls. Yet it is impossible to believe that legitimate consent has been provided by subscribers for over a billion telemarketing calls each month. To address this confusion, in this past year we have been advocating that the FCC provide guidance concerning its regulations in a way that should radically reduce the number of telemarketing calls for which consent can be claimed to have been provided. Section III explains this advocacy.

---

[9] All data comes from YouMail. The most recent data, which was supplied to us on October 17, 2023, was combined with publicly available data for previous time periods. Scam and telemarketing stats are likely conservative estimates based on known percentages rather than direct reporting, which would result in underreported volume on these categorizations. In the past, YouMail has cautioned that "[s]ome calls initially viewed as telemarketing are eventually recognized as illegal telemarketing or scam calls, so it's important to measure the overall quantity of scam and spam calls combined." PR Newswire, Robocalls Top 50.3 Billion in 2022, Matching 2021 Call Volumes Despite Enforcement Efforts (Jan. 5, 2023), available at *https://www.prnewswire.com/news-releases/robocalls-top-50–3-billion-in-2022—matching-2021-call-volumes-despite-enforcement-efforts-301714297.html* (quoting YouMail press release).

[10] Truecaller, Truecaller Insights 2022 U.S. Spam & Scam Report (May 24, 2022), available at *https://www.truecaller.com/blog/insights/truecaller-insights-2022-us-spam-scam-report.*

[11] Losses from phone scams reported to the FTC by consumers increased from $700M to $798M from 2021–22, and losses from text scams more than doubled from $131M to $326M. FTC Consumer Sentinel Network, Fraud Reports by Contact Method, Reports & Amount Lost by Contact Method (Losses & Contact Method tab, with quarters 1 through 4 checked for 2021, 2022) (last visited Mar. 10, 2023), available at *https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts.* These numbers represent live scams as well as robocalls. As the number of complaints received has decreased, this means the average reported losses are getting larger.

[12] Press Release, Juniper Research, Fraudulent Robocalls to Cost Mobile Subscribers a Record $58 Billion Globally This Year, Finds Juniper Research Study (Mar. 20, 2023), available at *https://www.juniperresearch.com/pressreleases/fraudulent-robocalls-to-cost-mobile-subscribers?utm_source=juniper_pr&utm_campaign=pr1_robocallmitigation_providers_operators_mar23&utm_medium=e* ("Despite the ongoing development of robocalling mitigation frameworks, such as STIR/SHAKEN in North America, the report predicts that fraudsters' ability to innovate fraud methods will drive these losses to reach $70 billion globally by 2027. STIR/SHAKEN includes standards to mitigate fraudulent methods popular in North America, such as caller ID spoofing, which imitates a legitimate enterprise through the use of temporary business numbers.").

[13] *See* Benjamin Siegel, Dr. Mark Adbelmalek, & Dr. Jay Bhatt, ABC News, *Coronavirus Contact Tracers' Nemeses: People Who Don't Answer Their Phones* (May 15, 2020), available at *https://abcnews.go.com/Health/coronavirus-contact-tracers-nemeses-people-answer-phones/story?id=70693586. See also* Stephen Simpson, *Few Picking Up Phone When Virus Tracers Call,* Arkansas Democrat Gazelle, July 10, 2020, available at *https://www.arkansasonline.com/news/2020/jul/10/few-picking-up-phone-when-virus-tracers-call/.*

[14] Federal Commc'ns Comm'n, Final Rule, Limits on Exempted Calls Under the Telephone Consumer Protection Act of 1991, CG Docket No. 02–278, 88 Fed. Reg. 3668, at ¶21 (Jan. 20, 2023), available at *https://www.govinfo.gov/content/pkg/FR-2023-01-20/pdf/2023-00635.pdf.*

FCC enforcement actions are not sufficient to make a meaningful difference in these illegal calls. U.S.-based providers continue to spurn the Commission's requirements to respond to traceback requests, as the FCC reports each year,[15] and as recently as Q2 2023.[16] Its "first-ever" robo-blocking order (issued more than three years after the passage of the TRACED Act)[17] has already been breached.[18] Traceback requests unearth gateway providers and point of entry providers (the providers who bring the calls into the U.S. phone network) that months earlier were subject to FCC cease and desist orders for transmitting illegal robocalls.[19] Of the more than 7,000 voice service providers with certifications in the Robocall Mitigation Database (RMD),[20] the FCC has brought a total of 27 enforcement actions for deficient certifications; many of these actions addressed providers' failure to upload relevant documents rather than actual sub-standard practices.[21] The fines issued against some of the most egregious fraudsters[22] have not been recovered, which undermines the intended deterrent effect of imposing these fines. Yet the Commission

---

[15] *Compare* Federal Commc'ns Comm'n, Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information, Attachment A, "Non-Responsive 2022" tab (Dec. 23, 2022), available at *https://www.fcc.gov/document/ fcc-submits-traced-act-annual-report-2022-congress* [hereinafter FCC 2022 Report to Congress] *with* Federal Commc'ns Comm'n, Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information, Attachment A, "2021 NR Providers" tab (Dec. 22, 2021), available at *https://www.fcc.gov/document/ fcc-submits-traced-act-annual-report-2021-congress* [hereinafter FCC 2021 Report to Congress] *with* Federal Commc'ns Comm'n, Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information, Attachment D, "2020 NR Providers" tab (Dec. 23, 2020), available at *https://www.fcc.gov/document/fcc-submits-traced-act-annual-report-2020-congress* [hereinafter FCC 2020 Report to Congress].

[16] Federal Commc'ns Comm'n, Report on Traceback Data for the Period of April 2023 Through June 30, 2023) (Sept. 29, 2023), available at *https://www.fcc.gov/ document/fcc-releases-traceback-transparency-report* [hereinafter Traceback Transparency report].

[17] Press Release, Federal Commc'ns Comm'n, FCC Orders Blocking of Calls from Gateway Facilitator of Illegal Robocalls from Overseas (May 11, 2023), available at *https://www.fcc.gov/ document/ fcc-issues-first-ever-roboblocking-order-against-one-eye* [hereinafter Blocking of Calls order].

[18] Traceback Transparency report, *supra* note 16, at 10, Traceback ID 13726; this call was in violation of the Commission's May 11 Blocking of Calls order, *supra* note 17.

[19] *See* Letter from FCC Enforcement Bureau to Jeff Lawson, CEO of Twilio Inc. and Mellissa Blassingame, Senior Director of Twilio (Jan. 24, 2023), available at *https://www.fcc.gov/ document/ fcc-issues-robocall-cease-and-desist-letter-twilio;* Letter from FCC Enforcement Bureau to Brittany Reed, President of SIPphony L.L.C. (Jan. 11, 2023), *available at* https://www.fcc.gov/document/fcc-issues-robocall-cease-and-desist-letter-sipphony; Letter from FCC Enforcement Bureau to Corey Seaman, CEO of Vultik Inc. (Jan. 11, 2023), available at *https://www.fcc.gov/ document/fcc-issues-robocall-cease-and-desist-letter-vultik-inc;* Letter from FCC Enforcement Bureau to Aaron Leon, Co-Founder & CEO of thinQ Technologies, Inc. (Mar. 22, 2022), available at *https://www.fcc.gov/ document/fcc-issues-robocall-cease-and-desist-letter-thinq.*

[20] Federal Commc'ns Comm'n, Robocall Mitigation Database, available at *https://fccprod.servicenowservices.com/rmd?id=rmd_listings.*

[21] *See* Press Release, Federal Commc'ns Comm'n, FCC Seeks to Remove Companies from Key Database for Non-Compliance with Anti-Robocall Rules (Oct. 16, 2022), available at *https://www.fcc.gov/document/fcc-seeks-remove-companies-robocall-mitigation-database;* Press Release, Federal Commc'ns Comm'n, FCC Plans to Remove Companies from Key Database for Non-Compliance with Anti-Robocall Rules (Oct. 3, 2022), available at *https://www.fcc.gov/document/fcc-remove-companies-robocall-database-non-compliance.*

[22] *See* Press Release, Federal Commc'ns Comm'n, FCC Proposes Record $225 Million Fine for Massive Spoofed Robocall Campaign Selling Health Insurance (June 9, 2020), available at *https://www.fcc.gov/document/fcc-proposes-record-225-million-fine-1-billion-spoofed-robocalls-0* (proposed in June 2020), Press Release, Federal Commc'ns Comm'n, Health Insurance Telemarketer Faces Record FCC Fine of $225 Million for Spoofed Robocalls (Mar, 17, 2021), available at *https://www.fcc.gov/document/fcc-fines-telemarketer-225-million-spoofed-robocalls* (adopted in March 2021), Press Release, Federal Commc'ns Comm'n, FCC Reaffirms $225 Million Spoofed Robocall Fine (June 7, 2023), 3available at *https://www.fcc.gov/document/fcc-reaffirms-225-million-spoofed-robocall-fine-against-rising-eagle* (reaffirmed in June 2023). *See also* Press Release, Federal Commc'ns Comm'n, FCC Imposes Record Penalty Against Transnational Illegal Robocalling Operation (Aug. 3, 2023), available at *https://www.fcc.gov/document/fcc-imposes-record-fine-transnational-illegal-robocalling-operation* (issued after the Ohio Attorney General brought the following case in July 2022: Complaint for Permanent Injunction, Damages, and Other Equitable Relief, State of Ohio *ex rel.* Attorney General Dave Yost v. Jones, No. 2:22-cv-2700 (S.D. Ohio July 7, 2022), available at *https://www.ohioattorneygeneral.gov/Files/Briefing-Room/News-Releases/Time-Stamped-Complaint-22-CV-2700-State-of-Ohio-v.aspx).*

has referred only three forfeiture orders to the Department of Justice related to unwanted calls since the FCC began TRACED Act reporting in 2020.[23]

As is described in this testimony, we believe that additional measures are necessary to protect Americans from the illegal calls.

II. The FCC should establish a system to suspend complicit voice service providers after one notice, preventing them from transmitting illegal calls.

There are currently insufficient deterrents to counter the $1 million in monthly revenue[24] earned by complicit providers that transmit the one billion or more illegal calls made monthly.[25] Under the current rules, the profit from these calls clearly makes it worthwhile for providers to run the risk of transmitting the calls. Yet the income to providers pales when compared to the approximately $3 billion stolen every month from consumers through these fraudulent robocalls.[26]

Scam robocalls are transmitted as the result of the choices made by telecommunication service providers regarding what calls they will accept and transmit. Providers receive a payment for each call they transmit.

Robocalls typically follow a multi-step path from a caller to the called party, passed along from one provider to another multiple times. Calls go first to an originating provider (or a "gateway provider" in the case of a call from another country). That provider makes a choice whether to accept the calls from that caller. If it accepts the calls, it will send them to an intermediate provider that chooses to accept and transmit those calls down the call path. If that first intermediate provider decides not to accept the calls from the originating provider, the scam calls are stopped at that point and do not reach the called party unless the originating provider finds another intermediate provider willing to take them. Similarly, each hop in the chain to a subsequent intermediate provider or the terminating provider represents a separate decision by the downstream provider to accept and transmit those calls or to block them. Currently, the primary determinant for many of these instantaneous decisions made by the providers in the call path is profit. That must change.

As we describe in Section IV, there are tools currently available that allow providers to identify and then block scam robocalls. But providers need to be incentivized to use these tools and to block the calls found to be illegal.

The choices that providers in the call path make about whether to accept calls from upstream providers should be guided not only by the price paid for those calls, but also by the risk involved in accepting calls from those upstream providers. The consequences of the wrong choice should be steep. Providers who might otherwise be tempted to be complicit in transmitting scam calls will be financially motivated to comply with the law if punishments are swift, certain, and sufficiently severe. Given the proper incentives, the communications industry in the United States will develop and implement additional successful mechanisms as they become necessary.

---

[23] *See* FCC 2022 Report to Congress, *supra* note 15, at 7 (continuing the trend from 2021); *FCC 2021 Report to Congress, supra* note 15, at 8, and FCC 2020 Report to Congress, *supra* note 15, at 7.

[24] By some estimates, robocallers can send one million calls for as cheaply as $1,000 in call transmission costs; at a cost of $0.001 per call, more than one billion scam robocalls every month means that providers earn more than $1 million in revenue every month. *See, e.g., In re* Advanced Methods To Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor, Comments of ZipDX LLC, Seventh Further Notice of Proposed Rulemaking in CG Docket No. 17–59, and Fifth Further Notice of Proposed Rulemaking in WC Docket No. 17–97, at 2 (filed Aug. 17, 2022), available at *https://www.fcc.gov/ecfs/search/search-filings/filing/10818 2676204994.*

[25] Every month there are an average of one billion scam robocalls made to U.S. telephones, and a comparable number of illegal telemarketing calls. PR Newswire, Robocalls Top 50.3 Billion in 2022, Matching 2021 Call Volumes Despite Enforcement Efforts (Jan. 5, 2023), available at *https://www.prnewswire.com/news-releases/robocalls-top-50–3-billion-in-2022—matching-2021-call-volumes-despite-enforcement-efforts-301714297.html* (quoting YouMail press release) (scam calls made up roughly 41 percent of all robocall volume in 2022). The distinction between the two appears to be somewhat fluid, as they depend on how the calls are classified. The universally-reviled calls selling auto warranties—recently targeted by the Ohio Attorney General and the Commission, *see* Press Release, Office of the Ohio Attorney General, Yost Files Suit Alleging Massive Robocall Scheme (June 7, 2022)—are considered telemarketing calls, not outright scam calls. Conversation with Mike Rudolph, CTO, YouMail (Aug. 29, 2022).

[26] In May 2022, HarrisPoll, in a survey commissioned by Truecaller, estimated $39.5 billion in consumer losses over the past twelve months. *See* Truecaller, Truecaller Insights 2022 U.S. Spam & Scam Report (May 24, 2022), available at *https://www.truecaller.com/blog/insights/truecaller-insights-2022-us-spam-scam-report* (last visited Sept. 16, 2022). This is an average of more than $3.29 billion in consumer losses per month.

Telephone providers should be incentivized to develop and use procedures to guard against transmitting fraud robocalls. For originating, gateway, and first intermediate providers specifically, there is little excuse for continuing to transmit scam robocall traffic after any notice that the traffic is illegal based on previous tracebacks, FCC or FTC notices or cease and desist letters, similar notices from state attorneys general, or notices from service providers such as YouMail.

The FCC established the Robocall Mitigation Database (RMD) as a way to keep track of voice service providers and apply requirements to them.[27] The RMD provides a powerful and effective tool to the FCC to control non-compliant providers, as providers are prohibited from accepting traffic from voice service providers that have not submitted proper certification to the RMD.[28]

We believe that the FCC should be empowered to use immediate—but temporary—suspension[29] from its Robocall Mitigation Database as a mechanism to protect telephone subscribers from receiving illegal calls, pending investigations and due process determinations. This would prioritize protecting U.S. telephone subscribers from criminal scam calls over providing originating and gateway providers access to the U.S. telephone network.[30] Once a provider has been notified by any of the government enforcement agencies, or their service providers, that it has been found to be transmitting illegal calls, such notification should serve as legal notice that the next time it is determined to be transmitting illegal calls, it will be suspended from the RMD. These suspensions should be temporary and short-lived, but immediate, pending a due process review. The due process review would determine whether this latest finding that the provider was transmitting illegal calls was a mistake that will not be repeated, or whether it justifies permanent removal from the RMD.

We have recommended this type of immediate suspension to the Commission as a way of swiftly preventing complicit voice service providers from continuing to transmit tens of thousands of illegal calls.[31] The interests of American subscribers to be protected from dangerous, fraudulent, and invasive calls would be prioritized.

---

[27] *See* Federal Commc'ns Comm'n, Robocall Mitigation Database, available at *https://www.fcc.gov/robocall-mitigation-database.*

[28] *See* 47 C.F.R. § 64.6305(e)(1). *See also In re* Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking, WC Docket No. 17–97, at ¶ 8 (Rel. Mar. 17 2023), available at *https://docs.fcc.gov/ public/attachments/FCC-23-18A1.pdf.*

[29] Suspension should result in legally effective removal from the RMD. This can be accomplished via a prominent notation that the provider's status is suspended. *See, e.g., In re* Advanced Methods to Target and Eliminate Unlawful Robocalls *et al.,* Comments of ZipDX L.L.C., Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17–59, and Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17–97, at ¶ 64 (filed Dec. 7, 2021), available at *https://www.fcc.gov/ecfs/document/12080110629539/1* ("We would note that 'delisting' should not actually constitute complete removal from the database; rather, an entry should be retained so that it is clear to all others that the problematic provider has been explicitly designated as such. This will ensure that if (when) the problematic provider attempts to shift their traffic to a new downstream, that downstream will become aware of the situation before enabling the traffic.").

[30] Most, if not all, of the offending voice service providers are VoIP (Voice over Internet Protocol) services. VoIP is a technology that accesses the telephone network through the internet, and is commonly used by many large telecommunications providers in place of traditional landlines to provide service to residential and business customers. Often, the telephone service is paired with Internet access and cable television service. The VoIP providers that process the illegal robocalls are generally small, often simply one or two individuals with minimal investment or technical expertise who have set up a service in their home or other temporary quarters and offer services through online advertisements. *See* FCC 2021 Report to Congress, *supra* note 15, at 12 ("The Commission's experience tracing back the origins of unlawful call traffic indicates that a disproportionately large number of calls originate from Voice over Internet Protocol (VoIP) providers, particularly non-interconnected VoIP providers. Moreover, the Industry Traceback Group has found that high-volume, rapid-fire calling is a cost-effective way to find susceptible targets, although it does not collect data about which robocall originators are VoIP providers.").

[31] *In re* Advanced Methods To Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor, Comments of Electronic Privacy Information Center and National Consumer Law Center on Fifth Further Notice of Proposed Rulemaking in WC Docket No. 17–97 (filed Aug. 17, 2022), available at *https://www.fcc.gov/ecfs/document/10817350228611/1.* Our proposal for the immediate suspension of complicit providers contrasts with the Commission's procedure of issuing a Notification of Suspected Illegal Traffic, followed by an Initial Determination Order, then followed by a Final Determination Order, see FNPRM at ¶ 30. All three of those steps are required by the FCC before the provider is stopped from continuing to transmit illegal calls. In the time between the first and third steps, tens of thousands of illegal calls will reach subscribers.

We understand that this type of immediate suspension raises due process concerns for the affected providers. However, as we explain, those due process issues can be addressed.

Due process principles raise two concerns: 1) the timing and the content of notice given to the provider before the suspension from the RMD occurs; and 2) the opportunity for the provider to be heard and contest the factual basis for the suspension.[32]

The Commission can establish an expedited process of suspending providers from the RMD akin to the procedures established by Rule 65 of the Federal Rules of Civil Procedure for a court to provide a Temporary Restraining Order (TRO). TROs recognize the need to move quickly and without prior notice to the respondent to protect the moving party from immediate, irreparable harm.[33]

The Supreme Court has noted that "due process is flexible and calls for such procedural protections as the particular situation demands."[34] In this context, the Commission will be protecting telephone subscribers from the tens of thousands of illegal robocalls that would otherwise be placed but for the provider's suspension from the RMD. Protecting American subscribers from access by known criminals who seek to defraud them prevents irreparable harm and justifies a truncated procedure that provides notice to the provider of the suspension simultaneously with initiating an immediate suspension from the RMD. The U.S. government has an interest in protecting its residents from scam calls. The Supreme Court has recognized that the government's interests are to be balanced against the private interest affected by the action—in this case, the provider's removal from the RMD and subsequent inability to transmit calls into the network.[35]

Formal Notice. Just as when a TRO is issued by a court, the system we propose would require the Commission to issue a formal notice of the suspension to the provider at the same time it orders the suspension from the RMD. The notice to the provider would inform it of the basis for the suspension, the provider's right to request an evidentiary hearing to challenge the suspension, and other requirements related to the suspension. At the same time, the Commission would also notify all other providers on the RMD that they are prohibited from accepting calls from the suspended provider until otherwise notified.

Pre-Suspension Notice. The Commission can ensure that providers subject to these immediate suspensions have received previous notices of the consequences of continuing to transmit illegal calls. Currently, when the ITG sends a traceback request to a provider, it already includes information about the nature of the call subject to the traceback.[36] The traceback request is sent up through the call-path from the terminating provider, through the multiple intermediate providers, up to the originating or gateway providers. Not all these providers in the call path are complicit, as the illegal calls become mixed with legal calls as they travel—making it difficult for downstream providers to root out the illegal calls.

In the future, all traceback requests could include a warning that the failure to cease making illegal calls after notice, could trigger suspension from the RMD. The

---

[32] *See, e.g.,* Mathews v. Eldridge, 424 U.S. 319, 332, 96 S. Ct. 893, 47 L. Ed. 2d 18 (1976) ("Procedural due process imposes constraints on governmental decisions which deprive individuals of 'liberty' or 'property' interests within the meaning of the Due Process Clause of the Fifth or Fourteenth Amendment.").

[33] *See* "Legal Information Institute, Temporary Restraining Order, available at *https://www.law.cornell.edu/wex/temporary_restraining_order* (last accessed Oct. 19, 2023).

[34] Morrissey v. Brewer, 408 U.S. 471, 481, 92 S. Ct. 2593, 33 L. Ed. 2d 484 (1972). *See also* Mathews v. Eldridge, 424 U.S. 319, 349, 96 S. Ct. 893, 47 L. Ed. 2d 18 (1976) ("In assessing what process is due in this case, substantial weight must be given to the good-faith judgments of the individuals charged by Congress with the administration of social welfare programs that the procedures they have provided assure fair consideration of the entitlement claims of individuals.").

[35] *See* Mathews, 424 U.S. at 334–35 ("Accordingly, resolution of the issue whether the administrative procedures provided here are constitutionally sufficient requires analysis of the governmental and private interests that are affected. More precisely, our prior decisions indicate that identification of the specific dictates of due process generally requires consideration of three distinct factors: First, the private interest that will be affected by the official action; second, the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards; and finally, the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail." (internal citations omitted)).

[36] Each traceback notice sent to every provider in the call path contains a text description of the call, typically explaining what makes it illegal. *See* Complaint for Injunctive Relief and Civil Penalties, North Carolina *ex rel.* Stein v. Articul8, LLC & Paul K. Talbot, Case No. 1:22-cv-00058, at 30 ¶¶ 93–94 and 34 ¶¶ 98–99 (M.D.N.C. Jan. 25, 2022), available at *https://ncdoj.gov/wp-content/uploads/2022/01/FILED-Complaint_NC-v-Articul8_22-cv-00058-MDNC-2022.pdf* [hereinafter North Carolina v. Articul8 Complaint].

pre-suspension notice could also be included in notices from state attorneys general and the Federal Trade Commission. Providing notice of the *possibility* of suspension to all providers who are found to have transmitted illegal calls serves to remind every one of the potential ramifications of continuing the illegal activity.

Triggering Activity. Providers are complicit in transmitting illegal calls when they have received notice that their calls are illegal from any one of a number of enforcement agencies or their partners in this system and yet continue to pass along this traffic. Other Federal agencies are engaged in battling the scam calls, including the FTC and the Social Security Administration, as are the attorneys general in most states. Additionally, responsible intermediate providers currently alert upstream providers that they are transmitting illegal calls, as do some private service providers (such as YouMail and ZipDX) that are engaged in network monitoring. In the future, the Commission could establish a system under which any one of these entities—state attorneys general, the FTC and other Federal agencies involved in this work, intermediate providers, and private service providers—could alert the Commission when originating or gateway providers continue to transmit illegal calls even after repeated notice from any one or more of these entities. Alerts from any one of these trusted sources to the FCC could serve as the basis for the FCC to initiate immediately the suspension process. Once a trusted source provides information to the FCC regarding ongoing transmission of illegal calls by a provider, along with proof (information about the number and type of the calls, and the nature of the previous notice provided by the trusted source), that would trigger the immediate suspension notice from the FCC. At that point, the FCC would initiate the suspension of the targeted provider for a period of 10 days, by the end of which there would be a hearing to determine whether the provider would remain suspended from the RMD.

Opportunity to be Heard. Once a provider is given the formal notice from the Commission or its enforcement partners about the suspension, the basis for the suspension, and the provider's rights, the provider would have the right to contest the determination that it was transmitting illegal calls, had failed to comply with a traceback request or a Commission order, or was affiliated with providers previously suspended from the RMD.

We have advocated that the Commission should establish a mechanism to allow this type of fact-finding proceeding, possibly before a Commission Administrative Law Judge,[37] on an expedited basis. The Supreme Court has not required that these due process hearings always involve full evidentiary hearings and oral testimony; hearings can be conducted solely through the submission of written evidence.[38] The public's interest in being relieved of the illegal calls is a factor in determining the process that that is due. As the Court noted:

> In striking the appropriate due process balance the final factor to be assessed is the public interest. This includes the administrative burden and other societal costs that would be associated with requiring, as a matter of constitutional right, an evidentiary hearing upon demand in all cases prior to the termination of disability benefits. The most visible burden would be the incremental cost resulting from the increased number of hearings. . . .[39]

In this context, the Commission's priority should be protecting subscribers from the criminals seeking to defraud them through the scam robocalls. Moreover, the only procedures required are those "to insure that [the respondents] are given a meaningful opportunity to present their case."[40] The Supreme Court has emphasized that "substantial weight must be given to the good-faith judgments of the individuals charged by Congress with the administration of social welfare programs that the procedures they have provided assure fair consideration of the entitlement claims of individuals."[41] Like the Social Security Administration in the case quoted, the Commission is charged with the important task of protecting the American public—here, from illegal robocalls, and the billions stolen from American subscribers through these calls.

Length of the Suspension. The Commission should offer the suspended provider the opportunity to request a hearing within an appropriate number of days to contest the grounds for the suspension, provide evidence, and possibly provide sufficient sureties of good behavior in the future. If no hearing is requested, however, the

---

[37] Fed. Commc'ns Comm'n, Administrative Law Judges, available at *https://www.fcc.gov/administrative-law-judges* (last accessed Oct. 19, 2023)

[38] *See* Mathews v. Eldridge, 424 U.S. 319, 334, 343–44, 96 S. Ct. 893, 47 L. Ed. 2d 18 (1976).

[39] *Id.* at 347.

[40] *Id.* at 349.

[41] *Id.*

Commission should determine the appropriate length of the suspension based on the need to protect the telephone system from illegal robocalls. Permanent suspension from the RMD should be a valued tool in the Commission's authority to protect subscribers from illegal robocalls. This aligns with Commissioner Starks' statement: "[i]f we identify a bad actor, it's time to make it harder to operate. If it's a repeat offender, we should go further."[42] The Commission has already made clear in numerous instances that providers must comply with its rules, and it has listed potential consequences for failing to do so, explicitly including suspension from the RMD.[43]

If the Commission believes that it does not have the authority to exercise these immediate but temporary suspensions to protect American telephone subscribers from these illegal calls, we urge Congress to provide such authority.

III. The Commission should issue guidance confirming that its current regulations limit agreements for prior express consent and prior express invitation to calls from one seller, and that the E-Sign Act applies to agreements entered online.

The misuse of consumers' "consents" by lead generators and others is a major factor contributing to the increasing number of illegal telemarketing calls and texts. The number of telemarketing calls has been steadily rising in recent years, peaking at over 1.4 billion a month in March 2023.[44]

Lead generators, a common feature on the internet, refer potential customers to vendors.[45] The "leads"—the telephone numbers and other data regarding potential customers—are sold directly to sellers of products or services (such as lenders or insurance companies) or to lead aggregators that then sell the leads to sellers.[46] As courts and the FTC have noted, it is not always apparent from a particular website that it is operated by a lead generator rather than an actual lender or seller of other products or services,[47] and misrepresentations and outright consent fraud on lead generators' sites are common.[48]

Consumers who visit a lead generator's site are typically invited to enter their contact information into a form or application on the site. Typically, the consumer is asked to click on a link that includes language in tiny font[49] that does not any-

---

[42] *See* Statement of Comm'r Geoffrey Starks, *In re* Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17–59; Call Authentication Trust Anchor, WC Docket No. 17–97; Report and Order, Order on Reconsideration, Order, and Further Notice of Proposed Rulemaking (May 19, 2022).

[43] For example, since at least as early as its Second Report and Order in October 2020, the Commission has given U.S. voice service providers (as well as foreign providers that use U.S. numbers to send voice traffic to U.S. subscribers) notice that deficient certifications or failure to meet the standards of its own certifications could be met with enforcement "including de-listing the provider from the database." *In re* Call Authentication Trust Anchor, Second Report and Order, WC Docket No. 17–97, at ¶93 (Oct. 1, 2020), available at *https://docs.fcc.gov/public/attachments/FCC-20-136A1.pdf.* Also, the Commission has required that providers submit updates regarding "any of the information they filed in the certification process" within 10 business days of the change. *Id.* The Commission took a similar step against the robocallers themselves in 2020. *See* Press Release, Federal Commc'ns Comm'n, FCC to Robocallers: There Will Be No More Warnings (May 1, 2020), available at *https://docs.fcc.gov/public/attachments/DOC-364109A1.pdf.*

[44] PR Newswire, U.S. Consumers Received Roughly 5 Billion Robocalls in March, According to YouMail Robocall Index: National Monthly Robocall Volume Reached Highest Peak Since November 2019 (Apr. 7, 2023), available at *https://www.prnewswire.com/news-releases/us-consumers-received-roughly-5-billion-robocalls-in-march-according-to-youmail-robocall-index-301792292.html.*

[45] *See* Federal Trade Comm'n, "Follow the Lead" Workshop, Staff Perspective (Sept. 2016), available at *www.ftc.gov* (overview of lead generation industry).

[46] *Id.* at 2 ("A lead is someone who has indicated—directly or indirectly—interest in buying a product.").

[47] *See, e.g.,* CFPB v. D & D Mktg., 2016 WL 8849698, at *1 (C.D. Cal. Nov. 17, 2016).

[48] *See* Federal Trade Comm'n, Follow the Lead Workshop—Staff Perspective 5 (Sept. 2016), available at *www.ftc.gov. See also* Consumer Fin. Prot. Bureau v. RD Legal Funding, L.L.C., 332 F. Supp. 3d 729, 782–783 (S.D.N.Y. 2018); MacDonald v. CashCall, Inc., 2017 WL 1536427, at *12 (D.N.J. Apr. 28, 2017), *aff'd on other grounds,* 883 F.3d 220 (3d Cir. 2018) (affirming denial of arbitration motion); CFPB v. D & D Mktg., 2016 WL 8849698, at *1 (C.D. Cal. Nov. 17, 2016); Consumer Fin. Prot. Bureau v. CashCall, Inc., 2016 WL 4820635, at *10 (C.D. Cal. Aug. 31, 2016). *See also* McCurley v. Royal Seas Cruises, Inc., 21–55099, 2022 WL 1012471 at *3 (9th Cir. Apr. 5, 2022) ("The amount of mismatched data in the record cannot all be explained by data-entry errors or family members with different last names. . . . These facts, in combination with the evidence of widespread TCPA violations in the cruise industry, would support a finding that Royal Seas knew facts that should have led it to investigate Prospects's work for TCPA violations.").

[49] For example: By clicking "Get My Auto Quotes" the consumer is supposedly agreeing that the lead generator can "share my information to the providers in our network for the purpose

where indicate that the lead generator is planning to use that click to justify telemarketing calls from hundreds—or even—thousands—of telemarketers.[50]

The site operator then sells the consumer's information to interested lenders or sellers, sometimes with some level of data analysis, and often through an automated auction. A 2011 survey found that leads are sometimes sold for over $100[51]; more recent online data indicates that leads can be sold for as much as $600 each.[52]

One organization of lead generators admitted in its comments to the Commission in a March 2023 Notice of Proposed Rulemaking that lead generators are responsible for a "meaningful percentage" of entirely fabricated consent agreements.[53] These comments provide particularly helpful information about how the lead generator industry works to facilitate telemarketing robocalls: *"once the consumer has submitted the consent form the company seeks to profit by reselling the 'lead' multiple—perhaps hundreds—of times over a limitless period of time. Since express written consent does not expire, the website is free to sell the consent forever."*[54]

Each party that owns the consent, including the original lead generator and every subsequent purchaser of the consent, "is *free to sell it again."*[55] As the lead generators explain: the result of all these sales is that "[e]ach time the website operator—or an intermediary "aggregator" . . . sells the consumer's data *a new set of phone calls will be made to the consumer."*[56]

Additional comments in the FCC's proceeding support the point that the practice of lead generators sharing consents is a major contributing factor in the proliferation of unwanted telemarketing calls:

- The known fact that one click can sign up a consumer to thousands of businesses, related or not, is a dreadful problem. Aged leads are also problematic because, currently, consent never expires.[57]
- Until lead buyers stop purchasing non-compliant leads there will be incentives that lead to bad practices.[58]

On the other hand, comments from the telemarketing industry and lead generators defend the sharing of consumer consents with hundreds, and even thousands, of callers. For example, a trade association for telemarketers argues against the Commission's proposal in the NPRM: "It is easy to say that 1,000 companies are too many but there are many markets, such as insurance, where hundreds of relevant companies provide differentiated products."[59] The level of objections to the FCC's concerns by the lead generator industry underscores the extent to which that industry is responsible for so many of the billion monthly telemarketing calls made to American telephones.

FCC regulations already require consumers' written consents to apply to just one seller and to be non-transferable. The Telephone Consumer Protection Act[60] requires the FCC to establish regulations governing telemarketing calls. For the past several decades, the FCC's regulations have outlined explicit requirements for callers before

---

of providing me with information about their financial services and products." But to see the full list of callers and other lead generators that this website could sell the consumer's lead to, one must place their mouse and hover over a link embedded in the long paragraph under the place to be clicked, described *infra* at 50.

To access this form, a person must go to QuoteWizard's website at *https://www.quotewizard.com/* and provide information about the insurance product they seek, as well as their name, address, and telephone number, birth date, and other personal information.

[50] *See, e.g.,* the list of thousands of insurance carrier partners of QuoteWizard, available at *https://quotewizard.usnews.com/form/static/corp/providers.html?bn=U.S.%20News&bf=usnews.*

[51] Consumer Federation of America, CFA Survey of Online Payday Loan Websites 7 (Aug. 2011), available at *https://consumerfed.org/pdfs/CFAsurveyInternetPaydayLoanWebsites.pdf.*

[52] *See* Leads Hook, Blog post, *How to Make Money Selling Leads in 2023 (& How Much to Charge)* (July 12, 2023), available at *https://www.leadshook.com/blog/how-to-sell-leads/.*

[53] Comment of Responsible Enterprises Against Consumer Harassment, CG Dockets Nos. 21–402, 02–278, at 1 (filed May 9, 2023), available at *https://www.fcc.gov/ecfs/document/10509951114134/1.*

[54] *Id.* at 3 (emphasis added).

[55] *Id.* at 6 (emphasis added).

[56] *Id.* at 3 (emphasis added).

[57] Comment of Drips, CG Dockets Nos. 21–402, 02–278 (filed May 8, 2023), available at *https://www.fcc.gov/ecfs/document/10509043191182/1.*

[58] Comment of National Association of Mutual Insurance, CG Dockets Nos. 21–402, 02–278 (filed May 8, 2023), available at *https://www.fcc.gov/ecfs/document/10508029328611/1.*

[59] Comment of Professional Associations for Customer Engagement, CG Dockets Nos. 21–402, 02–278, at 9 (filed May 8, 2023), available at *https://www.fcc.gov/ecfs/document/10508798 33281/1.*

[60] 47 U.S.C. §§ 227 *et seq.*

they can make prerecorded telemarketing calls to cell phones and residential lines,[61] or any calls to lines registered on the Nation's Do Not Call (DNC) Registry.[62] Both regulations require that, before those calls can be made, the recipient must have signed an express written agreement consenting to telemarketing calls by or on behalf of a single seller.[63]

The requirements for consent or invitation to receive telemarketing calls in the current FCC regulations are quite specific, and they have been the law for a long time.[64] The current regulations prohibit telemarketing calls to a line registered on the DNC Registry unless the telemarketer has a "personal relationship with the recipient" or the caller has the subscriber's prior express invitation or permission. The rule specifies:

> Such permission must be evidenced by a signed, written agreement *between the consumer and seller* which states that the *consumer agrees to be contacted by this seller* and includes the telephone number to which the calls may be placed; . . .[65]

The critical language in this regulation is a) the agreement must be "between the consumer and seller," and b) it must specify that the consumer agrees to be contacted by "this seller." As each agreement must be between the seller and the consumer, and each agreement must be limited to the calls from that seller, the FCC's regulation clearly prohibits any agreement from providing consent to more than one seller or consent that can be sold or transferred to another seller.

Similarly, the FCC's rules for prerecorded telemarketing calls to cell phones and residential lines requires prior express written consent,[66] which the current regulations define in 47 C.F.R. § 64.1200(f)(9) as:

> (9) The term prior express written consent means an agreement, in writing, bearing the signature of the person called that clearly authorizes *the seller* to deliver or cause to be delivered to the person called advertisements or telemarketing messages using an automatic telephone dialing system or an artificial or prerecorded voice, and the telephone number to which the signatory authorizes such advertisements or telemarketing messages to be delivered.
>
> (i) The written agreement shall include a clear and conspicuous disclosure informing the person signing that:
>
> > (A) By executing the agreement, *such person authorizes the seller* to deliver or cause to be delivered to the signatory telemarketing calls using an automatic telephone dialing system or an artificial or prerecorded voice;[67]

Unlike the requirements for prior express invitation under 47 C.F.R. § 64.1200(c)(2)(ii) for calls to DNC lines, this regulation does not explicitly require that the agreement be "*between" the person to be called and the seller.* But the references to "*the seller"* make it clear that the agreement can permit calls from only one seller.

Thus, both of these consent provisions are explicit in allowing consent to be given to receive calls *only from a single identified seller.* If there were any ambiguity, the FCC's rule should be interpreted to be consistent with the parallel provisions of the Federal Trade Commission's (FTC) Telemarketing Sales Rule (TSR).[68] Congress has

---

[61] 47 C.F.R. § 64.1200(f)(9).

[62] 47 C.F.R. § 64.1200(c)(2)(ii).

[63] 47 U.S.C. § 227(a)(4). The regulation makes exceptions for calls to DNC lines when the calls are on behalf of charities, and when the caller has an "established business relationship" with the recipient.

[64] The Commission's regulation governing consent for calls to DNC lines were promulgated in 2003. *See* Rules and Regulations Implementing the Telephone Consumer Protection Act (TCPA) of 1991, Final Rule, CG Docket No. 02–278, 68 Fed. Reg. 44,144, 44,148 ¶ 22 (F.C.C. July 25, 2003) ("Consistent with the FTC's determination, we conclude that for purposes of the national do-not-call list *such express permission must be evidenced only by a signed, written agreement between the consumer and the seller* which states that the consumer agrees to be contacted by this seller, including the telephone number to which the calls may be placed." (emphasis added)). The regulations requiring prior express written consent for prerecorded telemarketing calls to residential lines and cell phones were promulgated in 2012. *See In re* Rules & Regulations Implementing the Telephone Consumer Protection Act of 1991, Report and Order, Docket No. 02–278, 27 F.C.C. Rcd. 1830, 1873 ¶ 28 (F.C.C. Feb. 15, 2012).

[65] 47 C.F.R. § 64.1200(c)(2)(ii) (emphasis added).

[66] 47 C.F.R. § 64.1200(a)(3).

[67] 47 C.F.R. § 64.1200(f)(9) (emphasis added).

[68] 16 C.F.R. §§ 310.1 *et seq.* With respect to prerecorded calls, before a telemarketing call can be made, the TSR requires that the "*seller* [must have] obtained [consent] only after a clear and conspicuous disclosure that the purpose of the agreement is to *authorize the seller to place prerecorded calls to such person;*. . ." 16 C.F.R. § 310.4(b)(1)(v)(A)(i) (emphasis added).

instructed the Commission to maximize consistency with the FTC's rules,[69] and even without a congressional directive it is obvious that inconsistent rules governing the same activity would be problematic.

The TSR's requirements that "the seller" obtain the consumer's consent, and that the consent allows delivery of prerecorded messages "by or on behalf of a specific seller," make it clear that a third party that is not the seller's agent cannot obtain the consumer's consent, and that consent cannot be sold or transferred. And the FTC has explicitly reiterated this point in its Business Guidance,[70] which explains:

> May a seller obtain a consumer's written permission to receive prerecorded messages from a third-party, such as a lead generator? No. The TSR requires the seller to obtain permission directly from the recipient of the call. The seller cannot rely on third-parties to obtain permission.

The FCC should simply issue guidance reiterating the clear meaning of its existing regulations. To confirm what the FCC's regulations have said for the past twenty years, and to show consistency with the FTC's rule, the FCC should similarly issue guidance that under its existing rules, consent agreements must identify a single seller and that a seller or telemarketer cannot obtain consent by purchasing it from, or obtaining a referral from, a lead generator, another seller, telemarketer, or an independent contractor.

In March 2023, the Commission proposed new regulations intended to limit the collection and selling of consent agreements among lead generators.[71] However, we—on behalf of a broad coalition of consumer and privacy groups—have strongly urged the Commission *not* to proceed with its proposed changes to its regulations, as that proposal would be a reduction in consumer protections from the current regulations, and would be inconsistent with the existing language which already addresses the problem. In extensive comments, and several meetings,[72] we have explained how the current TCPA regulations already set the necessary standards. Instead of issuing new regulations, we have urged the Commission to issue *guidance* reiterating the requirements in its current regulations, along with a reminder that the Federal E-Sign law applies whenever writings or signatures are provided electronically. Our comments on these points have been reiterated by USTelecom-The Broadband Association,[73] as well as comments filed on behalf of 28 state attorneys general.[74]

Instead of issuing new rules, the FCC should simply issue guidance to industry, reiterating that the existing rules require a consumer's consent to be limited to calls by or on behalf of a single seller, and that this consent cannot be sold or transferred. Insisting on compliance with current TCPA regulations will significantly reduce the

---

[69] The Do-Not-Call Implementation Act, Pub. L. No. 108–10, § 3, 117 Stat. 557 (2003) ("Not later than 180 days after the date of enactment of this Act, the Federal Communications Commission shall issue a final rule pursuant to the rulemaking proceeding that it began on September 18, 2002, under the Telephone Consumer Protection Act (47 U.S.C. 227 et seq.). *In issuing such rule, the Federal Communications Commission shall consult and coordinate with the Federal Trade Commission to maximize consistency with the rule promulgated by the Federal Trade Commission*. . . ." (emphasis added)).

[70] Federal Trade Comm'n, Business Guidance, Complying with the Telemarketing Sales Rule, available at *https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#prerecordedmessages.*

[71] *In re* Targeting and Eliminating Unlawful Text Messages Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Report and Order and Further Notice of Proposed Rulemaking, CG Docket Nos. 21–402, 02–278 (Rel. Mar. 17, 2023), available at *https://www.fcc.gov/document/fcc-adopts-its-first-rules-focused-scam-texting-0.* The Proposed Rule was published in the Federal Register at 88 Fed. Reg. 20,800 (Apr. 7, 2023) and is available at *https://www.govinfo.gov/content/pkg/FR-2023-04-07/pdf/2023-07069.pdf.*

[72] *See In re* Targeting and Eliminating Unlawful Text Messages Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Comments of National Consumer Law Center *et al.,* CG Docket Nos. 21–402, 02–278 (filed May 8, 2023), available at *https://www.fcc.gov/ecfs/document/1050859496645/1* and *In re* Targeting and Eliminating Unlawful Text Messages Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Reply Comments of National Consumer Law Center *et al.,* CG Docket Nos. 21–402, 02–278 (filed June 6, 2023), available at *https://www.fcc.gov/ecfs/search/search-filings/filing/10606186902940.*

[73] *In re* Targeting and Eliminating Unlawful Text Messages Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Comments of USTelecom—The Broadband Association, CG Dockets No. 21–402, 02–278 (filed May 8, 2023), available at *https://www.fcc.gov/ecfs/document/10508915228617/1.*

[74] *In re* Targeting and Eliminating Unlawful Text Messages Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Reply Comments of 28 State Attorneys General, CG Dockets No. 21–402, 02–278 (filed June 6, 2023), available at *https://www.fcc.gov/ecfs/search/search-filings/filing/10606091571575.*

number of unwanted telemarketing calls by limiting the sale of consent by lead generators. Most of the billion-plus monthly telemarketing calls that consumers receive today are based on consents supposedly obtained through lead generators on various websites. Yet the fact that lead generators and their telemarketing customers have been ignoring the requirements of the Commission's regulations on telemarketing calls—and getting away with it for many years—is not a reason to allow that behavior to continue. As the Commission has repeatedly recognized, it is largely because of too many robocalls that the use of the telephone has declined in recent years.[75]

Limiting the ability to use a consumer's single agreement of consent to justify multiple calls from different telemarketers will stop a large number of unwanted telemarketing calls, as only a tiny fraction of the consents previously used to justify the calls will meet the requirements. Requiring the calling and lead generation industries to comply with regulations that have been on the books for over a decade may force a change in their practices, but it will be a change that will greatly benefit consumers.

Complying with the existing rules will not prevent lead generators from putting consumers in touch with sellers they want to hear from. Nothing in the FCC's rules prevents lead generators from providing information to consumers, including direct referrals to sellers of products and services through weblinks. And nothing prohibits lead generators from providing the offered referrals through e-mail or snail mail (addresses are often required information), or even by simply displaying the information right on the website. Many lead generators currently do not require the entry of a telephone number to refer a consumer to a seller,[76] and others ask for minimal information (like zip code) and then refer the consumer right to a seller's website.[77] All of these practices, which are far less invasive than unleashing a torrent of telemarketing calls, will be unaffected by compliance with the existing rules.

The FCC should also issue guidance reiterating that online consent agreements must comply with E-Sign. Although few parties comply, the Federal E-Sign Act applies when signatures are provided electronically, and when electronic records are used to satisfy requirements for a writing. The E-Sign Act establishes the rules for satisfying a requirement for a writing or a signature with their electronic equivalents.[78]

It is only because of the E-Sign Act that an electronic action like a click on a website can carry the same legal significance as a "wet" signature.[79] As a result, an electronic click used by a telemarketer to signify a person's signature on an agreement providing express consent or invitation to receive telemarketing calls under either the TCPA regulations or the TSR will qualify as a signature that can bind the person to the agreement *only if* that click meets the definition of an electronic signature in the E-Sign Act at 15 U.S.C. § 7006(5). Among other things, this definition requires that the signer have the intent to sign the electronic record.[80] When the agreement is to provide consent for telemarketing calls, the place on the electronic form where the electronic action is to be applied must clearly indicate that the consumer, by taking the electronic action, is intending to sign the related electronic agreement to receive those calls. An electronic sound, symbol, or process applied on a website that is hyperlinked to a list of multiple other parties from whom the person is purportedly agreeing to receive calls should not be construed to indicate consent by the person applying the click, because the person would not have had the required intent to sign an agreement with all of the callers each and every one of the hundreds or thousands of callers included in the hyperlinked list.[81]

---

[75] *See* FNPRM at ¶ 1 ("Many of us no longer answer calls from unknown numbers and, when we do, all too often find them annoying, harassing, and possibly fraudulent. Consumers are not the only losers when this happens; legitimate callers have a hard time completing the calls consumers do want to receive.").

[76] *See, e.g., https://www.google.com/travel/flights.*

[77] *See, e.g., https://best.ratepro.co/; https://www.esurance.com/; www.nerdwallet.com.*

[78] 15 U.S.C. §§ 7001 *et seq.*

[79] 15 U.S.C. § 7001(a)(2).

[80] 15 U.S.C. § 7006(5) ("The term 'electronic signature' means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person *with the intent to sign the record.*" (emphasis added)).

[81] *See, e.g.,* Federal Commc'ns Comm'n, *In re* Urth Access, Inc., Order, File No. EB–TCD–22–00034232, 2022 WL 17550566, at ¶¶ 16 (Rel. Dec. 8, 2022), available at *https://www.fcc.gov/document/fcc-orders-voice-service-providers-block-student-loan-robocalls* ("The websites included TCPA consent disclosures whereby the consumer agreed to receive robocalls from 'marketing partners.' These 'marketing partners' would only be visible to the consumer if the consumer clicked on a specific hyperlink to a second website that contained the names of each of 5,329 entities. We find that listing more than 5,000 'marketing partners' on a secondary website is not sufficient to demonstrate that the called parties consented to the calls from any one of these 'marketing partners.'" (footnote omitted)).

Because the telemarketing industry has routinized non-compliance with the FCC's current regulations, we have urged the FCC to issue guidance clarifying how these regulations apply to telemarketing calls.

IV. Legal callers should leverage their power in the marketplace to protect their calls from blocking and mislabeling, which will assist in the efforts to eliminate the illegal calls.

The FCC's efforts to address illegal calls include its recent proposal [82] to encourage terminating providers to block more suspicious calls, as well as continuing to label suspicious calls.[83] While supporting these proposals, we have respectfully suggested that just doing more of the same—requiring blocking of calls from FCC-identified providers, encouraging opt-out blocking and labeling, and enforcing and tweaking rules for STIR/SHAKEN authentication—seems unlikely to change the basic dynamic that drives these illegal calls: originating and gateway providers are making sufficient income from these calls to make it more profitable to keep making the calls and risking the punishment.[84] Clearly, the potential for costly consequences from conveying these illegal calls is sufficiently remote and outweighed by the income from these calls such that the current measures fail to dissuade these providers from continuing their current practices.[85]

Instead, we have urged the Commission to adopt a set of best practices for legal callers that—if widely used—will likely eliminate many of the illegal calls plaguing subscribers' telephone lines. These best practices would leverage the market power of the legal callers to change the calculus of voice service providers that are currently complicit—either knowingly or with deliberate blindness—about their transmission of illegal calls. If legal callers were to demand, on a uniform basis, that the voice service providers that transmit their calls must adopt the Commission's best practices and avoid transmitting illegal calls, the profit from illegal calls would plummet. Even more importantly, the illegal calls would no longer mixed with the legal calls, making it much easier for the terminating providers to identify and block these calls.

Legal callers have repeatedly complained that their legal—and often wanted—calls are erroneously blocked or labeled. As a result, subscribers are likely missing some calls that they want or need from callers,[86] and legal callers are experiencing escalating costs and frustrations with consistently and reliably completing their calls to subscribers. These problems are caused by the mislabeling and incorrect blocking of their *legal* calls.[87]

Legal callers are responsible for placing over two billion robocalls every month. While some of these calls are surely unwanted, there is no dispute that a significant percentage of these calls are desired, welcomed, or critical to their recipients (*e.g.,* school, government, security, or disaster alerts). The difficulties with reliably completing these wanted calls are apparently increasing. Legal calls are mixed with a torrent of illegal calls at shared originating and intermediating providers, causing legal calls to be tainted by illegal calls in the same call path. The result is that legal calls end up mislabeled or blocked by downstream providers seeking to protect subscribers from illegal calls.

We have proposed that the Commission facilitate leveraging the considerable marketplace power of these legal callers to assist in the efforts to eliminate dangerous

---

[82] FNPRM. The Proposed Rule was published in the Federal Register at 88 Fed. Reg. 43,489 (July 10, 2023) and is available at *https://www.federalregister.gov/documents/2023/07/10/2023-13032/advanced-methods-to-target-and-eliminate-unlawful-robocalls.*

[83] We note that call labeling should only be used in lieu of blocking when there is meaningful doubt about the legality and value of the call, such that allowing the call to go through poses less risk than blocking it. In other words, calls that appear to be likely scams should always be blocked, as the risk to consumers from those calls is significant. Blocking scam calls should be the first and primary line of defense, not labeling.

[84] *See In re* Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor, Reply Comments of National Consumer Law Center, Electronic Privacy Information Center, & Public Knowledge Relating to Seventh Report and Order and Eighth Further Notice of Proposed Rulemaking, CG Docket No. 17–59, WC Docket No. 17–97 (filed Sept. 8, 2023), available at *https://www.fcc.gov/ecfs/search/search-filings/filing/1090831416629.*

[85] This dynamic was noted in 2021 by Commissioner Starks: "[I]llegal robocalls will continue so long as those initiating and facilitating them can get away with and profit from it." *In re* Call Authentication Trust Anchor, Further Notice of Proposed Rulemaking, WC Docket No. 17–97 (Sept. 30, 2021) (Statement of Comm'r Geoffrey Starks).

[86] *See, e.g., In re* Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor, Comments of Numeracle, Inc, CG Docket No. 17–59, WC Docket No. 17–97, at 2, 19 (filed Aug. 9, 2023), available at *https://www.fcc.gov/ecfs/document/108102252803712/1.*

[87] *Id.*

and unwanted calls—scam and illegal telemarketing calls. If legal callers are armed with the information about how to avoid using the providers that are processing illegal calls, the sheer economic power of legal callers may be sufficient to force voice providers to stop transmitting illegal calls.

We have suggested that the Commission define best practices for legal callers and provide clear recommendations to enable these callers to use their power in the telephone marketplace to ensure that their calls are placed only with providers that do not originate calls or transmit from illegal callers. A market-based approach like this would a) provide strong financial incentives to originating and intermediate providers to avoid transmitting illegal calls; b) facilitate the transmission of legal calls through call paths that would eliminate the likelihood that the calls would be labeled improperly or blocked by downstream or terminating providers; and c) supplement the other mechanisms created by the Commission intended to address illegal calls. *The foundation of a market-based approach is providing legal callers with the information that they need to keep their calls separate from illegal calls.* As we explain below, this information is already available from private analytics-based platforms. The Commission need only lead the way.

Legal calls are mistaken for illegal calls because of the lack of transparency regarding the providers that are transmitting both types of calls. As described in Section II, *supra,* automated calls take circuitous routes from origination to the call recipient through the least-cost routing process.[88] The least-cost routing process allows downstream providers to refuse to take calls from upstream providers if they do not like the price offered for the transmittal or if they deem the calls potentially illegal—and thus too costly. The issue is how to incentivize downstream providers to refuse more of these illegal calls. The providers that are complicit in transmitting illegal calls are well aware of what they are doing. They know that the calls are illegal because they have received multiple traceback requests. With each traceback request, they are given a notice from the Industry Traceback Group (ITG) that they are transmitting suspicious calls.[89] So, even if the providers did not know before they received the traceback request from the ITG that the calls transmitted over their networks were illegal, the providers are fully aware once the traceback requests start arriving.

The phone network currently allows for legal calls to be mixed with illegal calls, which frustrates attempts to identify the illegal calls accurately and label or block them. Disaggregating legitimate calls from illegal traffic is the first step to resolving both problems. To do that, legal callers need to be equipped with the means to avoid the providers transmitting high volumes of illegal traffic alongside their legal calls.

The results of tracebacks and government investigations into illegal providers are only reported publicly after they are completed. To protect themselves, legal callers need to know in real time which providers are responsible for illegal calls, and they need to be made aware of how to use that information to protect their calls from being mislabeled or blocked.

In their enforcement efforts, the Commission and other Federal and state government agencies currently use information from non-government service providers that maintain real-time *content-based analytics* platforms. These platforms capture live evidence of illegal calls, including the content of the calls (both audio and transcribed), the telephone numbers of the callers and called parties, the date and time, the upstream voice service providers that provided STIR/SHAKEN attestation, and more. This information is aggregated to show volumes of calls, patterns in the calls, call paths, compliance with STIR/SHAKEN, and more. These content-based analytics platforms are also used by private enterprises in banking, health care, and hospitality and government agencies seeking to protect themselves from callers pretending to be these businesses to scam consumers. The platforms assist these insti-

---

[88] *See* Appendix to Complaint, United States of America v. Palumbo, Case 1:20-cv-00473, Declaration of Marcy Ralston at 10–12 ¶ 22 (E.D.N.Y. Jan. 28, 2020). Marcy Ralston, a Special Agent in the Social Security Administration's Office of Inspector General, Office of Investigations, provided a sworn statement in *United States of America v. Palumbo.*

[89] Each traceback notice sent to every provider in the call path contains a text description of the call, typically explaining what makes it illegal. *See North Carolina v. Articul8 Complaint, supra* note 36, at 30 ¶¶ 93–94 and 34 ¶¶ 98–99. In addition, most traceback notices include a link to the recorded message that was captured. North Carolina alleged that ITG notified Articul8 of this illegal traffic 49 times for calls. *Id.* at 30 ¶ 93. In one version of the Social Security scam, "the caller says your Social Security number has been linked to a crime (often, he says it happened in Texas) involving drugs or sending money out of the country illegally." Jennifer Leach, Federal Trade Comm'n, Consumer Advice, *Fake calls about your* SSN (Dec. 12, 2018), available at *https://consumer.ftc.gov/consumer-alerts/2018/12/fake-calls-about-your-ssn.*

tutions by identifying the voice service providers responsible for transmitting the imposter calls, thereby facilitating the disruption of illegal calls.[90]

There is no reason that legal callers could not use the information from these content-based analytics platforms to identify the providers responsible for transmitting illegal calls. Once aware of which providers are participating in that conduct, a legal caller could switch to another originating provider that is not associated with illegal calls. Additionally, in its contracts with the providers originating their legal calls, the legal callers could require that the provider not send this caller's traffic to immediately downstream providers that are transmitting illegal calls from upstream providers that are currently accepting bad traffic.

If sufficient numbers of legal callers employ these practices, in combination, considerable market pressure would be exerted on telecom providers to improve their mitigation efforts, as they would risk losing legal call traffic to competitors that are more effective at detecting and blocking bad traffic. Instead, at present, these originating and intermediate providers are rewarded when legal and illegal traffic are mixed together. That mixing masks illegal traffic, allowing the providers that are transmitting illegal traffic to continue profiting from it and further degrading the reliability of the American telephone system.

The Commission can provide information on best practices that would clarify for legal callers how to ensure that their calls are not mixed with the illegal calls. Once these best practices are adopted by legal callers, the Commission can impose additional requirements on downstream and terminating providers to step up their blocking of suspicious calls, providing further incentives to legal callers to ensure that their calls are sent on legitimate call paths. Callers will be incentivized to use this method because it will facilitate the delivery of their calls, but the Commission's expanded blocking requirements may provide an additional stimulus.

To prevent the telephone system from becoming further degraded by the prevalence of illegal, dangerous, and invasive calls, we have urged the Commission to consider recommending and facilitating these types of best practices for legal callers.

Conclusion

I very much appreciate the opportunity to provide the Committee with our ideas and proposals for how to address illegal robocalls. Please let me know if you have questions.

Senator LUJÁN. Thank you very much, Ms. Saunders. Ms. Brown, the floor is yours for five minutes.

STATEMENT OF MEGAN L. BROWN, PARTNER, WILEY REIN LLP, ON BEHALF OF THE U.S. CHAMBER INSTITUTE FOR LEGAL REFORM

Ms. BROWN. Thank you very much. Good morning, Chairman Luján, Ranking Member Fischer, and members of the Subcommittee. My name is Megan Brown, and I am a partner in the telecom, media, and technology practice at Wiley Rein. I am here on behalf of the U.S. Chamber Institute for Legal Reform.

The U.S. Chamber is the world's largest business federation, representing the interests of more than 3 million businesses of all sizes and sectors, as well as State and local chambers and industry associations.

Its Institute for Legal Reform is a division of the chamber that promotes civil justice reform at the global, national, State, and local levels. Thank you for the opportunity to testify. The Chamber has been involved in robocalling issues for years and offers the per-

[90] Both YouMail and ZipDX capture audio evidence and other material information on tens of thousands or millions of illegal calls daily. YouMail's solutions assist subscribers by identifying likely illegal calls, transferring those calls to voice-mail, and then, with the permission of the called consumers, capturing and transcribing the content of these calls. ZipDX performs similar functions using banks of its own telephone numbers (referred to as honeypots) to receive the calls. Both platforms categorize and analyze the calls, providing extensive detail about call patterns and call paths as well as transcripts of the illegal calls. Both can also identify which telephone providers are continuing to provide STIR/SHAKEN attestations to illegal calls even after receiving notice of the bad traffic.

spective of the American business community which values reliable and trustworthy ways to communicate with customers and the public.

This is a highly regulated space with lots of litigation, something the Chamber has been vocal about for years because TCPA remains a major source of class action litigation that, in its view, does little to help consumers. So, the Chamber today would like the Committee to leave with four main points.

First, American businesses support cracking down on illegal and abusive robocalls. Businesses want consumers to continue to trust the ecosystem and answer their calls and texts. American businesses work hard to comply with these very complex regulations at the Federal and State level.

They are hurt by caller ID spoofing and fraud against consumers. And because of those harms, companies are fighting back against robocall scams. For example, Marriott did its own investigation into millions of calls placed illegally using—misusing its brand. It worked with the Industry Traceback Group and YouMail, and then it sued the malicious robocallers, getting an injunction against the marketing agency that placed all these calls—bless you. U.S. businesses take the law seriously and work hard to comply with it.

Second, Congress has passed major legislation recently on a bipartisan basis to address illegal robocalls. You can ensure that your hard work bears fruit by encouraging the Department of Justice to make robocall scams and illegal spoofing a priority.

The Federal Communications Commission has taken major steps to implement all of this new Congressional direction, and I know FCC staff have been working really hard on these issues. They have issued enormous forfeiture orders against bad actors that blatantly break the law, and its cease and desist orders have been particularly impactful.

Likewise, the Federal Trade Commission has been addressing scams using illegal robocalls and texts, and State Attorneys General have partnered with Federal agencies and bring their own cases. DOJ, however, is a vital partner here, and Congress should urge the Department to make enforcement a priority by acting aggressively on the referrals it gets from the FCC and by bringing its own cases directly for violations of laws like the Truth in Caller ID Act, but also mail and wire fraud for some of these really egregious scams.

Third, unfortunately, the TCPA's private right of action and statutory damages continue to fuel abuse of litigation against American businesses. The Institute for Legal Reform has tracked lawsuit abuse for years and the operating environment under the TCPA continues to hurt businesses and consumers.

Class actions seeking enormous damages and attorneys? fees, professional to TCPA plaintiffs, and the threat of crushing liability for mistakes creates a challenging environment for American businesses. An important takeaway here is that the TCPA class actions and those large settlements do not address the bad actors that are intentionally violating Federal law to send millions of illegal calls.

Here I have in mind people like Adrian Abramovich, Greg Robbins, John Spillers, or the shell companies that they used to make massive numbers of fraudulent calls, often pretending to be legiti-

mate American businesses. Fourth, the Chamber knows that some on this committee are considering additional legislation.

Congress has been active on robocalling over the past several years, and the Chamber suggests that if the Committee goes forward with legislation, it should also consider modest but important changes that would limit the abuse of our judicial system through TCPA class actions that do not stop bad actors.

So, in sum, the Chamber appreciates the Committee's attention to these issues, as well as the hard work of the FCC, State AGs, and the other panelists here to go after bad actors that abuse our networks, steal corporate goodwill, and harm consumers. Thank you for the opportunity to testify.

[The prepared statement of Ms. Brown follows:]

PREPARED STATEMENT OF MEGAN L. BROWN, PARTNER, WILEY REIN LLP, ON BEHALF OF THE U.S. CHAMBER INSTITUTE FOR LEGAL REFORM

Thank you Chair Luján, Ranking Member Thune, and members of the Subcommittee. My name is Megan Brown, and I am a partner in the Telecom, Media and Technology practice at Wiley Rein LLP. I am here on behalf of the U.S. Chamber Institute for Legal Reform ("ILR"). The U.S. Chamber is the world's largest business federation, representing the interests of more than three million businesses of all sizes and sectors, as well as state and local chambers and industry associations. The ILR is a division of the U.S. Chamber that promotes civil justice reform through regulatory, legislative, judicial, and educational activities at the global, national, state, and local levels. Thank you for the opportunity to testify today about the robocalling landscape and how American businesses are protecting consumers.

I would like to leave the Subcommittee with four main points today:

- ***First,*** legitimate businesses support efforts to crack down on illegal and abusive robocalls in order to create a safe communications ecosystem; businesses have every incentive to ensure that consumers continue to trust the ecosystem and answer calls and texts.
- ***Second,*** Congress can ensure that its already-substantial efforts to address illegal robocalls bear fruit by ensuring that Federal agencies—and particularly the Department of Justice ("DOJ")—make illegal robocalls an enforcement priority.
- ***Third,*** the Telephone Consumer Protection Act's ("TCPA") private right of action continues to fuel abusive litigation against American businesses. This difficult operating environment hurts businesses and consumers, and Congress should distinguish between good calls—such as appointment reminders, notifications about school closures, and other communications that consumers want—and bad calls, such as fraudulent and harassing communications that originate from bad actors.
- ***Fourth,*** the Subcommittee could consider modest changes to the TCPA to limit the abuse of our judicial system through class actions that do nothing to stop bad actors—many of whom flagrantly and repeatedly violate existing laws.

I. Industry Supports A Safe And Trustworthy Communications Ecosystem And Is Devoting Resources To Protecting Consumers From Scammers.

Legitimate businesses have no interest in the perpetuation of illegal and abusive robocalls. The illegal robocalls that continue to plague U.S. consumers originate with bad actors that seek to defraud consumers and exploit the brand names and goodwill of trusted American companies. The business community abhors this conduct and shares Congress's concerns about protecting consumers.

Indeed, the entire business community suffers when consumers cannot trust calls and text messages. Legitimate businesses use automated tools every day to communicate with the public. As former FCC Commissioner Michael O'Rielly explained, "information is often better and more accurately conveyed by dialing automatically from a list or through pre-recorded messages rather than through a live operator."[1]

[1] Remarks of FCC Commissioner Michael O'Rielly Before the Washington Insights Conference, FCC, at 3–4 (May 16, 2019), *https://www.fcc.gov/document/orielly-remarks-aca-intl-washington-insights-conference ("O'Rielly Remarks").*

For example, businesses may opt to use robocalls or robotexts to deliver "flu shot reminders," "food delivery order alerts," "customer satisfaction surveys," and other messages.[2] But if consumers are inundated with illegal and abusive robocalls, they may ignore or doubt the veracity of these helpful communications.[3]

Further, legitimate businesses, including small businesses, are also victims of illegal and abusive robocalls. For example, businesses face the serious risk from illegal robocalls of dilution of their brand through impersonation fraud. Indeed, "1 in 3 businesses" report having "had their name used by an impersonator making scam calls."[4] The Federal Trade Commission ("FTC") concurred with this data, finding last year in a notice of proposed rulemaking that business "impersonation fraud is" both "prevalent" and "harmful."[5] This fraud carries serious consequences for businesses: 13 percent of consumers "have since switched brands after receiving an impersonation call."[6] The U.S. Chamber supports the FTC 's continued enforcement in this space to address business impersonation fraud.

The risks to businesses from impersonation fraud do not stop at the business being impersonated. For example, a common scam is for fraudsters to impersonate representatives from Internet search engines and threaten to delist businesses from search results if they do not hand over personal information. With their livelihood on the line, these businesses may comply, exposing companies to identity theft.[7] This scam creates two business victims—the company being impersonated and the company being targeted.

Because of significant harms to consumers and businesses from robocall scams, companies are fighting back against robocallers directly. For example, a major hotel chain brought its own trademark lawsuit against malicious robocallers and earlier this year obtained an injunction against a marketing agency that placed millions of calls illegally using its brand name.[8] Other companies are devising innovative technologies to ward off illegal calls, such as analytics-powered software.[9]

The private sector partners with the Government in tackling illegal and abusive robocalls. The Industry Traceback Group ("ITG"), is a group of "companies from across the wireline, wireless, VoIP, and cable industries" that "collaborate to trace, source, and ultimately, stop illegal robocalls."[10] The ITG has conducted more than 10,000 tracebacks over the past three years[11] supporting state and Federal investigations. As the FCC explained, the ITG's efforts have "played a key role in combating the scourge of illegal robocalling campaigns."[12]

The telecommunications industry also has developed technology to help in the fight. Industry technologists developed a standard called STIR/SHAKEN to authenticate caller ID information for calls carried over an IP network to "combat illegal spoofing."[13] With the TRACED Act, Congress mandated the use of this industry-spearhead approach.[14]

These are just a few examples of the business community's many efforts to address illegal and abusive robocalls.

---

[2] TCPA Litigation Sprawl: A Study of the Sources and Targets of Recent TCPA Lawsuits, U.S. Chamber Institute for Legal Reform, at 4–5 (Aug. 2017), *https://instituteforlegalreform.com/research/tcpa-litigation-sprawl-a-study-of-the-sources-and-targets-of-recent-tcpa-lawsuits/ ("TCPA Litigation Sprawl").*

[3] *See* State Of The Call 2023,Hiya, at 11, available at *https://www.hiya.com/ state-of-the-call* (updated June 2023) *("State Of The Call 2023")* ("17 percent of businesses report a decline in answer rates due to spam calls").

[4] *State Of The Call 2023* at 9.

[5] *Trade Regulation Rule on Impersonation of Government and Businesses,* Notice of Proposed Rulemaking, 87 Fed. Reg. 62,741, 62,746 (Oct. 17, 2022).

[6] *State Of The Call 2023* at 10.

[7] *See Robocall Scam of the Week: Google Business Scam,* YouMail (Feb. 22, 2023), *https://blog.youmail.com/2023/02/robocall-scam-of-the-week-google-business-scam/*.

[8] *See Marriott Int'l, Inc. v. Dynasty Mktg. Grp. LLC,* No. 1:21–CV–0610, 2023 WL 2230433 (E.D. Va. Feb. 6, 2023), *report and recommendation adopted,* 2023 WL 2226782 (E.D. Va. Feb. 24, 2023).

[9] *See* Haley Henschel, *7 of the Best Robocall Blocking Apps and Tools for Avoiding Phone Spam,* Mashable (Apr. 26, 2023), *https://mashable.com/roundup/best-robocall-blocking-apps.*

[10] *See Industry Traceback Group, https://tracebacks.org/* (last visited Sep. 25, 2023).

[11] FCC Report to Congress On Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information, FCC, at 19 (Dec. 23, 2022), *https://docs.fcc.gov/public/attachments/DOC-390423A1.pdf ("2022 TRACED Report").*

[12] *Id.*

[13] *Call Authentication Tr. Anchor; Implementation of Traced Act Section 6(a)—Knowledge of Customers by Entities with Access to Numbering Res.,* Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd. 3241, ¶5 (2020).

[14] *See* Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116–105, §4(b)(1)(A)-(B), 133 Stat. 3274, 3277 (2019).

II. Congress Should Ensure That Prosecuting Illegal Robocallers Is A Priority.

A. Fraudulent And Abusive Robocalls Are Already Illegal.

Illegal and abusive robocalls do not stem from a lack of laws on the books. To the contrary, the TCPA and its associated rules prohibit autodialed and artificial or prerecorded voice robocalls to personal numbers unless the consumer consents or the call is otherwise permitted (*e.g.,* calls made for emergency purposes).[15] The TCPA also establishes a number of other robust protections for consumers with respect to telemarketing and solicitation calls—regardless of the technology being used to place the call.[16] Further, the TCPA is not the only tool in enforcers' toolbox to fight illegal actors. For example, the Truth in Caller ID Act of 2009—strengthened by the TRACED Act—broadly prohibits callers from "spoofing" their numbers "with the intent to defraud, cause harm, or wrongfully obtain anything of value."[17] Congress also empowered the FTC to "implement and enforce a national do-not-call registry,"[18] and under the FTC's Telemarketing Sales Rule ("TSR"), it is illegal to place most kinds of telemarketing calls to a number on the registry.[19] The TSR also prohibits deceptive and abusive telemarketing tactics and can be a powerful tool to go after bad actors.[20]

Illegal robocallers face serious potential criminal penalties. Fraud is of course a Federal crime. Specifically, the wire fraud statute provides for up to 20 years imprisonment for "devis[ing] any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises" over the phone.[21] In addition, the TRACED Act imposes criminal fines of $10,000 per violation of the prohibition on fraudulent spoofing.[22] Further, the Communications Act's general penalty provision provides that willful and knowing violators of the TCPA and its associated rules may be imprisoned and fined.[23]

In sum, the robocallers that target and harass American consumers and businesses with fraudulent scams have not found a legal loophole. Rather, they are already openly flouting the law.

B. There Has Been Progress In Stopping Illegal Robocalls.

Thankfully, we have seen progress in combatting the bad actors responsible for illegal robocalls. As the FCC's most recent report to Congress detailed, that agency pursues forfeitures for tens—and sometimes hundreds—of millions of dollars against the biggest robocalling operations targeting Americans.[24] Among these recent enforcement actions are the largest forfeitures in the agency's history: $225 million levied against a group of businesses that placed one billion fraudulent robocalls.[25] The FTC is also active, having recently initiated a lawsuit against a Voice over Internet Protocol ("VoIP") provider that funneled "hundreds of millions of illegal robocalls through its network."[26]

Businesses and States are supplementing these Federal enforcement efforts. A recently filed FTC complaint cites as evidence of robocalling violations "over 100 Traceback Requests" from the ITG, highlighting industry's crucial role in identifying illegal robocallers.[27] The States are likewise engaged. In July, a host of Federal agencies joined "attorneys general from all 50 states and the District of Columbia" in launching "Operation Stop Scam Calls"—an enforcement initiative to crack down

---

[15] 47 U.S.C. § 227(b)(1)(B), (2)(B); 47 C.F.R. § 64.1200(a).
[16] *See e.g.,* 47 C.F.R. § 64.1200(b), (c)(2).
[17] 47 U.S.C. § 227(e).
[18] 15 U.S.C. § 6151.
[19] 16 C.F.R. § 310.4(b)(1)(iii)(B).
[20] *Id.* §§ 310.4, 310.5.
[21] 18 U.S.C. § 1343.
[22] 47 U.S.C. § 227(e)(5)(B).
[23] 18 U.S.C. § 501.
[24] *See 2022 TRACED Report* at 5–6; *FCC Fines Telemarketer $225 Million for Spoofed Robocalls,* FCC (Mar. 18, 2021), *https://www.fcc.gov/document/fcc-fines-telemarketer-225-million-spoofed-robocalls. See also FCC Assesses Nearly $300M Forfeiture for Unlawful Robocalls,* FCC (Aug. 3, 2023), *https://www.fcc.gov/document/fcc-assesses-nearly-300m-forfeiture-unlawful-robocalls.*
[25] *Id.* at 6.
[26] Press Release, FTC, FTC Sues to Stop VoIP Service Provider That Assisted and Facilitated Telemarketers in Sending Hundreds of Millions of Illegal Robocalls to Consumers Nationwide (May 12, 2023), *https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-sues-stop-voip-service-provider-assisted-facilitated-telemarketers-sending-hundreds-millions.*
[27] Complaint ¶¶ 31–36, *United States v. Xcast Labs, Inc.,* No. 2:23–CV–3646 (C.D. Cal. May 12, 2023), ECF No. 1.

on illegal telemarketing calls.[28] And last year, a coalition of 50 state attorneys general formed a bipartisan Anti-Robocall Litigation Task Force that issued civil investigative demands to gateway providers suspected of routing "a majority of foreign robocall traffic."[29]

These efforts are yielding results. As one data point, consumers filed more than 100,000 informal FCC complaints about robocalls in 2018, but they filed under 40,000 in 2022.[30] Nevertheless, there is still a long way to go.

C. Robust Enforcement Is The Way To End Illegal Robocalls.

Despite all of this activity—including headline-grabbing FCC forfeiture orders—the Federal government is not doing enough to hold bad actors accountable. A lack of DOJ enforcement presents the biggest obstacle at this time.

DOJ has not been pursuing in court the forfeiture orders adopted by the FCC. The FCC recently reported that in "calendar year 2022," DOJ "did not collect any forfeiture penalties or criminal fines for violations of

[the TCPA] that the Commission has referred."[31] This is a missed opportunity for DOJ.

Nor is DOJ taking enough action to prosecute bad actors that actively and openly flout the law and seek to defraud Americans. DOJ has ample authority under the wire fraud statute and other provisions, as earlier described. And it has the means to use that authority because the ITG and other industry groups provide DOJ with tracebacks and other information that it could use. At the end of the day, however, it is DOJ that has to make the decision about whether to prosecute. While the DOJ has partnered with the FTC and others on some cases against robocallers,[32] DOJ does not appear to have made material prosecutions a high priority, which is particularly disappointing when it comes to recidivist robocall abusers.[33] As a former DOJ official myself, I see this as a profoundly squandered opportunity.

As lawmakers consider additional avenues to protect the public from illegal robocalls, it should consider ways to spur additional action from DOJ, such as:

- Requiring DOJ to file an annual report with Congress explaining enforcement activity it has undertaken in the last calendar year to combat illegal robocalls and its handling of FCC referrals, including the pursuit of forfeiture amounts. This requirement would be similar to the TRACED Act's annual TCPA reporting requirement for the FCC and should require DOJ to explain if and why it has not pursued FCC referrals.[34]
- Prioritizing DOJ funds for investigations and enforcement actions against illegal robocallers.
- Requiring DOJ to establish a robocall enforcement and education office.

However Congress might proceed, know that American businesses stand ready to assist DOJ and others in the fight against illegal and abusive robocalls.

III. The TCPA's Private Right Of Action Continues To Be The Source Of Ongoing Litigation Abuse, Which Does Not Address The Urgent Issue Of Combatting Bad Actors.

Although the TCPA has helped protect consumers, the same cannot be said for its private right of action. That provision is presently being abused by plaintiff's attorneys to seek enormous payouts from American businesses. Private TCPA lawsuits and the threat of litigation make it perilous for U.S. businesses to communicate with consumers. Although there was some initial thinking that the Supreme

---

[28] Press Release, FCC, FCC Joins Federal and State Robocall Partners to Launch 'Operation Stop Scam Calls' (July 18, 2023), *https://docs.fcc.gov/ public/attachments/DOC-395216A1.pdf.*

[29] Press Release, NCDOJ, Attorney General Josh Stein Leads New Nationwide Anti-Robocall Litigation Task Force (Aug. 2, 2022), *https://ncdoj.gov/attorney-general-josh-stein-leads-new-nationwide-anti-robocall-litigation-task-force/.*

[30] *See 2022 TRACED Report* at 5.

[31] *See 2022 TRACED Report* at 7.

[32] Press Release, DOJ Office of Public Affairs, U.S. Department of Justice, Federal Trade Commission, Federal Communications Commission and Other Federal and State Law Enforcement Agencies Announce Results of Nationwide Initiative to Curtail Illegal Telemarketing Operations (July 18, 2023), *https://www.justice.gov/opa/pr/us-department-justice-federal-trade-commission-federal-communications-commission-and-other#:~:text=The%20department's%20Consumer%20Protection%20Branch,that%20transmitted%20illegal%20phone%20calls.*

[33] *In the Matter of Sumco Panama SA et al.,* Forfeiture Order, File No. EB–TCD–21–00031913, FCC 23–64, ¶12 (Aug. 3, 2023) ("Cox and Jones, key participants in the Enterprise, are currently banned from any form of telemarketing, and have been since 2013 and 2017, respectively. However, they have continued illegal telemarketing practices by using an international network of companies to conceal their involvement.").

[34] 47 U.S.C. §227(h).

Court's 2021 decision in *Facebook v. Duguid*[35] would significantly improve the situation, well-meaning businesses continue to be harassed by harmful and opportunistic TCPA lawsuits. This ultimately harms the ability of consumers to utilize modern communications tools and access innovative services. Ultimately, any discussion of robocalling and the TCPA must distinguish between legitimate and lawful communication on the one hand, and abusive scam calls on the other.

A. Not All Automated Calls Are Bad.

Automated calls and texts can provide an efficient and effective means of communication to which consumers regularly and willingly consent. As a former FCC Commissioner explained: "There are good and legal robocalls, and there are scam and illegal robocalls, and it's the latter that are wreaking havoc on the Nation's communications networks."[36] Such a distinction is critical. Consider some of the ways in which institutions use robocalls and robotexts to communicate:

- "Alerts from a school that a child did not arrive at school, or that the building is on lockdown."
- "Notifications regarding storm alerts, utility outages, and service restoration."
- "Immunization reminders for underserved, low-income populations."
- "Updates from airlines" to provide critical flight information to passengers.
- "Text messages from taxi and ridesharing services to alert customers when their driver has arrived."[37]

Such automated communications are not merely convenient; they are effective. For example, "significantly more patients who received automated telephone messages regarding hypertension treatment achieved blood pressure control than patients who received ordinary care only."[38] Likewise, energy companies have reported survey data showing "that customers would like outage and restoration notifications, and prefer communications via text message or telephone call, with e-mail being the least requested method of contact."[39]

These beneficial communications are also protected by the First Amendment. The Supreme Court has long recognized that the Government may not "suppress the dissemination of concededly truthful information about entirely lawful activity," even when dissemination is "commercial" in nature.[40] In striking down part of the TCPA as unconstitutional in 2020, the Supreme Court confirmed that robocalls constitute speech protected by the First Amendment.[41]

In sum, there are many beneficial robocalls that provide customers with timely, convenient, and desirable information. The Chamber urges this body to avoid conflating those calls with the fraudulent and harmful calls placed by scammers and abusers.

B. The TCPA Encourages Litigation Against American Businesses Instead Of Bad Actors.

Unfortunately, the TCPA continues to be abused and inhibits constitutionally protected pro-consumer communications. The Chamber's research has repeatedly shown how the TCPA has created a cottage industry of unnecessary and often abusive class-action litigation, burdening how businesses reach their customers, while doing little to stop truly abusive robocalls and protect consumers.[42] This litigation cash

---

[35] *Facebook, Inc. v. Duguid,* 141 S. Ct. 1163 (2021).

[36] *O'Rielly Remarks* at 3.

[37] *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 et al.,* Declaratory Ruling and Order, 30 FCC Rcd. 7961, 8084–85 (2015) (O'Rielly, Comm'r, dissenting in part and approving in part) *("2015 TCPA Declaratory Ruling and Order").*

[38] *Id.* at 8085 (alterations omitted).

[39] *Id.* at 8086 (internal quotations omitted).

[40] *Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc.,* 425 U.S. 748, 771–73 (1976).

[41] *See Barr v. Am. Ass'n of Pol. Consultants, Inc.,* 140 S. Ct. 2335, 2347 (2020) (plurality) ("The law here focuses on whether the caller is *speaking* about a particular topic." (emphasis in original)); *id.* at 2357 (Sotomayor, J., concurring) (concluding that relevant provision of the TCPA unconstitutionally burdened "robocall speech" (internal quotations omitted)); *id.* at 2364 (Gorsuch, J., concurring) ("no one doubts the TCPA regulates speech.").

[42] *See, e.g., TCPA Litigation Sprawl;* Ill-Suited: Private Rights of Action and Privacy Claims, U.S. Chamber Institute for Legal Reform (July 2019), *https://instituteforlegalreform.com/wp-content/uploads/2020/10/Ill-Suited - Private Rights of Action and Privacy Claims Report .pdf;* Turning the TCPA Tide: The Effects of Duguid, U.S. Chamber Institute for Legal Reform (Dec. 2021), *https://instituteforlegalreform.com/wp-content/uploads/2021/12/1323_ILR_TCPA_Report_FINAL_Pages.pdf ("Turning the TCPA Tide").*

cow has become a major obstacle, inhibiting legitimate and lawful communications between businesses—large and small—and their customers. It places businesses at risk for potential litigation each time they pick up the phone or send a text message. And it does nothing to address the real bad actors: repeat scammers who abuse our communications networks to harm consumers.

Indeed, just a handful of plaintiff's lawyers—and some professional *pro se* plaintiffs—are responsible for the majority of the thousands of TCPA cases brought each year.[43] Repeat TCPA plaintiffs also come up with ways to game the system—such as purchasing dozens of prepaid cellphones—to procure huge cash payouts.[44] One serial TCPA plaintiff in New Jersey has filed over 30 TCPA lawsuits, pocketing as much as $800,000.[45] Another has filed more than fifty cases in the Northern District of Texas in the last decade.[46]

ILR's members know firsthand the difficulties with this kind of "gotcha" operating environment. The statute's private right of action is expansive. Any person who receives an unlawful robocall may bring a lawsuit to recover $500–$1,500 per call.[47] There is no cumulative limit to these damages, leading some plaintiff's lawyers to seek mind-boggling damages awards. Further, massive classes—such as a recent class certification of over one million people in a TCPA case against a bank[48]—is often sufficient to drive companies into a coercive settlement. For example, one lawsuit alleging violations of the TCPA for advertisements led to a class action settlement fund of $35 million with 1,237,296 class members.[49] Other examples include a class action settlement with a telecommunications company for $45 million[50] and another with a utility services company for $38.5 million.[51]

With enormous potential damages in play, plaintiffs have little incentive to go after criminal or overseas scammers, who offer a miniscule chance to generate easily such large payouts.[52] Instead, TCPA plaintiffs have opted to target legitimate businesses—many of them household names—and not the offshore robocallers flooding Americans' phones with fraud and scam calls. Consider some examples of recent targets of TCPA lawsuits:

- The City of Albuquerque was sued after sending text messages to local residents during the COVID–19 pandemic, notifying them of the opportunity to engage in socially-distanced town halls.[53]
- Serve All, Help All, a non-profit company that provides financial aid and assistance to those with housing needs, was sued by a serial *pro se* litigant[54] for an automated phone call offering a Public Service Announcement for homeowners in default.[55]
- A ride-share company was sued for notifying a driver that he needed to update an expired driver's license.[56]

---

[43] *See e.g., Johansen v, Bluegreen Vacations Unlimited, Inc.,* No. 20–81076–CIV, 2021 WL 4973593, at *1 (S.D. Fla. Sept. 30, 2021), *aff'd,* No. 22–10695, 2022 WL 17087039 (11th Cir. Nov. 21, 2022) ("Plaintiff appears to have an extensive history with filing lawsuits alleging violations of the TCPA. (See Pl. Dep. (estimating that, prior to 2020, Plaintiff had filed sixty (60) TCPA lawsuits and estimating that, since 2014, Plaintiff has made on average $60,000 per year from TCPA lawsuits).)") (some internal citations omitted); *see also TCPA Litigation Sprawl* at 4 ("around 60 percent of the TCPA lawsuits examined in the study's 17-month period were brought by only 44 law firms/lawyers, with two firms filing well over 200 TCPA litigations each.").

[44] *TCPA Litigation Sprawl* at 15.

[45] *Id.*

[46] *Hunsinger v. Offer, LLC,* No. 3:21–CV–2846, 2022 WL 18143951 (N.D. Tex. Dec. 7, 2022).

[47] 47 U.S.C. § 227(b)(3).

[48] *Head v. Citibank, N.A.,* 340 F.R.D. 145, 149 (D. Ariz. 2022).

[49] *Drazen v. Pinto,* 41 F.4th 1354 (11th Cir. 2022), *reh'g en banc granted, opinion vacated,* 61 F.4th 1297 (11th Cir. 2023).

[50] Final Judgment ¶ 14, *Joel Hageman v. AT&T Mobility LLC,* No. 1:13–CV–00050 (D. Mont. April 9, 2013), ECF No. 68.

[51] *Jenkins v. Nat'l Grid USA Serv. Co., Inc.,* No. 15–CV–1219, 2022 WL 2301668, at *3 (E.D.N.Y. June 24, 2022).

[52] *See* David Adam Friedman, *Impostor Scams,* 54 U. Mich. J.L. Reform 611, 658 (2021), *https://repository.law.umich.edu/cgi/viewcontent.cgi?article=2527&context=mjlr* (explaining that parties "increasingly responsible for the majority of TCPA violations are located overseas" and are often "judgment proof.").

[53] *Silver v. City of Albuquerque,* No. 1:22–CV–00400, 2023 WL 2413780 (D.N.M. Mar. 8, 2023).

[54] The plaintiff filed 11 TCPA lawsuits in the Western District of Washington in 2021, two lawsuits in 2022, and this lawsuit in 2023.

[55] *Barton v. Serve All, Help All, Inc.,* No. 3:21–CV–05338, 2023 WL 1965905, at *1 (W.D. Wash. Feb. 13, 2023), *motion to certify appeal denied,* No. 3:21–CV–05338, 2023 WL 2372904 (W.D. Wash. Mar. 6, 2023).

[56] *Eller v. Uber Technologies, Inc.,* No. 4:23–CV–03526 (S.D. Tex. Sept. 19, 2023).

This litigation environment makes it hard to communicate. Indeed, much of the recent litigation involves technical errors and honest mistakes. In one recent case where a technical glitch resulted in a company accidentally misdialing consumers, the defendant settled almost immediately to avoid potentially paying more than $4 million for the 8,645 alleged violations of TCPA.[57] In another case, a court treated the TCPA as a strict liability statute, finding that a company could be on the hook for damages where it called a number for which consent had been obtained but—unbeknownst to the company—the number was subsequently reassigned to a different consumer.[58] The court so held, notwithstanding a regulatory "safe harbor" that is designed to prevent this problem.[59]

The end result is that well-meaning businesses committed to compliance can nevertheless be subject to bet-the-company liability every time they call or text.

This system does not protect against the scammers and bad actors who continue to prey on consumers.[60]

C. Facebook v. Duguid Has Not Materially Improved The Situation.

There was some optimism after the Supreme Court's decision in *Facebook v. Duguid* that we would see a decline in frivolous TCPA lawsuits. In that case, the Court clarified that an "automatic telephone dialing system"—a key term in the TCPA—must use a random or sequential number generator.[61] Because some lower courts had previously found that *any* system capable of storing numbers could trigger TCPA liability, this interpretation clarified the statute's language and should have limited some lawsuits against callers. Several courts since have heeded the Supreme Court's interpretation and rejected efforts to evade it with strained arguments about equipment.[62]

Unfortunately, that has not happened. An ILR study concluded that although there was a short term reduction immediately following *Duguid* in the volume of TCPA lawsuits filed, most lawsuits were still "allowed to proceed to discovery instead of being dismissed at the pleadings stage."[63] Given the expense of discovery, plaintiff's attorneys still have ample leverage to coerce companies into massive settlements in a post-*Duguid* world.

Worse, that initial slowdown in TCPA lawsuits has now been reversed. TCPA filings year-to-date are up 16.8 percent from last year.[64] Even more problematic, there has also been an increase in class action lawsuits. More than 50 percent of the 2,457 TCPA cases filed in Federal court in 2022 and so far in 2023 have been class actions.[65] In August 2023 alone, 66.2 percent of all TCPA lawsuits filed were class actions.[66]

Thus, *Duguid* has not led to long-term meaningful protections against opportunistic TCPA lawsuits. Worse still, there have also been suggestions that the FCC should unilaterally revise key terms defined by Congress and definitively interpreted by the Supreme Court, suggesting that even this limited protection could be on the chopping block.[67]

---

[57] *Fralish v. Ceteris Portfolio Services, LLC,* No. 3:22–CV–00176, 2022 WL 19920239 (N.D. Ind. Mar. 7, 2022).

[58] *Hylton v. Titlemax of Virginia, Inc.,* No. 4:21–CV–163, 2022 WL 16753869, at *1 (S.D. Ga. Nov. 7, 2022).

[59] *Id.* at *5–*8; *see also* 47 C.F.R. § 64.1200(m).

[60] *In the Matter of Sumco Panama SA et al.,* Forfeiture Order, File No. EB–TCD–21–00031913, FCC 23–64, ¶ 1 (Aug. 3, 2023).

[61] *Facebook, Inc. v. Duguid,* 141 S. Ct. 1163, 1173 (2021).

[62] The Ninth Circuit and Third Circuit have followed the Supreme Court's interpretation. In *Borden v. eFinancial, LLC,* the Ninth Circuit held that an automatic telephone dialing system must "randomly or sequentially generate telephone numbers, not just any number." *Borden v. eFinancial, LLC,* 53 F.4th 1230, 1233 (9th Cir. 2022). Similarly, in *Panzarella v. Navient Solutions, Inc.,* the Third Circuit held that use of a system with the capacity to be an automatic telephone dialing system is not sufficient to establish a TCPA violation. Judgment, *Panzarella v. Navient Solutions, Inc.,* No. 20–2371 (3d Cir. June 14, 2022), ECF No. 60.

[63] *Turning The TCPA Tide* at 2.

[64] Eric J. Troutman, *HUGE INCREASE: TCPA Lawsuits Up Double Digits From Last Year—Class Action Numbers Spike,* TCPA World (Sept. 12, 2023), *https://tcpaworld.com/2023/09/12/huge-increase-tcpa-lawsuits-up-double-digits-from-last-year-class-action-numbers-spike/*.

[65] Westlaw Litigation Analytics, *Telephone Consumer Protection Act* (last visited Sept. 25, 2023).

[66] Eric J. Troutman, *HUGE INCREASE: TCPA Lawsuits Up Double Digits From Last Year—Class Action Numbers Spike,* TCPA World (Sept. 12, 2023), *https://tcpaworld.com/2023/09/12/huge-increase-tcpa-lawsuits-up-double-digits-from-last-year-class-action-numbers-spike/*.

[67] *See* Review of the FY 2024 Budget for the Federal Communications Commision: Hearing Before the S. Comm. on Appropriations' Subcommitte on Financial Services and General Gov-

Continued

D. The TCPA's Private Right Of Action Harms Consumers.

In all this talk about precedent and statistics, I do not want to lose track of what is at stake here. The TCPA's private right of action hurts businesses and consumers. Given that even innocent missteps can lead to business-ending liability, some companies may understandably choose to "cease communicating" altogether.[68] But, as explained above, many consumers *want* these communications. They want to know if their flight has been delayed, if their medication is ready for pickup, or if their child did not arrive at school. An *in terrorem* litigation environment that chills these communications is fundamentally anti-consumer.

IV. Modest Changes To The TCPA Could Limit Litigation Abuse.

Since the TCPA's 1991 enactment and in more recent legislation to address illegal robocalling, Congress has tried to strike a balance by addressing the abuse of mass communication tools while protecting the ability of businesses to communicate with customers using modern technology by delivering desired and timely communications in an efficient manner. The current litigation climate has seriously undermined that balance. If Congress wants to address the calling ecosystem, it could take steps to rein in the counterproductive abuse of the TCPA's statutory damages provision and the near-strict liability approach that has developed.

To restore that balance, Congress should consider modest changes to reduce abusive litigation under the TCPA, including:

- *Cumulative Damages Cap:* Total exposures in TCPA cases can become extraordinary because of the combination of statutory damages and large numbers of class members who may have received only one errant call and experienced no meaningful harm. Facebook in the *Duguid* case faced billions in potential damages, and there are countless examples of eyepopping settlements and damage calculations.[69] Congress should consider adding a cap on the TCPA's damages to help alleviate the specter of crushing liability for simple mistakes. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") offers a model for this approach. It caps penalties in tiers based on the culpability of the violator, with the low tier limiting the statutory penalty amount to "$100 for each such violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $25,000."[70] Congress could similarly impose a limit on the "total amount" of damages available under the TCPA.
- *Safe Harbor:* The law should provide businesses an opportunity to cure inadvertent alleged violations of the TCPA without being subjected to liability. Safe harbors allow businesses to remedy good-faith mistakes, thereby leaving consumers better off and allowing enforcers to better focus their efforts on true bad actors. The idea of a safe harbor is not unfamiliar in important societal issues. For example, the FTC's Children's Online Privacy Protection Act (COPPA) Safe Harbor Program allows industry groups to be considered in compliance with COPPA regulations if their proposed COPPA oversight programs are approved by the FTC.[71] Additionally, in May of this year, Florida amended the Florida Telephone Solicitation Act to allow consumers to respond with "STOP" to cease further text message solitications.[72] However, the law also provides a safe harbor period of 15 days for solicitors to react to the "STOP" text, and no action can be brought against a telephone solicitor unless a text is received more than 15 days after the initial "STOP" message was sent.[73]
- *Limit Attorney's Fees:* Congress should consider limiting attorney's fees that may be available in TCPA cases. One reason for the onslaught of TCPA litigation is that attorneys are incentivized to go after American businesses, regardless of culpability or actual consumer harm because large damage awards can generate large attorney's fees. Reasonable limits on attorney's fees could blunt that distorted incentive. Congress could borrow from other Federal statutes that limit attorney fee recoveries, ensuring that any damages award benefit consumers.

---

ernment, 118th Cong. (2023) (statement of Jessica Rosenworcel, Chairwoman, Federal Communications Commisson), *https://docs.fcc.gov/public/attachments/DOC-397034A1.pdf.*

[68] *2015 TCPA Declaratory Ruling and Order* at 8093.

[69] *See, e.g., Wakefield v. ViSalus, Inc.,* No. 3:15–CV–1857, 2019 WL 2578082 (D. Or. June 24, 2019) (denying request to treble $925,220,000 damage award).

[70] 42 U.S.C. § 1320d-5(a)(3)(A).

[71] 16 CFR § 312.11(b).

[72] H.B. 761, 2023 Leg., Reg. Sess., § 1 (Fla. 2023).

[73] Fla. Stat. § 501.059(10)(c).

Each of these approaches offer Congress a way to limit some of the most abusive TCPA litigation without undermining efforts to crack down on the bad actors responsible for harmful and abusive robocalls.

The business community wants to end illegal robocalls and foster a safe and trustworthy communications ecosystem for businesses and their customers. Companies take pains to comply with the TCPA and stand ready to continue assisting state and Federal partners to go after scammers and those who intentionally flout Federal and state law. As Congress considers paths forward, enforcement should remain a top priority of all Federal agencies and Congress should consider reforms to prevent legitimate businesses from being ensnared in abusive TCPA litigation.

I want to again thank the Subcommittee for the opportunity to discuss these important issues. I look forward to answering your questions.

Senator LUJÁN. Thank you—[technical problems]—very much for your testimony today. Mr. Bercu, the floor is yours for 5 minutes.

STATEMENT OF JOSHUA M. BERCU, EXECUTIVE DIRECTOR, INDUSTRY TRACEBACK GROUP; VICE PRESIDENT, POLICY & ADVOCACY, USTELECOM—THE BROADBAND ASSOCIATION

Mr. BERCU. Thank you, Chair Luján and Ranking Member Fischer, for the opportunity to join this important conversation.

I am Josh Bercu, Executive Director of the Industry Traceback Group, or ITG, and I also serve as Vice President of Policy and Advocacy at USTelecom, the Broadband Association. USTelecom established the ITG to address the illegal robocall problem, and today, pursuant to the TRACED Act, the ITG is designated by the FCC as the official consortium to traceback unlawful robocalls.

We are proud to support the FCC, FTC, DOJ, State Attorneys General, and other Government efforts to stop illegal robocalls through our traceback data. And I am pleased to be here today to discuss that collective effort and how Congress can bolster it.

As I explain in my written testimony, various technological and economic changes have made it cheap and easy for bad actors to call American consumers from anywhere in the world. All anyone needs to initiate robocalls is a computer, some associated software, and a website. In the past, providers had no true—had no way to know the true origin of the calls.

Industry traceback solves for that by piecing together the entire path of any given suspicious call, regardless of the number of providers involved. We obtained within a day or two the same information that would take enforcement agencies multiple months to get via subpoenas, and virtually all of the data we get makes its way to those enforcement agencies.

Thanks to ITG data, Federal and State agencies are bringing more enforcement actions against illegal robocallers than ever before, and these efforts are working. For example, data from my colleagues at YouMail show that scam robocall volumes have dropped over 50 percent from their peak in October 2019.

And after FCC and State enforcement actions based on ITG tracebacks, the billions of auto warranty robocalls that were plaguing Americans early last year have dropped almost to zero. Notably, even absent any affirmative enforcement action, tracebacks disrupt illegal robocalls in real time.

Nearly 85 percent of completed tracebacks result in the originating provider warning or firing its offending customer. But as industry and Government innovate to fight illegal robocalls, so do their perpetrators.

For instance, instead of robocallers, robocalls, scammers are now making more targeted live calls, sometimes combined with communications through other channels. The scammers know precisely who they are calling as they convincingly pretend to be your bank, for example.

Also, the decline in scam robocalls has been supplanted by a substantial rise in unsolicited and unwanted telemarketing robocalls. These are the robocalls your constituents are most likely to receive today.

A consumer may sign up on a job listing website, for example, but miss the fine print linking to a second page with hundreds or thousands of marketing partners that each now purportedly have the consumer's consent for robocalls.

Even worse, ITG evidence suggests that these already flimsy claims of consent could be entirely falsified by bots consenting on behalf of consumers for calls they never asked for and do not want.

While the STIR/SHAKEN, and call authentication framework makes it harder to send spoofed calls to consumers, prolific robocalls now engage in number rotation where they cycle through assigned, not spoofed numbers, sometimes for a single call per number.

But this practice is intended to evade industry safeguards, and harms both consumers and legitimate callers, because calls from new numbers are far more likely to be treated as spam as a result.

In my written testimony, I provide several steps that Congress can take to further empower industry and Government efforts to stop illegal robocalls, but I want to emphasize a few today. First, Congress should ensure that DOJ prioritizes prosecuting the criminals behind unlawful robocalls.

Second, to address problematic number rotation, Congress should formally expand the role of the Traceback Consortium to investigate how bad actors get access to scores of numbers.

Third, Congress should reintroduce and pass the Robocall Traceback Enhancement Act, which Senators Thune and Markey introduced last Congress to protect the consortium in the work protecting consumers. Thank you again for the opportunity to speak.

We look forward to continuing to collaborate with the Subcommittee and Federal and State Government partners in solving the illegal robocall problem.

[The prepared statement of Mr. Bercu follows:]

PREPARED STATEMENT OF JOSHUA M. BERCU, EXECUTIVE DIRECTOR, INDUSTRY TRACEBACK GROUP; VICE PRESIDENT, POLICY & ADVOCACY, USTELECOM—THE BROADBAND ASSOCIATION

Thank you Chair Luján and Ranking Member Thune for the opportunity to speak on behalf of the Industry Traceback Group (ITG) and USTelecom—The Broadband Association (USTelecom), which leads the ITG.

I am Josh Bercu, and I serve as the Executive Director of the ITG, and also as Vice President, Policy & Advocacy at USTelecom. I have held these roles for over three years, and before that, for nearly a decade, I was in private practice focusing on privacy, consumer protection, and telecommunications law.

I am pleased to be here today to share my insights on why this country has an illegal robocall problem and what industry together with Federal and state government partners is doing to address it. Illegal and unwanted robocalls started to grow and get out of control in the early 2010s. The problem grew in large part because of the rise of the internet-based calling technology known as voice over Internet protocol, or "VoIP." VoIP technology made it easier and more affordable for consumers

to call their friends and family anywhere in the world, but it also made it cheap and easy for bad actors to call American consumers from anywhere in the world. These bad actors care little about the legal restrictions that apply to such calls.

Worse, many VoIP platforms based here and abroad allowed bad actor callers to input any number into the caller ID field, a practice known as spoofing. Over the years, we have seen bad actors experiment with spoofing to increase the odds that their fraudulent calls are answered by unsuspecting consumers. Their practices evolved to use the same or neighboring area codes, a practice known as "neighborhood spoofing," as well as quickly cycling through calling numbers to evade the blocking and labeling tools carriers have deployed, a practice known as "snowshoeing." Sometimes bad actors also spoof the telephone numbers of government agencies, banks, or other well-known brands.

It would be reasonable to question why the phone network allowed spoofing in the first instance. There are some legitimate spoofing use cases, as Congress recognized when it passed the Truth in Caller ID Act, making spoofing illegal only with the intent to defraud, cause harm, or wrongfully obtain anything of value. For instance, domestic violence shelters often spoof outbound calls to hide the victim's location. Enterprises and call centers frequently spoof an outbound number to provide a better number to call back. Congressional telephone town hall calls do the same, displaying the Member of Congress's office number rather than a number tied to the platform vendor.

It is also based on the nature of how the phone network evolved. Before VoIP, to be a phone provider, you had to lay wire to each customer's physical location. It was a high capital, expensive business. And when you wired a local bank or call center, you generally knew they were a real entity. You knew your customer. With VoIP and Internet technology, that is no longer the case. Today all anyone needs to be a phone provider or calling platform is a computer, some associated software, and a website.

The U.S. phone system is a collection of interconnected telephone networks. Therefore, in most cases—and certainly before the deployment of the STIR/SHAKEN call authentication framework that has made it harder to spoof calls—providers had no reliable way to know where a given call actually originated from and who made it. And given the nature of an interconnected network, where a provider found a problem and fired a calling customer or wholesale provider because of questionable call traffic, the offending traffic often still made its way to the provider—just through additional wholesale providers, or "hops." In the ITG's experience, illegal robocalls average six hops before they get to the call recipient.

Given these challenges, in July 2016, then-AT&T CEO Randall Stephenson responded to then-Federal Communications Commission (FCC) Chairman Tom Wheeler's request to establish an industry task force to address the growing robocall problem. The result was the industry-led Robocall Strike Force, through which a broad cross-section of the industry brainstormed creative solutions to abate the proliferation of illegal and unwanted robocalls and promote greater consumer control over the calls they wish to receive. The Strike Force ultimately made numerous recommendations to the industry as well as to the FCC, including but not limited to deploying the STIR/SHAKEN call authentication framework and expanding traceback efforts.

The deployment of the STIR/SHAKEN call authentication framework has undoubtedly made it harder to get spoofed calls through to consumers. In response, we have seen a shift to a practice called "number rotation," where callers making hundreds of thousands of robocalls no one asked for cycle through *assigned* – not spoofed—numbers, sometimes averaging only 1.2 calls per number. This practice—designed to evade the protections that the industry has deployed—not only harms consumers, it also harms legitimate callers. That is because the analytics show that a new calling number is far more likely to be a spam call than a real call, impacting how calls from such numbers are treated by analytics providers and their carrier partners.

The Industry Traceback Group was a voluntary industry initiative established by USTelecom in 2015. USTelecom initially established it as a working group to explore the notion of industry tracebacks, and then evolved it to a broader and more formal industry effort to systematically conduct tracebacks. The effort expanded to include representatives beyond USTelecom members and from across the telecommunications industry. The TRACED Act then created a formal role for industry traceback through the establishment of the registered traceback consortium, which the FCC followed up with a mandate to cooperate with traceback requests from the consortium. We are proud that the FCC recently designated the ITG as the official traceback consortium for the fourth year in a row.

Prior to the ITG's establishment, the true origin of illegal robocalls was difficult to discern given the interconnected nature of the phone network, the potential for multiple voice service providers to be involved in the path of a single call, and the limited information that each provider has about the traffic they receive with any given call. Industry traceback solves for these challenges. As a general matter, all any voice service provider in the call path knows is the *direct* upstream provider from whom it received the call. And that is the primary information we request from each voice service provider in the call path of a traceback. Through this process, the ITG is able to rapidly piece together the path of any given suspected unlawful robocall, regardless of the number of providers in the call path.

The ITG obtains data of suspected illegal call examples from various sources, including analytics companies, honeypots, or referrals from law enforcement or others harmed by the calls. The ITG team reviews the examples to ensure that we have information to support a reasonable suspicion that the given call campaign and examples are fraudulent, abusive, or otherwise unlawful. We then initiate tracebacks that are representative of hundreds of thousands or millions of illegal calls. Our system sends notifications to each provider in the call path and continues hop to hop to hop until we identify the provider that originated the call as well as its customer. We also find out other information along the way, including the provider that let the call into the country, in instances where the call originated overseas.

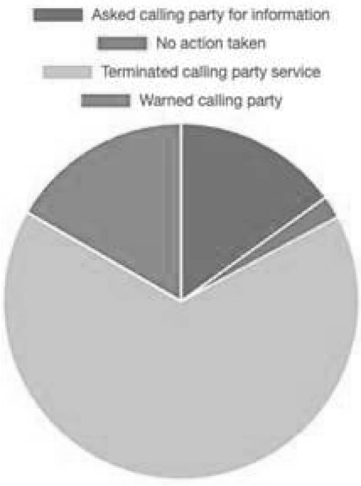
Today, providers from across the phone ecosystem support and guide the ITG effort, and hundreds more cooperate, including hundreds of providers located abroad that send calls to the United States. We often get results within a day or two, whereas it would take two or three months for an enforcement agency to get the same information through subpoenas and investigative demands. And through the ITG's ongoing innovation and enhancements to the process, we are conducting tracebacks at much greater scale across a wider set of campaigns and calls.

Generally speaking, there are three types of calls that the ITG traces back:

- ***Government and Brand Imposter Calls.*** Fraudulent high-volume robocalls that impersonate the Social Security Administration, sheriff offices, utilities, financial institutions, technology companies, and the like. In our experience, these calls predominantly originate abroad.
- ***Unsolicited Lead Generation Telemarketing Calls.*** Unsolicited high-volume lead generation telemarketing calls. These calls seek to sell a service or product, *e.g.,* warranty, insurance, or debt reduction products, but in violation of consent requirements, and sometimes trademark law as well. These are the robocalls that your constituents are most likely to receive today.
- ***Malicious Live Calls.*** Targeted attacks, often with a live caller. These include voice phishing (or "vishing") attempts, "Grandma scams," swatting calls, and more. For instance, earlier this year, the ITG worked with a local police department in Indiana to traceback a series of spoofed calls, including bomb and mass shooting threats to a high school and a swatting call targeting a student in the school, helping the police apprehend the suspect before any harm was done.

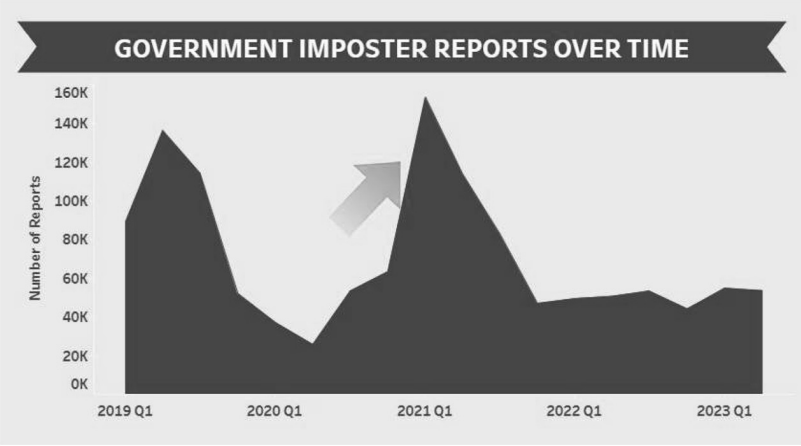
Tracebacks generate information about the entities responsible for the illegal calls, and traceback has enabled more FCC, Federal Trade Commission (FTC), and other Federal and state enforcement actions to be efficiently and quickly brought against robocallers and their enablers than ever before. But equally important, even absent any affirmative enforcement actions, tracebacks also disrupt the flow of illegal calls in real time. Nearly 85 percent of completed tracebacks result in the originating provider warning or firing its offending customer, which is up almost 20 percent from 2022.

Actions Taken by Originating Providers in Response to ITG Tracebacks



Providers that do not cooperate with tracebacks, or fail to comply with straightforward FCC rules like filing in the FCC's Robocall Mitigation Database, are identified, and the providers that accept their traffic are put on clear notice that the provider they are accepting traffic from is not complying with applicable rules. This puts the downstream provider in a position to take corrective action or face a potential Federal or state enforcement action.

But beyond immediate disruption, the collective work of industry and government is having a more persistent impact. According to YouMail data, scam robocall volumes have dropped 50 percent since January 2019, and 55 percent since they peaked in October 2019. Once prevalent robocalls purporting to be the Social Security Administration and other government entities are increasingly rare, a trend that correlates to an overall decline in government impersonation scams.

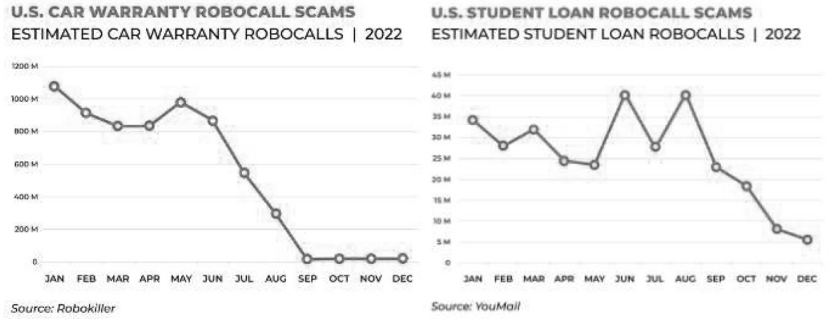


Source: FTC Consumer Sentinel

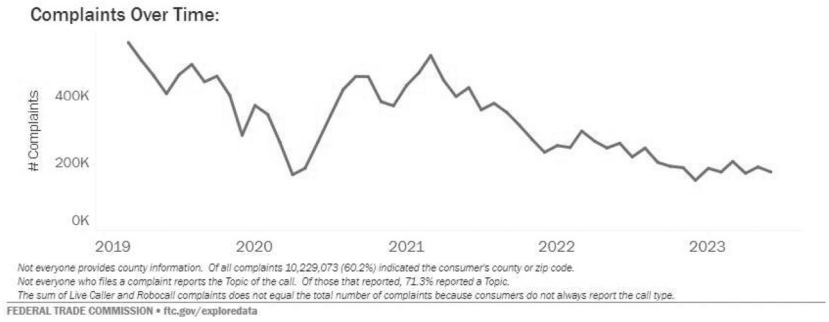
The drop in scam robocalls has unfortunately been supplanted by a substantial rise in unsolicited telemarketing calls. The lead generators responsible for these billions of unwanted robocalls do not sell any product or service; rather, as the government has alleged in one case, they act as "a massive 'consent farm' enterprise, using deceptive ads and websites to induce nearly one million consumers a day to provide

their personal information and purported consent to receive telemarketing calls." [1] These lead generators then sell these questionably obtained consents to various third parties. For example, a consumer may sign up for a job listing website or to participate in a raffle, but that person almost certainly missed the fine print that links to a second page of "Marketing Partners" and purportedly gave consent to receive robocalls from hundreds, or even thousands, of entirely unrelated entities. Worse, the ITG has seen some evidence that suggests these already flimsy claims of consents could actually be entirely falsified, where a bot used public data to consent on behalf of consumers for calls they never asked for and do not want.

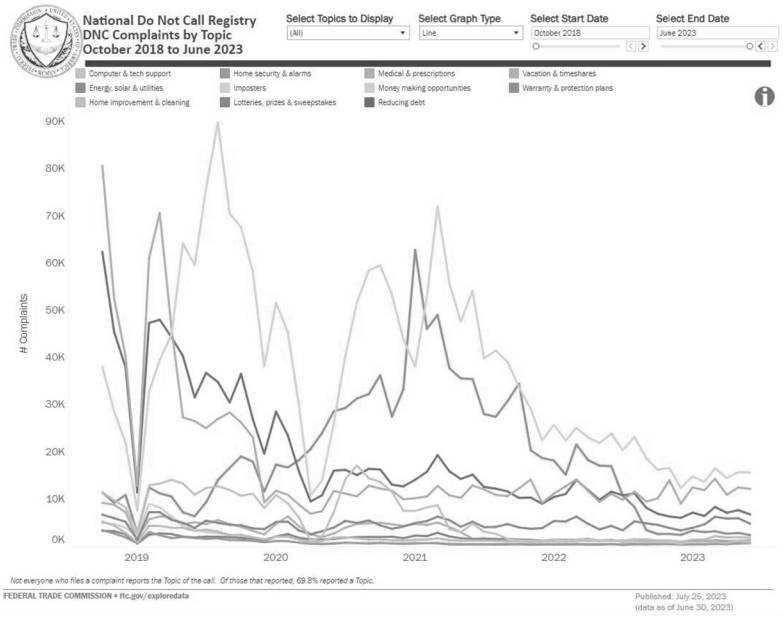
But even with these illegal robocalls, consumers are in fact seeing the positive impact of the ITG's efforts and Federal and state enforcement actions. The billions of unsolicited robocalls offering auto warranties which you and your constituents almost certainly received have dropped almost to zero after FCC and state attorney general enforcement based on ITG data. Unwanted student loan robocalls have also faced a similar fate, now operating at a fraction of peak levels.



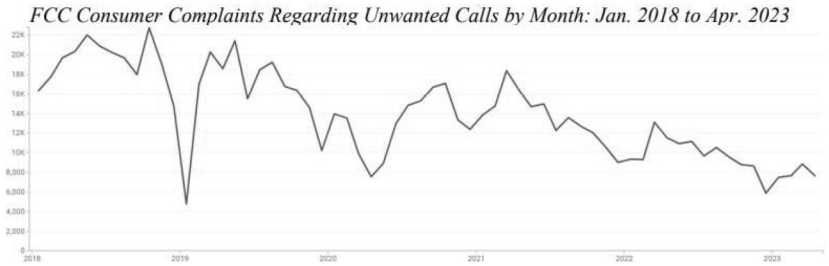
Americans are starting to notice these differences. There were over 560,000 Do Not Call complaints to the FTC in March 2019. Complaints declined after passage of the TRACED Act before peaking again in March 2021. Since then, however, there has been a steady and persistent decline—one that aligns with the industry's deployment of caller ID authentication as well as the ramping up of ITG-powered enforcement.



[1] Complaint for Civil Penalties, Permanent Injunction, Monetary Relief, and Other Relief ¶2, *United States v. Fluent, LLC,* No. 923-cv-81045, (S.D. Fla. July 17, 2023), ECF No. 1, *https://www.ftc.gov/system/files/ftc_gov/pdf/1923230fluentcomplaintandattachment.pdf*



FCC complaint data shows an equivalent trend.



To be clear, there are still too many complaints, and there continues to be far too many illegal robocalls and too much fraud initiated by phone. Consumers still are afraid to answer their phone when they do not know the number calling. In fact, that's precisely the advice often given by experts: Do not pick up if you do not know the caller.

There also are new trends of concern, including growth in dollars lost per victim of fraud, driven by targeted and increasingly sophisticated attacks. New technologies are also creating new challenges. In some of our tracebacks, we have seen automated robocalls that pretend to be a live caller, asking the call recipient about how they are doing and how their day is going. Regardless of how you respond—maybe with an assessment of your day and the weather, or with annoyance or confusion about receiving the call—the message continues and delivers the robocaller's offer.

For our part, the ITG is constantly adapting to bad actors' latest tactics to target and bombard consumers with illegal calls. We have expanded partnerships with entities in other sectors to help protect their customers victimized by fraudulent calls and we are constantly working to make the traceback process more efficient and more effective.

While the work of the ITG and that of Federal and state enforcement agencies to protect consumers from illegal robocalls continues, there are steps Congress can take to further empower these efforts:

- *Criminal Enforcement.* Congress should ensure that the U.S. Department of Justice (DOJ) has the resources, authorities, and prioritization it needs to prosecute the criminals behind unlawful robocalls, including fraudsters overseas as well as recidivist robocallers that stand up new entities under pseudonyms as soon as their prior ones are shut down. The criminal fraudsters overseas make their livelihood by defrauding Americans in some form, and will continue even if they cannot do so through robocalls. Likewise, recidivist robocallers are not deterred by financial penalties because these bad actors will never pay their fines. The threat of criminal enforcement for the fraud they have committed will make them think twice, however.
- *Support FTC and FCC Clarifications of Consent for Lead Generation Telemarketing.* The FTC recently released updated guidance under the Telemarketing Sales Rule regarding a consumer's consent to receive lead generation calls. The FCC has an open proceeding to clarify its view of consent for lead generation calls under the Telephone Consumer Protection Act. These efforts are important to ensure that bad actors cannot continue delivering millions of robocalls each day that no one asked for or wanted under flimsy-at-best claims of consent. Congress should support efforts to ensure that any telemarketing robocalls consumers receive are ones that they in fact consented to and are expecting to receive.
- *Number Trace.* To address problematic number rotation, Congress should formally expand the role of the traceback consortium to investigate how bad actors get access to the thousands and thousands of numbers they rotate through. Just as tracebacks have infused accountability about how unlawful calls get onto the phone network, number traces will infuse more accountability into how unlawful callers get numbers through the number wholesale market.
- *Re-Introduce and Pass the Robocall Trace Back Enhancement Act or Similar Protection.* The registered traceback consortium should have protection from frivolous and nuisance lawsuits intended to undermine the traceback process and detract resources of the consortium. Those resources are better dedicated to continuing to enhance the traceback process and its disruption of illegal robocalls and support of Federal and state enforcement.
- *Extend Consortium Designation Process to Every Three Years.* Under the TRACED Act, the registered traceback consortium must be designated by the FCC annually. The FCC's review and oversight are integral to confirming that the consortium operates in a neutral and non-discriminatory manner. Conducting the designation process on an annual basis, however, ties up the Commission's resources as well as those of the consortium. Those resources could be better dedicated to investments in continuing the fight against illegal robocalls.

Thank you again for the opportunity to speak, and we look forward to continuing to collaborate with this Subcommittee, the FCC, FTC, DOJ, and other Federal and state government partners on solving the illegal robocall problem.

Senator LUJÁN. Mr. Bercu, thank you very much for your testimony today as well. Mr. Rudolph, you are recognized for 5 minutes. The floor is yours.

STATEMENT OF MICHAEL RUDOLPH, CHIEF TECHNOLOGY OFFICER, YOUMAIL, INC.

Mr. RUDOLPH. Thank you for the opportunity to speak today regarding robocalls, robotexts, targeted attacks like vishing and smishing.

I am a CTO, so I am going to introduce a whole bunch of acronyms and new terms, I apologize. And the evolving landscape of threats, tools, and enforcement. My name is Mike Rudolph, and I am the CTO at YouMail. YouMail provides a service that protects individuals from harmful calls and texts, and we publish the robocall index summarizing nationwide and State robocall data.

We also provide blocking, analysis, audit, and investigative services to communication providers, enterprises, investment firms, and Government agencies. Prior to YouMail, I worked with many For-

tune 500 companies helping mitigate risk through automated controls and policies to comply with things like the Sarbanes-Oxley Act and implement processes performing background checks and pre-employment screening.

I see similar patterns and needs emerging and communications now as robocall mitigation controls and know your customer policies that balance the levers of risk and revenue at communication providers who can control those levers.

I am honored to work with talented—the talented YouMail team on the front lines of investigations, disruptions, and enforcement. Our team is small given the demands to monitor tens of thousands of monthly and weekly active messaging and voice campaigns targeting consumers. Some of our prioritized targeted success here in industry is well chronicled, working with states, particularly Attorney General's offices, Federal agencies, and private industry, such as one of Wylie's clients, resulting in 90 to 100 percent reduction when we target specific robocall campaigns.

I thank and commend those partners that made the identification and disruption of those campaigns a top priority for their fraud, cyber, or legal teams. Without their collaboration, it is significantly harder to escalate a robocall campaign from simply being unwanted and deceptive, all the way up to unlawful and eagle, so we can take—unlawful and un-legal, so we can take action. When the FCC identified specific robo-campaigns as poison pills for industry, I observed many providers that were previously uncertain about how to treat those calls suddenly decide with decisive action how to stop them.

We can credit 2022 as the year unwanted auto warranty calls were stopped. However, now we have home warranty, debt reduction, Government grant, loan and insurance calls taking their place.

Robo operators feverishly evolve their tactics in this cat and mouse game, and some embrace new techniques and tactics like generative AI, shifting from spoofing of numbers to using real numbers, and have adopted strategies to minimize the evidence they leave behind, which is necessary for companies like ours and the ITG and the FCC to ultimately stop these bad actors.

Who is to serve as our TSA screening guardian that stops bad actors from flying the skies of the public telephone network? These accounts at providers, checked only the first day they want to make a call, or are they checked routinely every time they want to traverse the network like airline travelers every time they fly?

By our estimates, we have endured over 250 billion, that is a quarter trillion, robocalls since 2019, about a thousand per American adult. We have taken a bite out of several of the most prolific robocall operations responsible for these few billion calls.

It is not just the sheer volume game, as every robocall campaign is different, and we are now in an era where there are fewer but more advanced calls causing more harm per call. There is no shortage of work to do if we are to continue to make progress. I look forward to your questions.

[The prepared statement of Mr. Rudolph follows:]

PREPARED STATEMENT OF MICHAEL RUDOLPH, CHIEF TECHNOLOGY OFFICER, YOUMAIL, INC.

Chairman Luján, Senator Thune, and Members of the Committee, I thank you for the opportunity to appear and testify today regarding the current state of the operations, investigations and enforcement actions relative to omni-channel robo-communications—both robocalls and robotexts as well as phishing tactics and platforms including vishing, smishing, and generative AI.

I provide my testimony today as Chief Technology Officer of YouMail, a privately held company whose mission is to protect the public from harmful communications and to restore trust in our communications networks.

I. Introduction

YouMail is often recognized for its role providing data in the behind-the-scenes battle against unwanted voice calls. The company's origins, as its name suggests, trace back to being one of the innovators and first providers of visual voice-mail and cloud-based voice-mail answering services in the United States.

As early as 2009, YouMail recognized that the demand for its solutions was linked to individuals who relied heavily on receiving dozens to hundreds of daily live, inbound calls to their personal mobile phone number. These individuals spanned a wide range of high-touch professions that are considered very small businesses (VSBs) in America: fitness trainers, tutors, repairman, electricians, plumbers, exterminators, realtors, interior designers, handymen, contractors (floor, paint, tile, carpentry, construction), appraisers, notaries, mobile mechanics and detailers, dog sitters/walkers, photographers, event planners, florists, babysitters, caterers, bakers, accountants, financial planners, landscapers, movers, stylists, barbers, beauticians.

It's important to acknowledge that professionals such as these find their success and income depends on how they respond to incoming calls from unknown numbers. Before unwanted and illegal calls from unknown numbers invaded our phone network, these calls from outside of contact lists typically meant a potential new customer for this VSB. For sole proprietors, unknown calls signaled an opportunity to connect with a prospective local customer to generate income to provide for themselves and their families. Failure to answer the live incoming call often meant the potential lead for their small business would move on to call the next highest rated provider, discovered on search engines or websites such as Yelp, that may have a lower rating, but were available at just that moment to answer the live call and interact with the caller. At one time, and still perhaps today, answering live calls from unknown numbers was a critical path to success for small businesses.

As any good business asking its customers what they needed next, YouMail recognized the need to silence the ringer for these subscribers when the call was almost certainly spam, but also to ensure real local customers calls would ring through to be answered live to then ideally become appointments and customers for very small businesses. As a visual voice-mail and answering service, and not just a device ring blocker, YouMail provided a fallback as voice-mail audio is converted into readable text and a small business, like any user, could quickly determine the purpose of the call.

In 2009, YouMail began investing in technology and techniques to identify calls as spam or unwanted, both in order to prevent ringing and also to move unwanted messages into a Spam folder, as most users are accustomed to experience with e-mail.

Eventually, as unwanted robocalls became an evidence signal in everyone's voice-mail box, YouMail launched the Robocall Index in 2015, which over time has become recognized as the standard for industry metrics on robocalls occurring nationwide, as well as per-state and per-metro region.

YouMail's role as an over-the-top app, trusted to provide answering services to millions of telephone numbers across all major U.S. and Canadian carriers, provided it with unique capabilities to respect consumer privacy while tracking and grouping unlawful communications throughout the mobile phone networks. It is worth noting that YouMail data is nearly entirely based on what reaches consumer handsets, and does not extend to communications blocked at the network of the underlying carrier, which certainly would indicate even more by way of voice and SMS communications attempting to reach consumers.

In late 2019, YouMail launched its YouMail Protective Services division, which assists law enforcement, financial services, enterprises, and communications providers with its data, evidence, intelligence, and investigative services.

As YouMail's role in industry has expanded, innovative bad actors behind unlawful and unwanted communications have become aware of YouMail's industry role. YouMail is already observing efforts by both telemarketing and threat actors to

evade YouMail's methods of detection by minimizing calls and voice evidence to YouMail users or by trying to directly obtain access to YouMail data for similar evasive purposes.

II. Caller and Call Recipient Relationships

As many state and Federal agencies have reported over the years, unwanted communications, particularly robocalls and robotexts, rank among the top complaints received by their offices.

One of the difficulties in analyzing communications is determining whether a communication is spam, generally unwanted by most recipients, or is perpetrating a scam or committing fraud. This is particularly challenging as the content of a communication may be nearly identical when it comes from an enterprise such as a bank, utility, or government agency as it is when it originates from an imposter.

It is helpful to consider different classes of originating callers from the perspective of an average person, as this classification helps to understand a common, generally desirable experience based on the relationship between that average call recipient and the calling party.

In the examination of types of caller relationships, we may consider why an individual may be at a moment in their life that would affect their susceptibility to answering a live, incoming communication from an unknown, non-contact telephone number.

- *Personal*—these are communications between two individuals who know each other and may or may not yet be saved contacts on the device. These are friends, family, colleagues, co-workers, classmates, acquaintances who usually have a direct, personal relationship, or may be introduced through a mutual acquaintance. If you or your child have joined a new school or club, you may be expecting a call or text message from a teacher or coach from an unknown number. While it's nearly universal, personal calls are not always wanted such as cases of harassment or stalking, but any desired blocking in this case is between two individuals for personal reasons.
- *Local Business*—these are not often personal relationships, but between an individual or household and small local businesses or services. This would include your dry cleaner communicating your garments are ready, or a local restaurant confirming a reservation, or your handyman, gardener, babysitter, dogwalker, trainer, or healthcare professional discussing an appointment, problem or matter. These are sometimes saved contacts, but often when someone has an urgent need, they may be expecting calls from several potential unknown numbers that provide a local service in order to address that time-based matter or need. While this is also nearly universal, sometimes disputes between a customer and service provider may lead to an individual wishing to block these communications. Or, if a local business has crossed a line from communicating about appointments/inquiries/problems into using the communication channel for marketing or lead generation, these calls may drift into unwanted and blocked territory. Once again though, these types of calls are almost universally wanted apart from the situation where two parties have a personal conflict.
- *Non-Local Business*—these are communications between a national, regional or online business and an individual and are also where most universally unwanted communications occur, although not all communications between individuals and households and non-local businesses are unwanted. These interactions typically fall into a few sub-categories:
  - Essential: these would be appointment reminders and confirmations, one-time or password reset events, critical account/emergency alerts where the individual's interaction is necessary (password reset or transaction confirmation) or the individual would be impacted based on their assumption of a time/place/occurrence.
  - Marketing, Originated by Individual/Household, Follow-up: these communications rely on a triggering event typically where the individual expressed an interest in the business, ideally directly through a communication initiated by the individual/household that occurred online, in-person or by phone.
  - Marketing, Originated by Non-Local Business, Goal-Driven: these communications usually begin with a sales, marketing or operations team at the business that is interested in demand generation to stimulate sales or engagement in products or services, regardless of any recent interaction by the individual/household.
- *Scam/Fraud*—these are communications which can be disguised to look like **any of the above** as they reach an individual or household and rely on TTPs

(tactics, techniques, and procedures) that emulate a real individual, local, or non-local business, as described previously, as closely as possible in order to maximize their success.

III. Call Recipients Want To Know Who Called

Society has been shifting away rapidly from voice calls, as the voice communications network has become filled with unwanted and unlawful voice calls.

When someone receives a call from an unknown number, they want to know *who called* and *the reason* the call was made.

Individuals and households are particularly susceptible to answering calls from unknown numbers based on time and situation-based events in their lives. The originators of unwanted and unlawful calls make repeated call attempts, hoping to get their timing right for these live answer opportunities.

Call recipients generally fall into one of two camps during these moments of answering susceptibility—those who will answer all unknown numbers during these windows of vulnerability, and those who allow the calls go to voice-mail, hoping to identify the anticipated call and to call it back if it matched an expected call. In the case of returning a call based on a voice-mail, this can mean having to wait on hold and navigate an interactive voice response (IVR), and a loss of time simply due to a best practice of screening incoming calls from unknown numbers.

When a legitimate caller has a significant enough situation to merit a voice call as the chosen medium of communication and places a call, they have no good reason to not leave a message.

Consider all the potential relationships and legitimate reasons for a call between a lawful caller and call recipient. If the caller suspects the call recipient doesn't know who it is based on the high likelihood it is not a personal contact saved to the device, the caller would want to identify themselves and their reason for calling to encourage engagement from the called party, since there was an important reason for initiating a voice call.

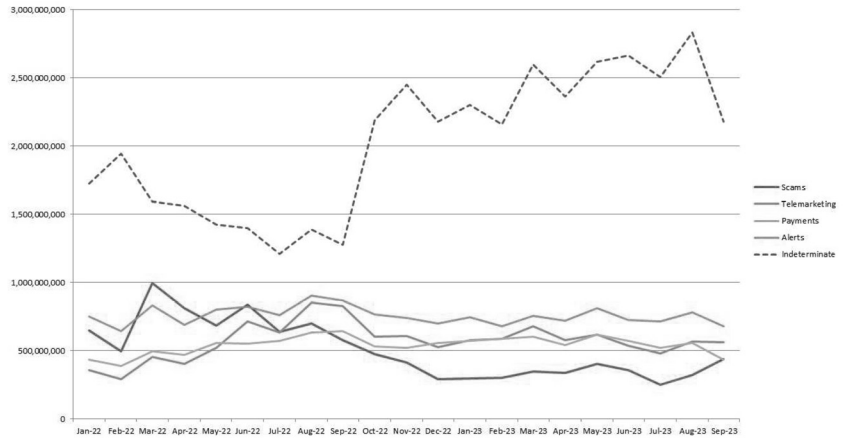
As we expand into the "Marketing, Originated By Non-Local Business, Goal-Driven" relationship and use case above, the company that is using the voice channel to engage in telemarketing, if they possess the conviction that their marketing offer is worth initiating the voice call, should maintain that conviction that the call is important enough to identify themselves and the purpose of their call initiation in a voice-mail message.

By not leaving a message, the call initiator could suggest their additional attempts, making many more calls to the recipient, are because they are still trying to deliver the message. The subsequent attempts may not be necessary if the message was left on the first attempt and the individual was able to make a decision based on this evidence to respond to the communication by any indicated, allowable channels.

YouMail attempts to classify calls received by consumers into several categories and has been tracking this data for several years. YouMail relies on lawful, legitimate call originators, or bad actors imitating those call originators, obeying this societal protocol that if it was important enough to initiate a voice call, it was important enough to indicate who you are and why you called.

YouMail, via the Robocall Index[1], observed a significant increase in indeterminate, non-categorizable robocalls beginning in September 2022.

[1] *https://www.robocallindex.com*



Because the telephone numbers linked to indeterminate robocall behavior do not possess a history of delivering desirable/wanted communications, YouMail infers that they are linked to unwanted and undesired behavior, as they do not provide audio evidence of their identity or reasons for calling recipients.

This increase in indeterminate calls also correlates to a decline in observable calls linked to scams and telemarketing, so it is reasonable to assume some of the parties behind those calls have shifted their tactics to call and hang up in order to evade consumer recognition, as well as detection by services such as YouMail that utilize audio evidence in voice-mail to prevent and support enforcement against unwanted and unlawful communications.

Present enforcement and traceback efforts often rely on the audio content of the call in order to wield it as evidence of unlawful activity in an investigative process. If a robocall operation is sophisticated enough to use evasive strategies such as utilizing attested calls made in very low volumes across an inventory of real numbers, and across a span of enabling providers, while leaving no audio evidence (permitting access to CPNI under the Communications Act Section 222-d-2), it becomes much more difficult to track, investigate, and prevent.

Establishing a requirement for business communications to leave a voice-mail when they introduce a new originating number to communicate with a specific call recipient not only serves the interest of consumers who want identity and purpose to accompany unanswered, unknown calls, it also serves the legitimate business to solicit reciprocal engagement from the recipient, assuming this communication achieved the litmus test of having been worth initiating a call in the first place.

Further, voice service providers can track this behavior in new and existing accounts, ensuring that their logs of calls from accounts that have identified as a business that need to make hundreds, thousands or millions of calls are making calls of a duration long enough to permit them to convey their identity and reason for calling. Accounts refusing to follow this policy would have no reasonable explanation, as their communications are either not valuable enough to pay for the extra 5–30 seconds per call (and thus were not valuable enough in the first place to disturb and disrupt the recipient's day), or they did not want recorded evidence by way of voice-mail of their operations and were likely unlawful or illegal.

IV. Omni-Channel Marketing & Communications

Marketing technology, communications technology, and their subsequent integration into consolidated platforms have made significant advances in the past decade. A litany of acronyms from the tenured CRM (Customer Relationship Management) and CPaaS (Communications Platform as a Service) to more recent upstarts such as CDP (Customer Data Platform) and CEP (Customer Engagement Platform) highlight the rapid innovation and convergence of automated omni-channel marketing applied to integrated recipient data.

Omni-channel marketing engages a single recipient through many media, sometimes simultaneously, sometimes as a scripted sequence of conditional events. A good omni-channel marketing platform allows the marketer to upload a list of recipients and to buy ad placements on search engines or websites, send e-mails, generate calls and send TXTs, engage in messaging conversations and host a telephone num-

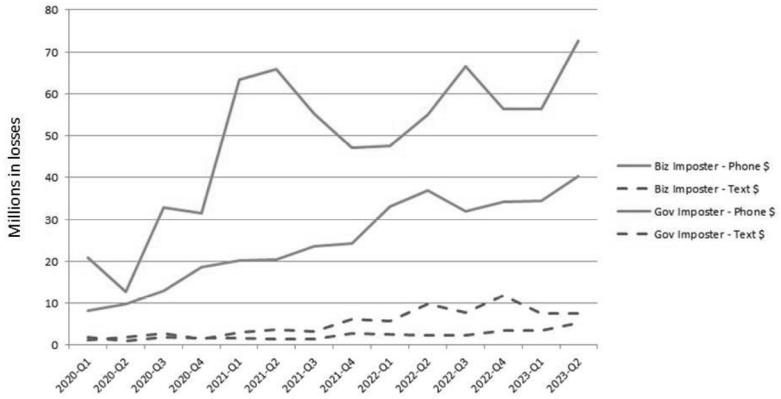
ber with a menu for incoming calls. Domain registration and website building has become trivial enough that some tools can be given a domain and create a similar looking website with a few clicks for under $20.

A competent individual can invent a company and deploy a sophisticated omnichannel marketing operation in hours and at low cost, choosing from hundreds of vendors, ranging from fledgling start-ups to publicly traded firms. Some platforms, seeking to accelerate their own growth through streamlined onboarding, allow communicating with a customer list on trial plans with no financial transaction (or vetting) necessary. The barriers to "looking big" and "communicating wide" have never been lower, which is tremendous for encouraging new entrepreneurial ventures in competitive markets, but also enables a tremendous opportunity for bad actors mimicking these real businesses to gain access to these advanced tools.

Though YouMail and its Robocall Index have observed that robocall volumes have declined slightly from 58 billion in 2021 to an estimated 53 billion by end of 2023, the FTC and FBI both indicate rising reported losses in the complaints gathered from consumers. These are only the losses reported to these specific agencies, and significantly understate the true consumer harm, as only a subset of losses is ever reported.

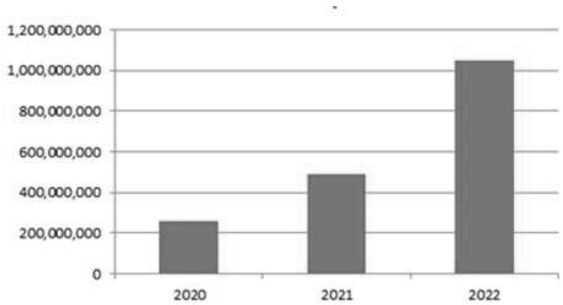
The FTC Consumer Sentinel Network Tableau site[2] shows a 400 percent increase in Business Imposter dollar losses reported since Q2 2022.

FTC – Reported Losses (in Millions) to Business, Government Imposter By Medium



The FBI IC3 Data[3] shows a rise in reported financial harm from Government Impersonation and Tech and Customer Support losses. These are the categories of losses in which voice or SMS were used to impersonate a known organization.

FBI IC3 – Losses to Government Impersonation + Tech and Customer Support Imposter



[2] *https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts*

[3] *https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf*

Legitimate enterprises have shifted to omni-channel marketing as it is more effective in soliciting customer engagement and inducing more transactions. Advanced threat actors who wish to successfully impersonate an organization study the organization's current practices and, recognizing the user of omni-channel communication (ads, online, web, e-mail, voice, SMS, app), it should be no surprise that the threat actors embrace similar tactics and platforms to increase their success rates with victims.

Even more advanced threat actors take advantage of APIs provided by these platforms and entrench themselves across multiple accounts and multiple platforms to reduce the impact of a single disruption or take-down. As astute recipients/targets report the attempt by the threat actor, only one of hundreds or thousands of accounts are deactivated, and criminal operation continues with minimal operational impact.

V. Generative AI & Pig Butchering

Since 2022, many omni-channel marketing and communications platforms have been rapidly introducing and announcing the benefits of integrating capabilities of LLMs (large language models) and generative AI.

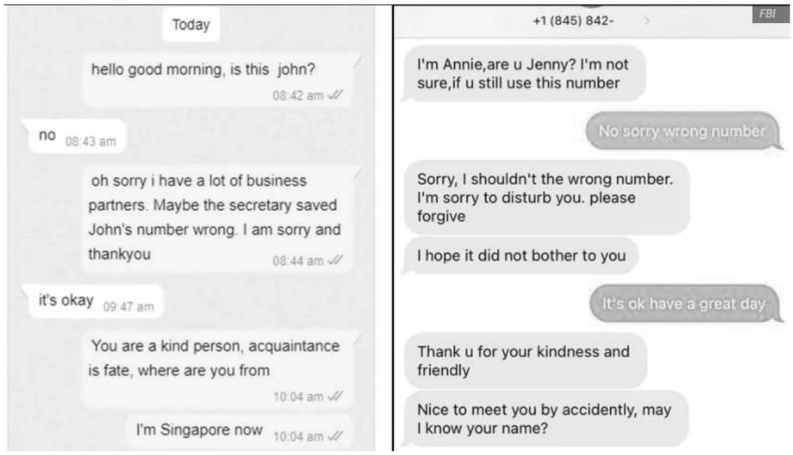
The benefits to a legitimate marketing operation should be obvious—you can simultaneously communicate with more people on a personal level through almost every available medium of communication. One marketer in a small operation can leverage generative AI to speak personally and fluently in nearly any supported language with tens of millions of recipients daily.

Prior to widespread use of generative AI, YouMail would observe 'broken English' in robocall or robotext campaigns that identified as a bank. Poor command of the English language serves as an obvious tell, indicating a campaign is operated by a fraudulent imposter.

One such example YouMail has shared is in generating the script "press 1 to connect to a fraud specialist" to emulate a financial services firm, a Chinese-speaking threat actor with limited skills at English may use a simplistic tool to translate the Chinese word "[handwritten characters]" (shēngchéng) to either "generate" or "connect". YouMail's investigators would observe the audio "press 1 to *generate* to a fraud specialist" as an indication of fraud as it is highly unlikely a US-based financial services firm would make such a mistake. With threat actors leveraging well-trained, fluent generative AI platforms, such mistakes rarely occur, which then requires additional investigative resources and collaboration to separate legitimate and imposter communications from one another.

As YouMail has expanded its investigative and protective solutions to cover SMS, MMS, RCS and other messaging technologies, it has observed conversations that are clearly evidence of "pig butchering" attacks.

"Pig butchering" often begins by using a messaging platform such as SMS to initiate a conversation that is otherwise indistinguishable from personal conversation by saying something like "Hi" or "Hey Ben, it was good talking last week". If engaged, the conversation apologizes awkwardly for the accidental message but maintains a friendly, charismatic tone and works to establish a casual friendship as a goal. Often, the threat actor is awkward and apologetic, citing English as a second language to cover for any misunderstandings.



Sample pig-butchering conversation provided by FBI and used by NBC Miami
https://www.nbcmiami.com/news/local/new-pig-butchering-crypto-scam-stealing-millions-from-south-floridians-fbi/3009914/

Over time, the threat actor builds a rapport and encourages its target to take certain actions which range from things that may feel trivial like checking out an app or visiting an interesting website. Ultimately, they are more successful the more they appear authentic and patient and don't force their target to immediately connect Apple Pay to their bank account or begin "investing" in cryptocurrency.

A single threat actor using generative AI connected to the communications network can run hundreds to thousands of simultaneous conversations, refining its model while learning from mistakes and exercising patience in rapport-building indistinguishable from a real person. The technology already exists to generate synthetic yet authentic appearing images, video and audio, if those prove necessary hurdles in carrying out further artificial trust-building to support the criminal endeavor.

Messaging continues to trend towards technologies with E2E (end-to-end) encryption (iMessage, RCS, WhatsApp, Telegram) and advanced pig butchering initiated by SMS often tries to move the conversation to an E2E encrypted medium in order to evade detection via unencrypted channels as it reaches deeper, detectible evidence of malfeasance in later steps of its script.

A recent blog[4] from digital risk protection vendor Phishlabs includes several screenshots of how quick and easy an aspiring threat actor can make a few clicks using a PhaaS (Phishing-as-a-Service) platform to deploy automated omni-channel phishing services with out-of-the-box capabilities to impersonate 11 U.S. financial services institutions. The site regularly holds sales.Recent rates to send SMS messages ranged from $130 to send 5,000 SMS messages or $620 to send 25,000 SMS messages.

[4] *https://www.phishlabs.com/blog/threat-actor-profile-strox-phishing-as-a-service/*

Real-time dashboard from PhaaS provider as live potential victims interact

Anniversary sale prices advertised by PhaaS provider with SMS messaging allowances

VI. Tools, Resources, Success

While the FTC and FBI data indicates an increase in reporting of individual financial harm from communications, despite stability in total robo-communication volumes, the media, trade shows and industry investments reveal a sprint to connect advanced tools such as generative AI and omni-channel marketing platforms to the communication network. Nonetheless, progress has been made in industry to use new tools and techniques to curb high-volume robocall operations that once upon a time plagued consumers.

STIR/SHAKEN

STIR/SHAKEN is one of most cited tools to assist in the combatting of unwanted, unlawful robocalls, with many deadlines for implementation passing in 2022 and 2023.

YouMail tracks the certificates on the voice calls that terminate at its network, and where the voice call matches a known unwanted, unlawful, or illegal campaign, it links the originating or gateway provider that indicated it owns responsibility for attesting to that call.

As of September 2023, YouMail was observing nearly 800 distinct certificates per week in the calls that it answers. YouMail has yet to publicly publish statistics on its observed certificates, but YouMail's observations match the approximately 800 signers in data published [5] by TransNexus. TransNexus also notes the approximate number of 1,200 SHAKEN-authorized providers as of September 2023.

As of October 18, 2023, YouMail observes that there are 17,900 entries in the FCC 499 Filer database [6]. 4,789 entries identify their principal communication type as 'Interconnected VOIP'. As of October 18, 2023, the FCC Robocall Mitigation Database [7](RMD) contained 8,562 entries. 2,891 of the RMD entries state "Complete S/S Implementation" and 1,980 entries state "Partial S/S Implementation, Performing Robocall Mitigation" for a total of 4,871, indicating some STIR/SHAKEN implementation.

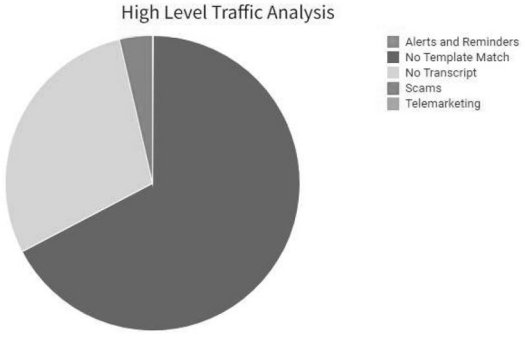
It would appear that there are somewhere between 8,000 and 20,000 entities that acknowledge themselves as relevant voice communication providers, so these 800 certificates presently active in September 2023 are potentially only indicating origination information for 4–10 percent of communication providers.

STIR/SHAKEN & Sample YouMail Investigations

YouMail, as an answering service for customers of mobile network operators (Verizon, T-Mobile, AT&T, et al.), relies on customers setting up their call forwarding feature to divert unanswered calls to YouMail's service. Consequently, YouMail, and services like YouMail's, rely upon voice providers implementing the IETF RFC 8946 Personal Assertion Token (PASSporT) Extension for Diverted Calls in order to carry the originator certificate through to YouMail as the final termination point for a call. When unimplemented at a network, YouMail typically observes a mobile network operator introducing its own certificate (at the lowest level of attestation, a C-attestation) in place of the originating provider's A-attestation, when diverting calls. This negatively affects transparency regarding the origination of unlawful call campaigns carried in the ecosystem on diverted calls going to voicemail services like YouMail.

When the originating provider's certificate carries successfully to the call termination point, companies such as YouMail can perform aggregate analysis on the calls received from an originating provider by matching content (such as voice-mail) to the originating service providers.

Below is a sample pie chart indicating the content carried by an originating provider's traffic for a month:



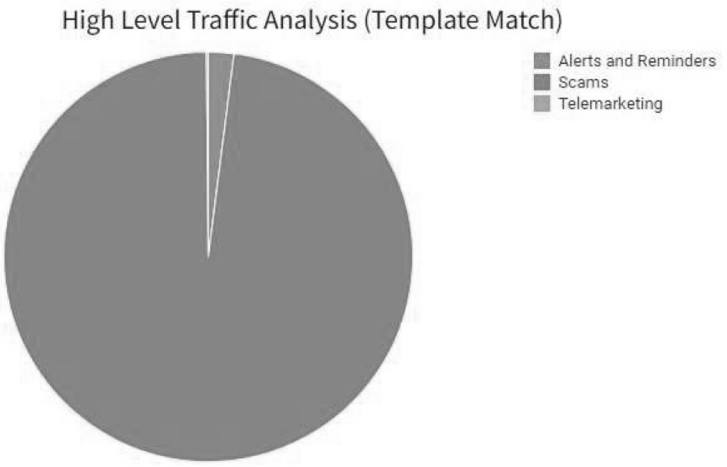
This pie chart reveals:

- a light grey area where callers left no message
- a dark grey area where a message was left but did not match the template of a known robocall

[5] *https://transnexus.com/blog/2023/shaken-statistics-september/*
[6] *https://apps.fcc.gov/cgb/form499/499View.htm*
[7] *https://fccprod.servicenowservices.com/rmd?id=rmd_welcome*

- a red area, representing calls for which the audio matched audio of a call suspected to be a scam

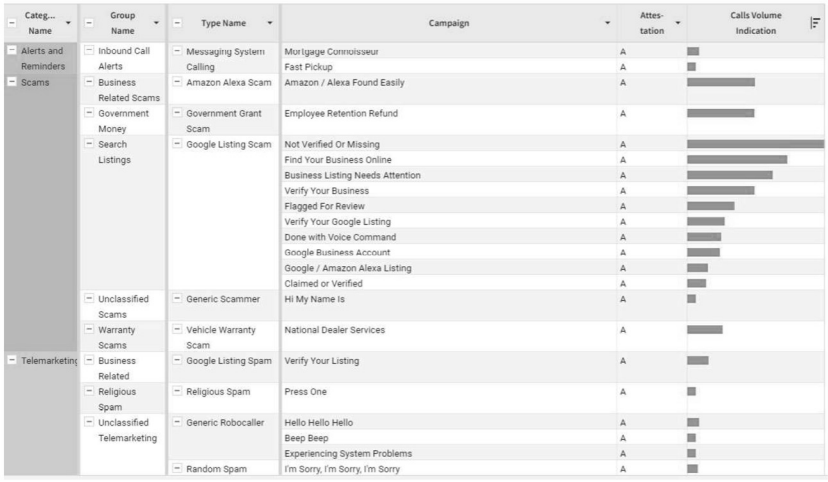
It is often helpful to exclude the light and dark grey areas (to remove calls not providing audio evidence and calls where the audio evidence wasn't able to be matched to known good or bad robocalls) in order to produce a drill-down pie chart of all recognized robocalls at that provider.



This pie chart reveals that, of the tracked robocalls at this provider, the majority appear linked to scam campaigns, with only a small green wedge linked to potentially legal/lawful alerts and reminders.

Underlying this pie chart, YouMail can examine the exact campaigns and their relative volumes as they compose this provider's traffic profile. At the time of this testimony, the current campaigns identified here are linked to their best, most likely classification, so this is not intended to be definitive attribution of a campaign to illegal behavior but rather the current suspected nature of these campaigns.

In the case of this sample provider, it reveals A-level attestations were given to audio and calls determined to be carrying illegal, unlawful content. It would indicate accounts that should be terminated if the activity is confirmed within the provider's records and a legal imperative to perform an investigation to find and terminate accounts carrying similar traffic. In the case below, the top campaigns found were "Google Business Listing Scams", "Amazon Alexa Scams", and "Government Grant Scams". What is also of note is that this provider has very little traffic that indicates lawful, desirable robocalls to be received by consumers (such as a prescription reminder, or change-of-venue alert, etc.).



Categ... Name	Group Name	Type Name	Campaign	Attes-tation	Calls Volume Indication
Alerts and Reminders	Inbound Call Alerts	Messaging System Calling	Mortgage Connoisseur	A	
			Fast Pickup	A	
Scams	Business Related Scams	Amazon Alexa Scam	Amazon / Alexa Found Easily	A	
	Government Money	Government Grant Scam	Employee Retention Refund	A	
	Search Listings	Google Listing Scam	Not Verified Or Missing	A	
			Find Your Business Online	A	
			Business Listing Needs Attention	A	
			Verify Your Business	A	
			Flagged For Review	A	
			Verify Your Google Listing	A	
			Done with Voice Command	A	
			Google Business Account	A	
			Google / Amazon Alexa Listing	A	
			Claimed or Verified	A	
	Unclassified Scams	Generic Scammer	Hi My Name Is	A	
	Warranty Scams	Vehicle Warranty Scam	National Dealer Services	A	
Telemarketing	Business Related	Google Listing Spam	Verify Your Listing	A	
	Religious Spam	Religious Spam	Press One	A	
	Unclassified Telemarketing	Generic Robocaller	Hello Hello Hello	A	
			Beep Beep	A	
			Experiencing System Problems	A	
		Random Spam	I'm Sorry, I'm Sorry, I'm Sorry	A	

YouMail's position is that STIR/SHAKEN is an extremely valuable tool that is still in the process of industry adoption, despite recent FCC deadlines. It is a tool presently lacking sufficient resourcing to carry out investigative, compliance, and enforcement efforts and success in curbing robocalls ultimately depends on the resources applied to ensure data is not only properly collected but integrated into the ecosystem to maximize transparency.

It is a non-trivial undertaking to prioritize and investigate thousands of active robocall campaigns each month, understand their legality and effect corrective action where necessary.

KYC (Know-Your-Customer), KYT (Know-Your-Traffic), Know-Your-Upstream (KYUP)

During our investigation-related discussions with voice service providers, they regularly indicate that they were unaware that the indicated account was carrying the communications provided in the supporting evidence attached to the reported incident. Conversations such as these indicate that many providers, intentionally or unintentionally, do not truly know their customers.

Over the past few years, a few parties have weighed in on best practices and requirements for communication providers to "know your customer" or "know your traffic". The FCC recently also included "know your upstream provider"[8] to this growing lexicon on April 27, 2023.

When illegal communications are injected into public communications, it should not matter whether the account holder is considered a "customer", "peer" or a "provider" and it should not matter what the enabling platform considers itself (gateway, intermediate, facilities-based, etc). All platforms enabling communications share responsibility in preventing accounts originating illegal, unlawful communications.

An FCC filing [9] by private company Numeracle, on April 27, 2023, included Numeracle's Model Standards v1.1 for KYC, which includes a list of questions to ask new customers. Numeracle's list is comprehensive, including asking the prospective customer to share marketing materials, reveal prior actions or judgements, provide descriptions of the calls along with consent collection and legal compliance practices. Another example of good KYC policies and controls can be found in settlements between recidivist providers enabling robocalls, such as the March 6, 2023 settlement between State of Texas et al and Rising Eagle Capital Group LLC [10] .

An account faced with strenuous onboarding Q&A that is planning to initiate illegal or grey-area telemarketing communications is unlikely to proceed with establishing the account at a provider using processes such as these, as it indicates the bad actor is likely to be either rejected before they can start sending communica-

[8] *https://docs.fcc.gov/public/attachments/DOC-392975A1.pdf*
[9] *https://www.fcc.gov/ecfs/search/search-filings/filing/1042778647719*
[10] *https://www.texasattorneygeneral.gov/sites/default/files/images/press/Spiller%20Stipulated%20Order.pdf*

tions, or if they misrepresent themselves, their ability to communicate would be short-lived before they face a permanent termination.

YouMail is often asked to comment on KYC Practices and observes many communication providers want to keep their current practices private, because they are viewed as both:

- a legal liability, if revealed (and ultimately proven intentionally or unintentionally insufficient)
- a competitive advantage

Interestingly, interpreting the KYC process as a competitive advantage perception cuts two ways. Some providers view their "light touch" policies, procedures, and controls as an advantage because they maximize their revenue in turning away only the most egregious new accounts, while permitting less egregious yet still unlawful revenue-bearing accounts to onboard. On the other side, providers with stricter controls and policies comment they are playing the "long game" and, while they lose out on this potential revenue in the short term, they envision they will eventually see account migrations from peers and competitors, as those peers and competitors are publicly identified as a risky supplier for legitimate high-revenue enterprises.

KYC, Analytics, Call Labeling & Blocking

Numeracle filed further comments [11] with the FCC on August 9, 2023, through which they addressed the current state of analytics, labeling, and blocking. Some of Numeracle's [12]commentary was furthered by an FCC filing made that same day by United Office [13], who included screenshots demonstrating how their customers' calls were displayed on Android and iOS devices across major carriers.

Both Numeracle and United Office cite working with customers who had their calls labeled as 'Spam Likely' or 'Scam Likely'. Seeking to remediate the labeling on behalf of their customers, they worked closely with them to get to know them and determine whether these calls were mislabeled, often to provide evidence to call analytics companies and voice providers in order to correct the mislabeling.

YouMail has observed that telephone numbers of legitimate calling parties (banks, government, security alerts, emergency, and disaster alerts) drift from accurate labeling to 'Spam Likely' or 'Scam Likely' treatment over time at individual mobile operators,without any evidence to show that the numbers have been compromised or spoofed by a threat actor. As the mislabeling occurs, YouMail also observes that its customers with the YouMail app installed on their device no longer answer these calls, indicating that mislabeling an incoming call effectively results in the same outcome as blocking the call as it drifts into an answer rate below 5 percent when prior answer rates exceeded 50 percent.

Typically, engagement with services or solutions that would remediate and clear up this mislabeling corrects the issue. As expected, this generates revenue for vendors that provide these solutions and results in increasing the costs of this business communicating with its customers, which could eventually mean this business passes those higher costs to communicate along to its customers.

YouMail has also observed in its investigations that many robocalls received by consumers receive a "green checkmark" treatment as they appear on devices. TransNexus indicated in their September 2023 blog.[14] that among prolific robocall signers, 88.46 percent of calls they signed with B-level attestation were robocalls and 79.4 percent of calls they signed with A-level attestation were robocalls. Robocalls with C-level attestation trend downward (from <40 percent in April 2023 to <20 percent as of September 2023).

Robocall operators are the most engaged, active calling parties seeking to stamp their calls with legitimacy in their quest to maximize engagement and answer rates. As a result, they have become the most prolific early adopters of new services that promise them A attestations for their calls. This presents distinct challenges to measure the benefit of labeling and display indicators like checkmarks to the public when legal, legitimate call originators are slower to adopt than the operators of suspect, grey-area or unlawful calls.

It is unclear how "pay to display" dynamics in the robocall labeling industry will ultimately play out. YouMail observes that calls with a green STIR/SHAKEN checkmark and display name generally have lower answer rates than calls without a green checkmark, which runs counter to the results promised by vendors charging call originators for these solutions. On the other hand, at the present time, this

---

[11] *https://www.fcc.gov/ecfs/search/search-filings/filing/108102252803712*
[12] *https://www.fcc.gov/ecfs/search/search-filings/filing/108092119116596*
[13] *https://www.fcc.gov/ecfs/search/search-filings/filing/108092119116596*
[14] *https://transnexus.com/blog/2023/shaken-statistics-september/*

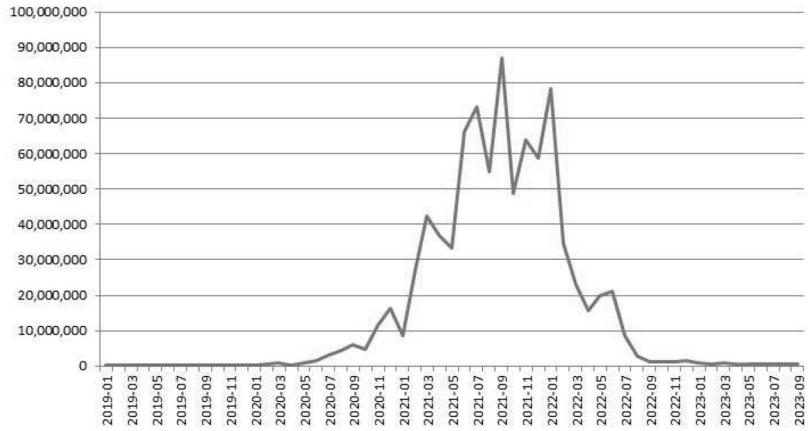
merely indicates the financial commitment of the marketing professionals operating highest volume telemarketing robocalls to spend to achieve their revenue goals and quotas, and their willingness to absorb an extra cost for the calls they place.

TCPA Class Actions

TCPA class action litigation can have a powerful effect on reducing unwanted robocalls. YouMail selected two recent class action settlements and the effect on calls received by Americans per month.

In 2022, DirecTV settled [15] a $17M TCPA class action lawsuit. DirecTV's robocalls per month reached a peak of an estimated 87 million calls received in the U.S. in September 2021. This data does not necessarily reflect which calls were subject to the TCPA actions in the assorted TCPA lawsuits filed against DirecTV, but provide YouMail's estimate of DirecTV robocalls per month over time where the surge in calls accounted for approximately 858 million total calls.

YouMail Estimated DIRECTV Calls Per Month (V1.0)

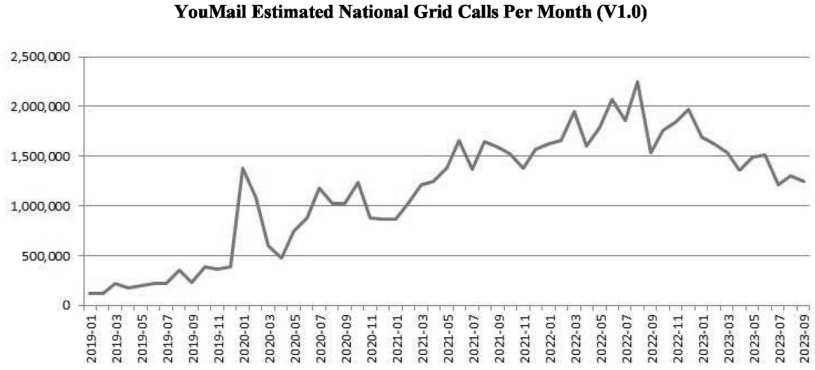


As can be seen, the class action litigation has reduced DirecTV robocalls by over 99 percent, which from its total volume has had a material impact in the total robocalls received by the public.

Also in 2022, National Grid settled [16] a $38.5M TCPA class action lawsuit. National Grid robocalls reached a peak of 2 million monthly calls by mid-2022, increasing 1500 percent from their pre-surge monthly volumes of ~150,000 per month.

[15] *https://topclassactions.com/lawsuit-settlements/closed-settlements/directv-unsolicited-calls-17m-class-action-settlement/*

[16] *https://topclassactions.com/lawsuit-settlements/closed-settlements/national-grid-pre-recorded-phone-calls-38–5m-class-action-settlement/*



YouMail only analyzed and modeled calls identifying as National Grid or referencing ngrid.com and did not include calls identifying as other entities from the class action suit (KeySpan Gas Corp, Brooklyn Union Gas Co, Niagra Mohawk Power Corp, Boston Gas Co, Colonial Gas Co, Massachusetts Electric Co, Nantucket Electric Co, Narragansett Electric Co). It is entirely possible that the robocall operation distributed call volume into different campaigns that no longer identified directly as National Grid at a point in time.

Based on YouMail estimates and models, the TCPA class action litigation appears to have caused a 45 percent reduction in monthly robocalls directly identifying at National Grid.

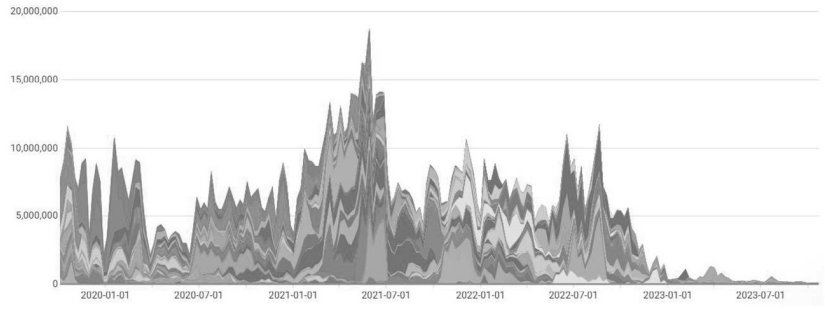
State & Federal Enforcement Actions & Coordination

YouMail works closely with partners in state and Federal enforcement agencies to model, track, investigate, provide, and analyze evidence of unlawful robocall campaigns. These efforts are largely concentrated on a campaign topic—robocalls that consumers recognize as carrying specific messaging to induce certain actions from them such as to purchase a vehicle warranty contract or to obtain loan assistance services. As consumer complaint data collected at a state or Federal level indicate specific areas of problematic robocalls, YouMail's ability to isolate the robocall campaigns from other communications enables real-time tracking, investigation, and enforcement action.

Student Loan Campaigns

In 2022, concerted efforts by state and Federal enforcement, in partnership with YouMail have effected a dramatic reduction in robocalls carrying student loan related campaigns. YouMail has modeled and tracked 234 distinct robocall campaigns related to student loans over the past 3 years and recent work to curb these robocall campaigns has resulted in a massive decrease in these calls received by consumers. YouMail attributes the December 8, 2022, FCC order [17] to all US-based carriers as the definitive signal to industry to no longer allow such robocalls in the network. After being made aware of this order, YouMail noted that many providers who had previously tolerated such calls began to adopt non-tolerance stances.

[17] *https://www.fcc.gov/document/fcc-orders-voice-service-providers-block-student-loan-robocalls*



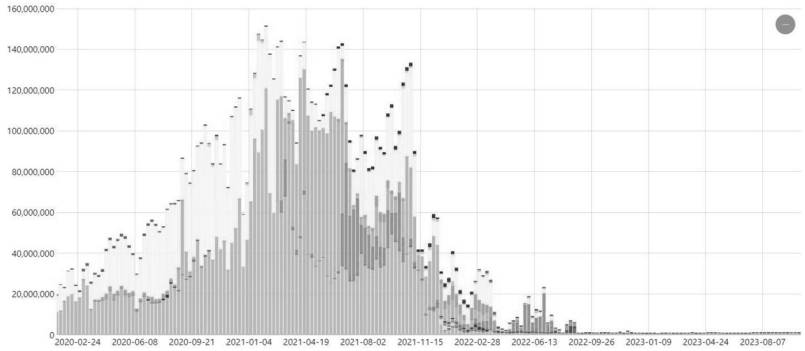
Weekly Estimated Student Loan Robocalls

YouMail does believe that many of these robocall operations have shifted from advertising as 'student loan' support to advertising their services as 'debt reduction', 'government grant' or other similar financial assistance offers in order to evade the FCC order restricting student loan robocalls. In this manner, providers cooperating with grey-area telemarketing operations providing underlying services have complied with the "no student loan robocalls" order by shifting their offering to "general loan" services. Further efforts to curb all loan and debt-related robocalls would be necessary to observe an overall reduction in total robocalls received by the public from these operations.

Auto Warranty Campaigns

YouMail estimates auto warranty robocalls peaked at 150M weekly calls. Joint efforts by state and Federal enforcement from late 2021 through 2022 have effectively eliminated the auto warranty robocalls with a 99 percent reduction to weekly auto warranty robocalls. At present, the small number of remaining auto warranty calls in the ecosystem,which are so small relative to the period of 2020–2022 in the graph they are only a few pixels tall on the graph, appear to be lawful, legal calls.

The final blows to these calls were delivered by the FCC on July 21, 2022, with an order [18] to all U.S. providers to avoid or cease carriage of auto warranty robocall traffic.



Weekly Estimated Auto Warranty Robocalls

Traceback & Transparency

On September 29, 2023, the FCC released a Traceback Transparency report [19]that detailed 844 tracebacks (1,043 tracebacks records, IDs 12808–13882) from the period of April 1, 2023, through June 30, 2023.

---

[18] *https://www.fcc.gov/document/robocall-enforcement-order-all-us-based-voice-service-providers*

[19] *https://docs.fcc.gov/public/attachments/DOC-397295A1.pdf*

The 844 tracebacks were grouped in campaigns from 21 campaign topics tracked by YouMail. These campaign topics were: Amazon Imposter, Authorized Order, Auto Warranty, Customs & Border Patrol Imposter, Camp Lejeune Solicitation, Financial Services Imposter, Package Delivery Imposter, Debt Reduction/Elimination, Financial Hardship, Healthcare Assistance, Home Services, CSP Imposter, Loan Approval, Medicare Offer, Mortgage Assistance, Disability Assistance, Contest/Sweepstakes, SSA Imposter, Student Loan Assistance, Tax/Debt Relief, Utility Imposter.

US Originating Providers (ORG)	61
Non-US Originating Provider (IOR)	14
Point-of-Entry Providers (POE)	51
Non-Responsive Providers (NR)	59
TOTAL Distinct Providers	174

Of the 174 unique providers receiving the 844 tracebacks, there was an average of 4.87 per quarter per provider, or 1.6 per month per provider.

In many cases, multiple tracebacks within the same day reached the same provider. If we recognize this as a "daily provider traceback incident" covering multiple tracebacks within the same day, there were 371 "daily provider traceback incidents" in the 3-month span across the 174 providers. The average provider received 2.1 "daily provider traceback incidents" in the period, or just 0.7 "daily provider traceback incidents" per month.

A provider receiving just a single "daily provider traceback incident" (1 per month) would be higher than the average provider (0.7 per month).

YouMail is often asked in industry discussions to reflect on how many tracebacks in a period are too many? This report is the first such report in which these types of averages can be calculated per provider, day, or campaign, which can enable any analyst engaged by a voice provider to measure relative concern when receiving a traceback.

Based on this now-public data, YouMail encourages providers to take even 1 isolated traceback as a serious matter to apply investigative resources to find all eliminate all present substantially similar traffic, while also implementing preventative controls to disallow new account creations that will bring back the same traffic under a new name. However, it is important to realize that every hour spent by a provider investigating beyond the minimum increases costs and decreases revenue, so the teams at these providers tasked with this responsibility are often at odds to the rest of their organization seeking to minimize costs and maximize revenue.

One Shutdown Equals Dozens of Sales & Revenue Opportunities

Voice service providers have tremendous freedom in how they react to becoming aware of unlawful traffic traversing their network. Some may shut down just a single account as their "responsible action" because that is all the evidence indicated to them was problematic. Providers currently employing policies of quickly shutting down a single account without an extensive investigation not only save expenses on investigating the traffic, but they also retain revenue by turning a blind eye to other accounts carrying similar traffic. In not introducing extra steps and friction into their new account onboarding process, they maximize the conversion rates and success of onboarding new, incoming revenue.

If a provider with effective investigative processes and strong controls succeeds in exterminating these accounts, while industry operates without an advisory to not enable the actor (such as the ones that industry received regarding auto warranty and student loan robocalls), the robocall bad actors have learned that they should use the services of multiple voice providers in order to have back-up routes to deliver their traffic and often contact dozens of voice providers over the next week to re-establish their operations. Thus, one decisive action by a thorough provider creates a sales opportunity for dozens of their less careful competitors, especially when those dozens do not employ strict requirements to verify the customer or their traffic, or obey similar no-tolerance policies before and after onboarding new accounts.

YouMail Direct Disruptions

Using intelligence and evidence from its own proprietary data sources, YouMail Protective Services conducts direct disruptions of illegal communication campaigns at cooperating communication service providers. These communications disruptions include voice calls, SMS, MMS, RCS and iMessage channels.

For the period of June 2023 to September 2023, YouMail Protective Services disrupted 2,366 non-voice messaging vectors, enabling illegal imposter communications over SMS, MMS, RCS and iMessage channels.

June 2023	700
July 2023	674
August 2023	603
September 2023	389

YouMail is expanding these capabilities, working jointly with enterprises in communications, finance, retail and hospitality, as well as trade associations, with the goal that once the illegal campaigns have been modeled and confirmed by the impersonated enterprise, they can be shut down at cooperating enabling communications platforms within their first minutes to first hour of operation.

VII. Concluding Remarks

My testimony reflects a brief assessment of industry relative to the current state of robocalls, robotexts, omni-channel marketing platforms used by telemarketers and threat actors, potential impacts of generative AI, and the successes and challenges in industry compliance and enforcement.

Significant enforcement progress has been made through Federal and state efforts, and I am proud that YouMail and its team have played an important role in some of the most notable successes, particularly when the crosshairs have been trained on specific unlawful robo-communication operations (robocalls, robotexts, and robo-messages on private platforms).

Communications have evolved significantly over the past decade, and businesses and individuals communicate through more channels and mediums than ever before in human history. As generative AI finally brings a robot, indistinguishable from a human to robo-communications, the public has never been at greater risk.

I urge Congress, as well as state and Federal agencies, to recognize that the digitalization of society, along with automation of and ease of accessibility to communication platforms, could very well mean that U.S. citizens are now at greater risk of harm sourced digitally than by physical threat. Agencies should strongly consider expanding their budgeted resources to increase investigative and enforcement capabilities, while simultaneously considering new policies to address bad early adoption threat actors, capitalizing on next-generation robo-communication tools.

Thank you for your time today. I am happy to answer any questions.

Senator LUJÁN. Mr. Rudolph, thank you so very much as well for being with us today. I am going to recognize myself for 5 minutes for your questions. Now, as you all can see on the image behind me, there are multiple examples of scammers impersonating companies to trick consumers and steal their information.

Now, these are real messages collected by my staff, but the links were changed so that we don't inadvertently encourage people to go to these links as well and therefore supporting that fraud. Now, this is a problem for so many industries, from delivery services, to streaming platforms, to financial institutions, to Government agencies.

And I very much appreciate the groups that are walking in now. I don't want to detract from the questions that I have, but you all know what robocalls are and robotexts are with your devices. I am seeing a lot of heads nodding yes. I am sure you are tired of them, and you want them to end.

That is what this hearing is about. And so, if you all have ideas as well, we would invite them to be submitted to us. So, the class or the trip that you are on, we may be leaning out to you to be able to solicit that information with what is happening to each and every one of you.

Now, Ms. Brown, yes or no, does the prevalence of texts and calls impersonating U.S. companies negatively affect the ability of your member companies to reach and build relationships with consumers?

[Technical problems.]

Senator LUJÁN. Your microphone——

Ms. BROWN. Oh, got it. Got it. Sorry. Thank you. Sorry about that. I don't know that it lends itself to a clean yes or no. The Chamber is really concerned about business impersonation fraud and the texts that you see. But I think, I don't know that we have seen a noticeable harm to the overall business relationship with our customers.

Like it is a part of the package and I think our—the Chamber members do a good job of keeping those relationships. But it is a worry, the brand dilution. And for instance, the Marriott case that I mentioned earlier, it is a concern that you know, the brands will be diluted by this kind of fraud.

Senator LUJÁN. And I will share with you my experience, Ms. Brown. There are some companies when they are calling my phone now, I will not answer, because I have been hit over and over by robocalls from them. There are some companies where they have been spoofed before, but it has not been time and time again. But I am less likely to answer them, or I am very cautious as well.

Now, that is my behavior. I don't know if that is consistent with others across the room. When I was asking them, I saw a lot of heads nodding yes. And so, we want to make sure that there is that trust that can be established with this form of communications. I appreciate that.

My follow up is, Ms. Saunders, I wanted to talk about the impact on consumers specifically. Can you share examples how messages and calls such as these defraud customers and limit access to goods and services?

Ms. SAUNDERS. Was that to me?

Senator LUJÁN. Yes.

Ms. SAUNDERS. Yes. I have an example of an elderly woman in Virginia who answered a prerecorded call purporting to be from the Social Security Administration that it had found drugs in a car associated with her and that if she didn't pay a certain amount of money to do a certain—take a certain number of steps, she would lose her Social Security.

And as a result, she actually ended up losing hundreds of thousands of dollars of savings. I have many more examples. I don't know how much time you want me to take with them, but there are—a lot of them are written up in our scam report that is on our website.

Senator LUJÁN. And Jeff, what I may do is, if we can get that report, we will ask unanimous consent to submit that into the record as well, Ms. Saunders, just so that it is part of the record for this particular hearing.

[The report referred to can be found at the following link:]

https://www.nclc.org/resources/scam-robocalls-telecom-providers-profit/.

Senator LUJÁN. So, thank you so very much. Mr. Bercu, one of the recommendations in your testimony supports the FTC and FCC clarifications of consent for safe calls.

Earlier this year, as you said, Senator Markey had worked on some other issues, but Senator Markey and I had also led a letter to the FCC Chairwoman asking the Commission to update guidance along the lines of the FTC, reinstating long held requirements for unwanted telemarketing calls.

Now, Mr. Bercu, you also cited evidence that consumer consent for telemarketing is increasingly falsified. Automated bots and other artificial intelligence systems are using public data to consent on behalf of a consumer for calls they never asked for or do not want.

How can industry, FTC, and FCC update guidance to develop standards that would limit the use of automated bots to falsify consent for robocalls?

Mr. BERCU. Thank you, Chair Luján. I think on this issue, I think the courts and the guidance that is out there are pretty clear already. You need an actual consumer's consent, and if it is falsified, it is not consent.

So, I think those are clear, and if there is any ambiguity, happy to work with you and your staff on resolving that ambiguity, because consumers should only be in the calls they actually consented to.

Senator LUJÁN. I appreciate that very much. Ms. Fischer, the floor is yours for questions.

Senator FISCHER. Thank you, Chairman Luján. To begin with, I would like to ask unanimous consent that a statement from Senator Thune, and a letter from ACA International and the Credit Union National Association be made part of the hearing record.

Senator LUJÁN. Without objection.

[The information referred to follows:]

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

Good morning and thank you Chairman Luján for holding today's hearing.

Protecting Americans from illegal robocalls has long been a priority of mine while serving on this committee.

Illegal robocalls are not only a major nuisance, but they can be dangerous and defraud consumers out of money or steal a consumer's identity information.

Many individuals who fall prey to these scammers can spend months or even years getting their life back.

At the same time, it's important to remember that not all automated calls are inherently negative.

Many important services are carried out via robocall where companies and call recipients have pre-established relationships and where the consumer has agreed to participate in these types of calls.

For example, some entities like hospitals and pharmacies use robocalls to remind a patient of an upcoming appointment or that a prescription is ready for pick-up; airlines use automated calls to notify a consumer if their flight is canceled; and credit card companies may use calls to notify consumers of important fraud alerts.

In an effort to reduce fraudulent and illegal robocalls, I authored the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act with Senator Markey, and the legislation was signed into law in 2019.

The TRACED Act made several important steps to fight the scourge of robocalls by providing regulators with the tools to discourage illegal robocalls and crack down on offenders.

It provided the FCC with more time to identify robocallers who intentionally violate the law.

It established rules to protect consumers from the issue of so-called one-ring scams, where international scammers try to get individuals to return their calls so they can charge them exorbitant fees.

TRACED required carriers to adopt an industry-developed standard for call authentication.

And it helped bolster private-led efforts to trace the origin of unlawful robocalls.

These are just a few of the provisions in the TRACED Act that are helping make it safer to answer your phone again.

We knew the TRACED Act wouldn't stop every illegal robocall, but the good news is that since the TRACED Act was signed into law, illegal and scam robocalls are down.

When TRACED Act was signed into law, consumers were receiving over 2 billion scam calls a month.

Since that time and with the implementation of the TRACED Act, scam robocalls have nearly been cut in half.

While that is a significant improvement, it's not to say there isn't more work to be done.

The prosecution of illegal robocallers can be difficult since many scammers are based abroad and can quickly shut down before authorities get to them.

New technologies have made it easier for scammers to hide from law enforcement and deceive consumers, such as using deepfakes produced by artificial intelligence to mimic family members' voices.

However, Congress has provided the regulators with several tools to go after illegal robocallers, and we need to also make sure the relevant agencies are using those tools to deter bad actors.

The Department of Justice is responsible to prosecute forfeiture orders issued by the FCC.

Despite having the clear authority to collect these unpaid fines, it appears the DOJ has not been carrying out this responsibility.

If we're going to hold bad actors accountable and truly tackle the issue illegal robocalls, it's going to require cooperation from all of the relevant Federal partners and industry.

So I'm interested in hearing from our panel today about what steps are needed to continue to reduce illegal robocalls because one of the biggest negative effects of these illegal robocalls is that they frustrate recipients to the point that they are less likely to answer legitimate calls.

I'll continue my work to protect Americans from illegal robocalls.

Today, I'm eager to hear about the TRACED Act's implementation, and what more needs to be done.

I appreciate each of the witnesses being here today and look forward to your testimony.

Thank you, Chairman Luján.

ACA INTERNATIONAL
October 24, 2023

Senator BEN RAY LUJÁN,
Chair of the Subcommittee on
Communications, Media, and
Broadband,
Washington, DC.

Senator JOHN THUNE,
Ranking Member of the Subcommittee
on Communications, Media, and
Broadband,
Washington, DC.

Dear Chairman Luján and Ranking Member Thune:

On behalf of ACA International, the Association of Credit and Collection Professionals (ACA), I am writing regarding the Subcommittee on Communications, Media and Broadband hearing titled "Protecting Americans from Robocalls." ACA represents approximately 1,700 members, including credit grantors, third party collection agencies, asset buyers, attorneys, and vendor affiliates, in an industry that employs more than 133,000 people worldwide. Most ACA member debt collection companies, however, are small businesses. The debt collection workforce is ethnically diverse and 70 percent of employees are women.

Background about ACA International

ACA International members play a critical role in protecting both consumers and lenders. ACA International members work with consumers to resolve consumers' debts, which in turn saves every American household, on average, more than $700, year after year. The accounts receivable management ("ARM") industry is instrumental in keeping America's credit-based economy functioning with access to credit at the lowest possible cost. For example, in 2018 the ARM industry returned over $90 billion to creditors for goods and services they had provided to their customers. And in turn, the ARM industry's collections benefit all consumers by lowering the costs of goods and services—especially when rising prices are impacting consumers' quality of life throughout the country.

ACA International members also follow comprehensive compliance policies and high ethical standards to ensure consumers are treated fairly. The Association contributes to this end goal by providing timely industry-sponsored education as well as compliance certifications. In short, ACA International members are committed to assisting consumers as they work together to resolve their financial obligations, all

in accord with the Collector's Pledge that all consumers are treated with dignity and respect.

ACA members support FCC efforts to target illegal scam calls and text messages. Illegal fraudsters should be eliminated from the marketplace. However, certain FCC policies have done little to stop bad actors who do not care about the law, and instead have resulted in limiting legitimate informational calls that consumers need. ACA supported the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act), because of its efforts to target bad actors harming consumers. However. Carriers and the FCC have not kept up with their end of the bargain in this important law. Instead of providing clear standards for transparency and redress options when calls and texts are blocked from legitimate businesses, the FCC has allowed for opaque and incomplete standards that allow carriers to continue blocking needed calls with must know information. We ask that Congress consider the following concerns:

FCC's Work on Text Message Blocking

This spring the Federal Communications Commission (FCC) proposed (1) to require terminating mobile wireless providers to investigate and potentially block texts from a sender after they are on notice from the Commission that the sender is transmitting suspected illegal texts, (2) to apply the National "Do Not Call" Registry's restrictions to text messages, and (3) to restrict the ability of entities to obtain a consumer's single consent and use that consent as the basis for multiple callers to place marketing calls to the consumer.

The Commission should not impede the completion of text messages sent by legitimate businesses to their customers and other consumers. To protect text messages from legitimate companies, the Commission should require mobile wireless providers to notify the sender immediately when the provider has blocked the sender's text message and to resolve disputes no longer than six hours after receiving the dispute. ACA with a large group of other stakeholders has outlined (*here*) actions the FCC can take to protect legitimate callers and consumers.

A sender of text messages can only take action to dispute an erroneous block if the sender knows that its text message has been blocked. Unfortunately, the FCC's erroneous thinking in this area in its Report and Order inaccurately stated that carriers are "already providing adequate notice when they block texts." The Commission should require immediate notification of blocking.

Call Blocking Activity

In May, the FCC put out another call blocking order and further notice for combatting illegal robocalls. The FCC unfortunately has missed the mark on requiring carriers to put effective processes in place to ensure call blocking is done with transparency and redress options, as Congress required in the TRACED Act. A large group of impacted callers outlined a number of concerns as they work towards seeking appropriate redress.[1] As noted, several industries report that the informational calls that they place, including fraud alerts and servicing calls, continue to be mislabeled as "spam" based on the analytics of voice service providers or their third-party analytics service providers. This can discourage customers from answering the call or lead voice service providers or third-party analytics service providers to block the call. Both of these results prevent consumers from receiving important and often time sensitive information.

Revoking Consent

The FCC's 2015 TCPA Order clarified that consumers may revoke consent using any reasonable means and barred callers from designating the exclusive means of consent.[2] This past summer the FCC proposed to codify this requirement. The notice specifically proposes to codify its "previous decision that consumers only need to revoke consent once to stop getting all robocalls and robotexts from a specific entity." The Commission, however, does not cite any previous decision where it has ruled that a single revocation stops everything. The Commission here also seems to be creating a new regulation rather than codifying an existing ruling. Most concerning, the FCC proposes to require callers to honor revocation requests within 24 hours of receipt. This is a dramatic departure from existing practice that, coupled with

---

[1] *https://policymakers.acainternational.org/wp-content/uploads/2023/08/ABAJointTrades CommentCallBlocking-FCCEighthNPRM-August2023.pdf.*

[2] Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02–278, WC Docket No. 07–135, Report and Order, 30 FCC Rcd 7961 (2015) ("2015 TCPA Order"). 3 Notice para. 8 (emphasis added).

banning use of exclusive procedures and deeming the revocation to apply to all future robocalls and robotexts, creates an impracticable standard.

The Commission predicates its 24-hour rule on the use of automated systems to process revocation or opt out requests. Requests to revoke consent do not, however, always utilize automated systems and the Commission's rules will allow a number of different channels to submit such requests. Even where automated systems are used, they only work to quickly process requests when consumers utilize prescribed means, which the proposed rules would disallow. For example, text messages almost universally enable consumers to cancel further messages by texting STOP. If a consumer instead texts a word that the system is not programmed to recognize, or sends a phrase, sentence, or emoji, the requests will not be processed automatically. Even if the consumer uses the prescribed method, the sender may process the revocation request only with respect to the category of information or channel of communication involved in the original message.

The proposed rule that a single revocation stops all future robocalls and robotexts requires coordination and communication throughout the enterprise and among the various third-party vendors a company may use for communications. The confluence of precluding exclusive means, an unlimited scope of revocation, and the 24-hour rule creates a standard that is impossible to meet in many cases, and at the very least creates compliance uncertainties.

Congressional Discussions

Congressman Frank Pallone, Jr. (D–NJ) issued a statement, "denouncing the ongoing epidemic of abusive robocalls practices," which he says have been exacerbated by the Supreme Court's ruling in *Facebook, Inc.* v. *Duguid,* which interpreted the Telephone Consumer Protection Act's definition of "autodialer". The Supreme Court correctly found that to qualify as an ATDS under the TCPA, a device must have the capacity to either: Store a telephone number using a random or sequential number generator, or produce a telephone number using a random or sequential number generator. In other words, equipment that can store or dial telephone numbers without using a random or sequential number generator does not qualify as an ATDS under the TCPA.[3] While the plaintiffs' bar surely regrets the clarity that the 9–0 decision from the Supreme Court provided on this issue, it is an important development for a host of businesses making informational calls with much needed information for consumers. It has also decreased class action litigation under the TCPA.[4] Fraudulent calls aimed to harm consumers should be limited. However, the wide variety of financial services calls that consumers need including account updates, information about stolen credit cards, and other must know financial information should be supported by Congress.

We understand the serious problem that fraudulent nuisance calls present for consumers and it is important to consider public policy objectives to limit them. However, the truth is that illegal scam artists do not care about the law and as evidenced in recent years, do not pay fines even when presented with them. More should be done to address this without laws or regulations that in an overreaction actually stop calls and texts with needed information.

Thank you for your attention to the concerns of the ARM industry. Please let me know if you have any questions.

SCOTT PURCELL,
Chief Executive Officer,
ACA International.

---

[3] In April 2021, the U.S. Supreme Court issued a 9–0 decision in *e your browser tools to copy the text, then click Close. Facebook, Inc. v. Duguid,* 141 S. Ct. 1163, finding that many lower courts were improperly interpreting what types of technology were considered an ATDS. The Supreme Court justices were clear that Congress drafted the TCPA to address abusive telemarketing, not to punish legitimate business callers.

[4] WebRecon Stats Dec '22 & Year in Review, available at *https://webrecon.com/webrecon-stats-dec-22-year-in-review/?utm_source=ActiveCampaign&utm_medium=e-mail&utm_content=WebRecon+Stats+Dec++22+%26+Year+in+Review&utm_campaign=Dec+2022+Newsletter&vgo_ee=AqSuxCM3%2B72kAO9%2FZXuiVzpLB9tk6tN1Fm%2BmFY3WWOeL8u0%2BWBCfKIYwvb2riYN9.* (noting that For the full year 2022, FDCPA (-31.3 percent) and TCPA (-10.8 percent) were both down significantly over 2021).

CREDIT UNION NATIONAL ASSOCIATION
Washington, DC, October 24, 2023

Hon. BEN RAY LUJÁN,
Chairman,
Committee on Commerce, Science, and Transportation,
Subcommittee on Communications, Media, and Broadband,
United States Senate,
Washington, DC.

Hon. JOHN THUNE,
Ranking Member,
Committee on Commerce, Science, and Transportation,
Subcommittee on Communications, Media, and Broadband,
United States Senate,
Washington, DC.

Dear Chairman Luján and Ranking Member Thune:

On behalf of the Credit Union National Association (CUNA), I am writing regarding the Subcommittee's hearing entitled, "Protecting Americans from Robocalls." CUNA represents America's credit unions and their more than 135 million members.

We share with Congress the overriding goal of restoring trust in communications networks that has been tarnished by unscrupulous persons preying on consumers or companies that make no serious efforts to comply with the Telephone Consumer Protection Act ("TCPA). Illegal robocalls not only harm consumers but also legitimate businesses that are increasingly being impersonated by fraudsters that send texts or make calls claiming to be one of our member credit unions. Fraud facilitated by illegal robocalls and robotexts causes financial harm to both members and their credit unions. Thus, we whole-heartedly support efforts to target bad actors, get them off and keep them off the network.

Unfortunately, the TCPA has little, if any, deterrent effect on bad actors' intent on defrauding consumers. Fraudsters are often located in other countries beyond the TCPA's reach or they simply ignore the law knowing they are unlikely targets of private litigation. Instead, all too often the TCPA, which combines strict liability with statutory damages, has become a mechanism to extract monetary settlements through threats of class action litigation against companies that are making good faith efforts towards compliance. America's credit unions spend substantial resources to comply with TCPA's complex array of regulatory requirements yet face litigation risk for making innocent mistakes, such as calling a wrong number. Further expanding the TCPA will not materially advance the goal of restoring trust in our communications network.

Recognizing the limitations of the TCPA to deter bad actors, the FCC has turned to technological solutions such as automated calling number authentication (STIR/SHAKEN), call blocking regime, and caller traceback. We applaud the Commission's recent successes in using these tools to identify and shut down some of the worst abusers. These tools are still evolving and, while aiding in identifying the worst actors, also result in legitimate calls being blocked or mislabeled.

Achieving a balance between facilitating legitimate calls while preventing illegal calls is necessary to restore trust in our communications network. Fortunately, Congress created a mechanism to achieve that balance. In the TRACED Act, Congress directed the FCC to ensure transparent and effective redress for companies whose calls are mishandled, and we have sought to work with the FCC to achieve the admittedly difficult balancing act of stopping bad calls without blocking good ones. We urge the FCC to move forward with the adoption of call blocking notification standards so that testing and implementation of this technology can begin.

On behalf of America's credit unions and their more than 135 million members, thank you for holding this important hearing and considering our views on the subject.

Sincerely,

JIM NUSSLE,
President and CEO.

Senator FISCHER. Thank you. I agree with the Chairman that this committee's focus on enforcement today is key.

First and foremost, though, I think we need to ensure that our laws and rules that are on the books are being enforced to the fullest extent. Since 2020, the FCC has issued 700 million in forfeiture orders for TCPA violations.

However, hardly any of these have been collected mostly due to the Justice Department's failure to pursue these cases in court. In

its obligations under the TRACED Act, the DOJ also seems to have missed the opportunity to submit a report with meaningful recommendations.

Ms. Brown, do you believe that the Justice Department is doing enough to ensure that bad actors carrying out illegal telemarketing and robocall schemes pay the penalties that the FCC assesses?

Ms. BROWN. Thank you for the question. And in my written testimony, we explain, no, I don't believe the Department of Justice is doing enough, and you can sense that frustration from the FCC Chairwoman.

They certainly at the department have a lot of tools that they can use, both to enforce FCC orders, but on their own to bring righteous mail fraud, wire fraud cases, and enforce the laws that you all have passed.

So, yes, we believe the United States Department of Justice should do more, and as a former DOJ official, I think it is a missed opportunity for them.

Senator FISCHER. So, what can we as Congress do to make sure that they do enforce those rules, that as you said, they have the tools. So how do we get them to use them?

Ms. BROWN. Well, I think that one challenge is it is hard for Congress to direct the Department of Justice to take specific action due to separation of powers. But you have a lot of power to nudge, cajole, and shape expectations.

And in my written testimony, we offer a few examples. In the TRACED Act, for example, you impose some pretty robust reporting obligations on the Federal Communications Commission. We think similarly you could impose those kinds of updates, mandates on DOJ to let you all know what they are doing.

We also suggest that DOJ should prioritize funds for investigations and enforcement, and you all can direct some of that. And then requiring DOJ, for example, to establish a robocall enforcement and education office.

Right now, at the Department, I think much of their robocall effort is housed under an elder justice initiative, and I think that is really important, obviously, but they can do more. And I think Congress can really look into that and impress upon them that this is a priority.

Senator FISCHER. You know, to me, this focus on enforcement really is two pronged. We want to make sure that the Government is going after the bad actors, and we want to avoid opening up legitimate actors to frivolous lawsuits.

Abusive litigation against businesses acting in good faith does nothing to stop criminals. Ms. Brown, would you provide some examples of TCPA filings that you view as litigation abuse?

Ms. BROWN. Certainly, thank you. And unfortunately, there are a lot, and I would commend to anyone's attention the work that the Chamber's Institute for Legal Reform has done. They have had several reports that give examples.

But one example that stuck out to me recently, the City of Albuquerque was sued after sending text messages to local residents during the COVID–19 pandemic to notify them of the opportunity to participate in socially distanced town halls.

And ultimately, Senator, I believe the city was able to get out of that lawsuit, but not after burdensome litigation. And that is just one example of many that seems to go after beneficial communications, or at least not the bad actors that I think we are here mostly to talk about.

Senator FISCHER. You know, we have many members on this committee who represent very rural states.

There is a lot of vastness in our states, and we want to make sure that rural Americans receive services, Governmental services, but also services from private industry. And many of rural America is still connected with copper mines and they are vulnerable when we look at these fraudulent schemes that are out there.

Mr. Bercu, what are the challenges that remain for these copper based voice service networks in terms of stopping illegal robocalls and their telemarketing schemes? And does this lack of fiber that we see in rural areas, does that have an outsized effort on most of our rural constituents that we have?

Mr. BERCU. Thank you. I think there are challenges. I know the industry is very committed to moving to IP and that work is ongoing. Yes, when STIR/SHAKEN information can't be passed to the legacy networks.

But what I would say is that the protections in place are helping all consumers. When we trace back calls, those calls are hitting people in New York. They are hitting people in rural America as well.

And so, when we get them off the network, that is helping everyone. Same with STIR/SHAKEN. It is helping infuse accountability that benefits everyone, whether they are getting their calls with STIR/SHAKEN or not.

Senator FISCHER. Yes, thank you. Thank you, Mr. Chairman.

Senator LUJÁN. Thank you very much. Senator Markey, you are recognized for your questions.

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

Senator MARKEY. Thank you, Mr. Chairman. In 2019, I was proud to partner with Senator Thune to pass the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, the TRACED Act, which directed the Federal Communications Commission to issue critical new rules to crack down on illegal robocalls.

The TRACED Act has helped stop some of the worst practices by robocallers, but robocalls remain a plague on our telephone system. My constituents in Massachusetts received over 623 million robocalls last year, nearly 20 robocalls per second. This year, Massachusetts residents are on pace to receive 800 million robocalls.

Across the country, Americans are on pace to receive 54 billion robocalls this year. Some robocalls are lawful, but of course the numbers of unlawful calls are astonishing. To each of the witnesses, starting with Ms. Saunders, do you agree that robocalls remain a serious problem for consumers, yes or no?

Ms. SAUNDERS. Yes.

Senator MARKEY. Ms. Brown.

Ms. BROWN. Unlawful and illegal robocalls certainly do. Yes—whoops, sorry.

Senator MARKEY. Yes. Mr. Bercu.

Mr. BERCU. Yes, illegal robocalls remain a problem.

Mr. RUDOLPH. Yes, absolutely.

Senator MARKEY. Thank you. These fraudulent robocalls cost consumers tens of billions of dollars every year and undermine trust in the telephone system. That is a serious problem, period.

And I want to turn to one particular element of the TRACED Act. The law directed the FCC to require the telephone providers adopt a technical standard to verify that caller ID information was accurate.

Senator Thune and I drafted this provision to stop bad actors from falsifying caller ID information, a practice known as spoofing. Robocallers often spoof calls to make the caller ID indicate that a call is coming from a local number.

I am pleased that the FCC has worked expeditiously to implement this provision, but I am also deeply alarmed by the sheer number of fraudulent robocalls and scams. Robocallers seem to be changing their methods faster than we can adjust.

Ms. Saunders, do you agree that the TRACED Act has been helpful in reducing the number of spoofed calls, but that robocallers have found ways to circumvent these rules?

Ms. SAUNDERS. Yes, sir, I do.

Senator MARKEY. And Mr. Rudolph, do you agree with Ms. Saunders' assessment?

Mr. RUDOLPH. Absolutely. I know we see less spoof numbers than ever before. We see that the threat actors, especially those impersonating banks, getting real active phone numbers. And also jumping when a bank branch closes down, grabbing that number and then using that number to contact people.

Senator MARKEY. Yes. It is unbelievable. Targeting robocallers is like an endless game of whack a mole, and so far the moles are winning by an astonishing margin in this battle. If the robocallers have evaded the caller ID system by exploiting how phone numbers are distributed, then we may need to adapt our regulations as well.

And I want to say one final word about the FCC's robocall mitigation data base. Every telephone provider must register with that database at the Federal Communications Commission, and companies that have not yet implemented the caller ID verification system must submit a plan for addressing illegal robocalls.

Last week, the FCC took an important step to begin removing 20 noncompliant companies from the robocall mitigation data base. Some of the companies' filings were laughable. Here is one. Here is one of the filings right here. Pretty simple to see. It is a blank piece of paper.

That is what they have submitted in terms of their compliance with the law. Another filing was a picture of the company's logo. Another provider submitted a document that said nothing in capital letters on the sheet of paper on the website, nothing.

I am glad the FCC has launched enforcement proceedings against these obviously problematic filings, and I appreciate the ideas that Ms. Saunders has suggested to further strengthen the robocall mitigation data base.

I look forward to continuing to work with the Commission and my colleagues on this issue. It goes right to the heart of the issue that just drives every American crazy every single day, the unwanted robocalls coming into their lives all day long at the most inconvenient times, almost knowing that you are home, and you are having dinner with your family to be the perfect time to get the whole family angry at these companies.

So, we thank you, Mr. Chairman, for having this hearing, and we just have to keep our focus on this issue. Thank you all so much for everything that you are doing.

Senator LUJÁN. Senator Markey, thank you very much. And especially bringing attention to the filings at the end of your testimony today. I am reminded that some of those filings also include menus from restaurants as being submitted as official documents as well.

So, thank you very much on bringing more and more attention to the enforcement side of this. Thank you very much, Senator, and your work on this. Senator Budd, you are recognized for 5 minutes.

STATEMENT OF HON. TED BUDD,
U.S. SENATOR FROM NORTH CAROLINA

Senator BUDD. Thank you, Chairman. And I thank you for the witnesses for being here today. You know, when I talk to folks from North Carolina, they ask me about this topic a lot. They talk about robocalls, and they express their frustrations, some of them. They don't want to download the app that helps screen these things or pay a few extra dollars for that. So, they are frustrated. They want some solutions.

When I was in the U.S. House a year ago, I was proud to be an original co-sponsor of the TRACED Act, which I think it is making a difference. According to YouMail, scam, robocall volumes have declined about 55 percent since their peak in October 2019. Tools like Industry—the Industry Traceback Group and deployed authentication technologies like STIR/SHAKEN—great name, by the way, they better detect spoofing. They seem to be working.

So, I think we all still agree, however, that there's still a lot of work to do. So, Mr. Bercu, in your written testimony you noted that, "Government and brand imposter calls predominantly originate abroad.

These are scams where someone claims to be calling from the IRS regarding back taxes or from the local power company on an overdue bill. These scams are particularly dangerous because they pretend to be communication from important institutions like Government agencies, utilities, or from banks."

In your working with the Industry Traceback Group, have you identified any gaps in Federal efforts to prevent illegal scam robocalls that make going after those foreign callers difficult?

Mr. BERCU. Thank you. Yes, it is difficult because they feel they are not going to face justice because they are not based here. They use shell companies. They get kicked off a network and find a new one. So, absolutely, we have been very effective in disrupting them. We have seen some of the impact, especially on the robocall side, that the scam volume is way down.

But, you know, it is one of the reasons, you know, I agree with my colleague here, Megan, that criminal enforcement against these individuals, these groups that is organized crime abroad doing this is absolutely critical because that—the only way they are going to stop trying to defraud Americans is if they are taken off the board. So, we think that is very important.

Senator BUDD. Thank you. So, you mentioned for—you mentioned the enforcement agencies. What could some of them do to improve the success rate of stopping these foreign placed robocalls?

Mr. BERCU. So again, I think criminal enforcement is key. When the—a few years ago, when the Department of Justice, FBI worked with the Central Bureau of Intelligence in India to raid some of these call centers, Government impersonation scams went down almost overnight. So, that is key. It is really working with those partners abroad and bringing people to justice, I think is the key.

Senator BUDD. Thank you. Ms. Brown, in your testimony you discussed how the Department of Justice does not sufficiently prioritize prosecuting bad actors who break robocall laws and they attempt to defraud Americans.

How does a lack of enforcement action influence efforts to shut down scams and make the cost of illegally robocalling significant enough to dissuade criminals?

Ms. BROWN. Thank you for the question, Senator. I think the lack of DOJ enforcement kind of shows that the FCC's efforts really run out of steam if the department is not there to sort of get them across the finish line to actually collect on some of those forfeitures.

Similarly, there are open and notorious scammers that seem to me very clearly violating the wire fraud and the mail fraud statutes. And I think sending a message, as Josh was just saying, whether it is to overseas scammers or domestic scammers—I mean, some of the folks the FCC has brought enforcement actions are right here in the United States.

And the Department has taken a few actions to bring some cases, but I think they could do far more to send that message that we are not going to tolerate these scams and the fraud that Margot discussed.

Senator BUDD. Thank you. So how would small businesses, who themselves can be victims of these robocalls and illegal scam calls, how would these small businesses benefit from increased DOJ enforcement of the existing laws?

Ms. BROWN. Is that to me, Senator?

Senator BUDD. Sure.

Ms. BROWN. Great. I think they would benefit in the same ways that consumers would if they are being victimized and they don't have the resources to deploy sophisticated anti-fraud, then sending that message to take, as Josh said, some of these bad actors off the board, I think would be really, really helpful to them in much the same way that consumers are being defrauded.

Senator BUDD. Anyone else helping small businesses?

Mr. RUDOLPH. First, I would like to commend your Attorney General. North Carolina is one of the top leaders in robocall enforcement at the State level.

I would say that small businesses, we have data that shows some of the threat actors understand that they have got deeper pockets,

I suppose, as a targeted victim. So, we are seeing a rise in specifically the robocalls and robotexts.

They are trying to hit small business owners and convince them, you know, to engage in their campaigns.

Senator BUDD. Thank you. My time has expired.

Senator LUJÁN. Thanks, Senator Budd. Senator Tester, you are recognized for questions.

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

Senator TESTER. I want to thank you for holding this hearing, you and the Ranking Member. I appreciate it very much. I want to thank the folks who are testifying today.

We got murderers, we got child molesters, we got rapists, we got drug peddlers, we got people who commit armed robbery, and then we got robocallers, OK. And it distresses me a lot when I hear that there is $700 million of fines that have been levied and no collections.

Ms. Brown, you were—were you with the U.S. Attorney's Office at one point in time in your career. Is that what I gathered?

Ms. BROWN. I was at Main Justice at the Department of Justice.

Senator TESTER. Well, that is good enough. So, look, they got all this stuff. I know the U.S. Attorney in Montana, for example, is very, very busy running down people who are doing horrific crimes.

By the way, I could make a claim that this is nearly as horrific as any of those ones I mentioned before. Why? Because I have got a business. I was on top of a combine this year. The phone is ringing. I am expecting a call from my wife. I bust off the combine, damn near break my leg.

I get to the call and the guy is asking me if I paid my loan for when I was in school. I haven't been in college in 45 years, and I didn't have a loan when I went then because it was a different time, OK.

So, these guys are bad, bad people. The question I have is, the DOJ has levied these fines and none of it has been collected. There is an effort here in this body to defund the Department of Justice. Do they have enough people? For you, Ms. Brown.

Ms. BROWN. Well, having been at Main Justice, I know they have a lot of priorities. They have a lot of people. I do think the department can probably walk and chew gum at the same time and prioritize a few more of these cases, if that is what you are asking.

Senator TESTER. I would love it, because we can pass all the laws we want here and we can take credit for passing these laws, but unless somebody drops the hammer on these clowns and makes them pay a price, puts them out of jail, or better yet even puts them in jail, and I would pay more taxes to put these people in jail, I think it is going to continue to happen.

And it is going to happen—when I was in the State legislature, 20 years ago, we passed the do not call list. I have signed up for multiple do not call list, and I get more robocalls today than I did back in 2003, for example, 20 years ago. So, the question is, does Congress need to do any more, or is this all about enforcement?

Ms. BROWN. For me, again, Senator?

Senator TESTER. Ms. Saunders, I will let you go. Ms. Brown got the last one, so we will spread it around.

Ms. BROWN. Yes. It is your turn.

Ms. SAUNDERS. Our main point in our test—in the testimony that I have submitted is that the incentives need to be changed, whatever way it is done.

Senator TESTER. Well, I understand if you hit somebody in their wallet, that kind of hurts.

Ms. SAUNDERS. Right, right. And what we have proposed is that the FCC adopt a methodology such as is permitted under the Federal rules of civil procedure to get a temporary restraining——

Senator TESTER. And they have not done that yet?

Ms. SAUNDERS. No. So that once a particular voice service provider is found to be a repeat offender——

Senator TESTER. Yes.

Ms. SAUNDERS.—and to continue to process illegal calls after it has been notified previously——

Senator TESTER. Yes.

Ms. SAUNDERS.—the FCC should be—should suspend immediately its ability to——

Senator TESTER. OK. Do the rest of the people on the panel agree with that perspective? Ms. Brown.

Ms. BROWN. I haven't reviewed closely Ms. Saunders' proposal, but I am not sold that we need new authorities over at the FCC to do the kind of suspensions that she is talking about. I think they have got——

Senator TESTER. But do you think those suspensions would be OK if they did them?

Ms. BROWN. On the voice service side, I am not sure exactly whether there would be some unintended consequences there of what she is proposing, but they certainly can do more with their cease and desist orders and notices.

Senator TESTER. Mr. Bercu.

Mr. BERCU. So, I think when we are talking about fraud, one of the themes is that the fraud actors change their behavior. They have moved from robocalls to more targeted calls.

And some of the tools we have built for robocalls don't work as well for a live call. There is a big difference from I let someone on my network make——

Senator TESTER. But you know what, I don't—I very seldom get live calls. I get a call from a damn computer that sounds like a live person that then if I stay on long enough, goes to a live person who I ask, why don't they get a real job because there is plenty of jobs out there in society now instead of being a crook. So why is there a difference here?

Mr. BERCU. So, in that, that would be a pre-recorded call. But I still think enforcement against the fraudsters is really the key there, because they are going to keep adapting as the rules and the protections change. It doesn't mean we shouldn't keep adding more protections, but they will always keep working to try to get around them.

Senator TESTER. I got it. That is what a crook does. They look for the—and by the way, these are crooks. They look for the weakest link in the fence.

So, I came to this hearing hoping that I would hear from some of you, and I did hear from Ms. Saunders, your view, what we can do to stop. Not to slowdown. We have been slowing down forever. But to stop these folks. Anybody have anything that Congress can do to stop them or—I haven't asked you a question yet, Mr. Rudolph.

Mr. RUDOLPH. You referenced, you received a loan robocall, right.

Senator TESTER. Yes. I have taxes, loan robocalls. And by the way, it is the same voice, the same computer, the same call, sometimes called from my neighbor's phone, by the way. So, I don't know if that is illegal now or not.

I had a neighbor that got a call from his own phone number one time. I mean, this is crazy. This is crazy stuff that this country doesn't need in their economy. Keep going.

Mr. RUDOLPH. So, your loan robocall, I would strongly suggest that is domestic originated and that is an area that I would call gray area telemarketing.

So, in this case, right now we don't have—we track thousands of active campaigns per week and current enforcement efforts are just working on the highest volume, prioritized campaigns.

So, your specific robocall, if you can get your state or you can get the FCC to put that on the priority list, that is one that we have got the tools and the techniques to diffuse. There is just not enough manpower to, you know, have a priority list that goes more than 10, 15 campaigns deep.

So, if we can get—if we can start working, you know, 50, 100 campaigns deep on a week to week basis, the FCC has showed effectively, you know, that the highest volume campaigns can be stopped.

Senator TESTER. Just for the record, if any of you know how many these are done out of State versus in country, out of country, I would love to know that information. Thank you all. This is a bunch of crap, I will just tell you. We need to stop this. This is not good for anybody. And for the robocallers out there, go get a damn job.

Senator LUJÁN. Thank you very much, Senator Tester. Senator Vance, the floor is yours for questions.

STATEMENT OF HON. J. D. VANCE,
U.S. SENATOR FROM OHIO

Senator VANCE. Great. Thank you, Mr. Chair. And I agree with Senator Tester, and my questions are going to pick up largely in the same vein. Mr. Bercu, the thing that I struggle with sort of reviewing materials that my staff prepared for me for this hearing and just obviously experiencing this particular problem as a human being.

And I—you know, my own mom just a couple of weeks ago sort of called me and gave me the quick hits of a particular scam that had been—targeted her. And it seems like we keep on tinkering around the edges here a little bit. We sort of do these little things and maybe they slow it down to Senator Tester's point.

But we are fundamentally allowing crooks to prey on some of the most vulnerable people in our country, people who are living on

fixed incomes and so forth. And I guess I am just wondering if we were willing to do something big.

And it is one of the few things maybe that you could get bipartisan majorities in this House or this chamber to do. If we wanted to do something really big here, what could actually stop this, right.

So, the example that we talked about, or that I was talking about earlier just with a friend, is, you know, you ban robocallers from calling a particular number, but then let's say an individual goes and signs up on something online and they don't read the 75 pages of fine print, and one of those pages of fine print effectively signs their number up to be robocalled and that opens up the floodgates that allows criminals to go after them.

I am just wondering like what can we actually do to stop this thing? I want to pick up where Senator Tester left off.

Mr. BERCU. Thank you, Senator, for the question. I think one of the challenges here is the phone system by its nature is a series of interconnected networks. So, the providers that are providing service to us, all they know is like your mailman would know, what is the address? Where is this going?

They don't know what's inside the content. So that is the fundamental challenge. And what we do in Traceback, we trace back the illegal calls and we hit five, six, seven, eight providers that all touch it on way, and it mixes in with legal traffic as well.

So, I think that is where—I think what is big is criminal enforcement. It is the theme that I am going to keep hitting here because if—even if we stopped every single robocall, the criminals who do this, their day job is still defrauding Americans, and they will just find a new version.

So, the only way to get them to stop defrauding Americans is criminal enforcement.

Senator VANCE. Do we have a sense of how many of these people are actually in America versus how many of them are overseas?

Mr. BERCU. So, in our experience, it varies a little bit based on the type of call. So, the pure fraud robocalls, the pure fraud vishing calls, voice phishing calls, et cetera, those are predominantly coming from overseas.

The unsolicited telemarketing calls, those may originate here and be done by people here. But to what Megan said before, we—one of the reasons it is hard to collect fines against them is they pop up a new shell company, dissolved the old one, and are now doing new robocalls under a new name.

And I do think there are some laws that might apply and that might make that criminal.

Senator VANCE. And where are they coming from, the ones overseas? I mean, are there particular areas? You know, you sort of hear about Eastern Europe or Nigeria, sort of—where are these things actually coming from?

Mr. BERCU. A lot are from India, some are from Dominican Republic, some other countries as well. But India is a big portion of the calls.

Senator VANCE. And has there been any effort sort of diplomatically, legally, to interface with some of the countries where this

fraud is most common and actually use the extraordinary leverage the United States has to bring some of these folks to justice?

Or is there sort of an attitude like once it is in another country, it is such small ball things relative to other international crime, we don't focus on it, but of course, it is not small ball to the people who are affected by it.

Mr. BERCU. There has been collaboration. And when there is collaboration, when our FBI works with the Central Bureau of Intelligence in India and raids these call centers, we see the impact. YouMail data will show just Government imposter scams dropped immediately after those raids. So, I think that is a testament to why we should keep prioritizing that, because it does work.

Senator VANCE. OK. One final question here. We are actually going to an artificial intelligence briefing with some industry leaders later this afternoon. What could we do to help AI platforms and social media companies shield their data or tools from being used for more elaborate, you know, family emergency scams, things like that?

Mr. BERCU. You know, happy to work with you on that. You know, I am not sure how—what exactly you could do on the social media side. But one thing I will say is that the TCPA right now makes illegal robocalls to cell phones, and robocalls are making the calls with a pre-recorded or artificial voice. So, I think there—just one thing there is the TCPA I do believe applies.

Senator VANCE. OK, great. Thanks, Mr. Chair. I yield.

Senator LUJÁN. Thank you, Senator Vance. Senator Klobuchar, you are recognized——

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

Senator KLOBUCHAR. Thank you, Mr. Chair. A lot of questions here. I will go fast. First of all, we know that after the TRACED Act passed in 2019, after new FCC rules were in place, the number of scam robocalls declined by almost half. Now we are having all kinds of new issues.

And Mr. Bercu, you noticed in your—noted in your testimony that we—that there is collaboration between industry and the FCC. How can we make sure that tracing illegal calls to their origin results in actual enforcement action?

Mr. BERCU. So, I think what we have seen, the FCC's approach with the cease and desist, I think it has been highly effective. They have targeted certain campaigns. They have dropped off the face of the earth almost.

So, I think we are making great progress. I think the more we do—some of the rules the FCC did about know your provider, I think it is a process, and over time that is going to keep going the right direction. So, I think we have done a lot of great work there.

Senator KLOBUCHAR. OK. Good. Ms. Saunders, why do you think particularly these telemarketing calls, that these volumes are so high? I mean, I was just looking. We have got so many people, 221 million numbers registered on the do not call list, and still, we are seeing a number of people call about violations. What solution should we prioritize here?

Ms. SAUNDERS. So first, let me say that I believe that the number of scam calls there have appeared to be reduced because there has been a reorganization or recategorization of many of those calls. Many of the calls that had previously been identified as scams have now been identified as telemarketing calls.

And as Mr. Bercu said, most of the telemarketing calls originate in the United States. We think that what needs to be done is the FCC should adopt a quick acting, temporary restraining order type of methodology, and once a voice service provider is found to have repeatedly, after notice, processed scam or telemarketing calls, they should be suspended immediately from the robocall mitigation data base. That will cost them money. And even if they—after they have——

Senator KLOBUCHAR. So, that will make—that will be an incentive to be more careful.

Ms. SAUNDERS. That is correct.

Senator KLOBUCHAR. OK. All right. I like it. AI voice cloning. Senator Vance mentioned this. We actually had, I had someone I know that got one of these calls. His son serving in the Marines, deployed. So, he knew he was deployed, didn't know where. They get a call, because they scraped his voice off the internet, asking for money to be delivered to somewhere in Texas.

I have had two other military families tell me this story in Minnesota. I don't—this is unbelievable to me. So, what are service providers, Mr. Bercu, what are they doing to get ahead of these robocalls made using voice calling?

These are obviously targeted ones with the person's voice, but all kinds of things could happen. And what can we do, Mr. Rudolph, to mitigate this?

Mr. BERCU. Thank you. You know, the voice service providers take protecting their customers very seriously. They are always looking at the greatest technology. They have implemented blocking and labeling. They have analytics running on their network.

So, I think they will continue to try to find out how they can identify those scams and how they can take action accordingly. One of the things with our Traceback effort, whether it is a robocall or one of those calls, we can trace those back.

We can find out who is making them. We can find out who put it on the network. So, I think Traceback will be a really important part of stopping those going forward as well.

Mr. RUDOLPH. Your specific use case is a targeted attack.

And based on the investigations that we have done so far into similar attacks, those are threat actors who have gotten a personal phone and a personal phone number, just like anybody going into a store to get a device.

So those are extremely hard for a communication provider to deal with. It looks just like a customer making those phone calls, yes.

Senator KLOBUCHAR. Right. I understand. I get it, I get it. Yes, I am not—actually, I am just using it as an example. Then it could get worse, right?

Mr. RUDOLPH. Absolutely.

Senator KLOBUCHAR. And to the voice of general in that they know I am famous commander or something, anything, and it

would go to all the military families, or it would go to people thinking it is a political person and turns into a robocall. So, I do think this adds to the danger.

Last thing, robotexts. There were over 12 billion spam texts to Americans just last month. I think I got half of them. And these texts often include links that install malware and spyware on a consumer's device. In March, the FCC adopted rules. Ms. Saunders, what other measures should they consider to go with these illegal robotexts?

Ms. SAUNDERS. We have recommended to the Commission that it adopt special security rules for robotexts that include URLs just because of this significant damage. Congress could also pass regulations that—or statutes that provided more protection for consumers once they have had their money stolen from their bank accounts. There are—that would be a big help as well.

Senator KLOBUCHAR. All right. Thank you. Thank you, Mr. Chairman.

Senator LUJÁN. Thank you, Senator. Senator Welch, you are recognized.

STATEMENT OF HON. PETER WELCH,
U.S. SENATOR FROM VERMONT

Senator WELCH. Thank you very much. I mean, you are hearing the incredible frustration all of us have. You heard Senator Vance, Senator Tester, Senator Klobuchar. I mean, it is really driving our constituents crazy.

Vermont with 3.5—small State, 3.5 million robocalls just last month. It is like six calls per Vermonter. And it is really—it is really, really unsettling, especially to older people, who think they may be getting a call from a grandchild or a son or a daughter and they have to pick it up and figure out what is going on.

And I know you are trying to do stuff, but it is not working. It is not working in the way it needs to. You know, I joined Senator Luján and Senator Markey in asking the FCC to align its do not call registry guidelines with those of the FTC, as well as prohibit telemarketers from calling consumers without explicit consent.

Ms. Saunders, do you believe these actions would benefit consumers? And what additional steps can Congress take to push the FCC and better protect consumers from robocalls?

Ms. SAUNDERS. Thank you for the question, Senator. We have been pushing the FCC for months now to simply reiterate that the language in its current regulations mean what it says. And instead, the FCC has proposed regulation that would reduce protections from the current regulations, and we have been very afraid of this. So, actually——

Senator WELCH. Why is that? Why are they doing that?

Ms. SAUNDERS. We—I am not sure whether it is a misunderstanding or whether the lead generators and the sellers who are benefiting from these telemarketing calls have gotten to them, frankly.

But the proposed regulation or anything like it is very dangerous. The FCC issued regulations 20 years ago explicitly requiring that every telemarketing call is only legal if it is prerecorded.

If the consumer has provided a signed, written consent allowing that caller to make calls to that consumer.

And the proposed regulations would allow more calls per consent. Would not require a writing—and so, I can't tell you why they are issued—why they are proposed. But I can say that if you can encourage the FCC not to proceed in this way, it would be beneficial.

Senator WELCH. All right. Let me move on to a question for Mr. Rudolph. It is about generative AI. And, you know, there is some argument that that could help actually push back on the scammers, but it also obviously is a tool that is going to be used by scammers, especially generating a familiar voice.

Can you tell me how the evolving landscape for generative AI impact the ongoing efforts to combat fraudulent communications and protect consumers?

Mr. RUDOLPH. First, I would like to recognize your State as well. There is robocall platforms and robocall operations that refuse to call Vermont. That state is too hot to call.

So, your constituents benefit from your Attorney General's work in that regard. On the topic of generative AI, clearly threat actors have flocked to it. It allows them—allows one person to do the work of hundreds. Generative AI doesn't have ethics or questions about what it is doing as it is affecting social engineering.

On our side, on the good guys side defending against, you know, what is going on in industry—a Senator earlier showed a blank piece of paper as a robocall mitigation plan. Generative AI can—or a large language model can rip through the robocall mitigation database filings and actually synthesize and understand if there are sufficient or lacking sufficient controls.

So that is a great place where we can apply that technology and probably discard half the entries in the database in an afternoon or a week of work.

Senator WELCH. All right, Mr. Saunders, again, thank you. The STIR and SHAKEN, I want to go through it. You know it. But how can the FCC incentivize providers to use the available tools to block calls?

Ms. SAUNDERS. I think the FCC has done a very good job at implementing STIR/SHAKEN. And the problem with STIR/SHAKEN is not the particular technology. It is the fact that there is this whole other method for robocallers to use borrowed numbers, rotating numbers for—as Mr. Rudolph explained, for a minute or for a particular call.

And the ability of robocallers to use the numbering resources or misuse them in this way completely undermines the whole purpose of STIR/SHAKEN. So, I think now it is time for the FCC to drill down on the numbering resources misuse.

Senator WELCH. And thank you. I yield back, Mr. Chairman.

Senator LUJÁN. Thank you, Senator Welch.

Senator Hickenlooper, you are recognized.

STATEMENT OF HON. JOHN HICKENLOOPER, U.S. SENATOR FROM COLORADO

Senator HICKENLOOPER. Thank you, Mr. Chair. And thank all of you. What a fascinating issue that—I mean, you look at some of the issues around the world and this seems relatively small, and

yet when you talk to constituents in any of our states, we see this is top of mind, something that drives people batty. I mean, just they can't function.

Ms. Saunders, a number of cyber security experts have raised the issue of some companies functioning as consent farms. They are essentially tricking the consumers into, you know, they may be browsing a website, but they are tricked into basically signing on to—a consent to receive robocalls.

And first, I can't imagine how anyone—whether anyone, people actually intentionally would do that. I guess they must. Anyway, the FTC has launched investigations into companies who are behaving this way, acting as consent farms.

And my question to you is, do you believe that a stronger cybersecurity practices or clearer online disclosures would be sufficient and would be successful protections for consumers who obviously don't want to get the calls?

Ms. SAUNDERS. No, sir, I do not. I think that disclosures are, unfortunately, uniformly ineffective at protecting consumers. I think the problem needs to be that the rules need to be sufficiently clear. That the sellers who are using the telemarketers to make these calls and benefiting from these calls will be much more careful who—which callers they employ to make the calls. Because if they are not careful, they will be zinged with a TCPA class action.

And unfortunately, although I understand the frustration of the Chamber of Commerce with inappropriate class actions at the moment, the danger of class actions is also one of the prime ways that incentivizes sellers and callers to comply with the law.

So, we want the law to be clear, and we want the law to create those incentives to comply with it.

Senator HICKENLOOPER. Great. And, Mr. Rudolph, I would ask you just, and this is off—my staff will chide me later, but I am curious, it seems like there is a market there. This is so frustrating to people that for a relatively low monthly cost, lots of people, I think, would buy protection. In other words, you know, does generative AI have the potential to really effectively protect people from these kinds of scammers?

Mr. RUDOLPH. Going back to the question you just asked Margot, I want to really reinforce the robocall operator who can use tens of thousands or millions of numbers to contact you. If you think about what we can do on a device, it is very easy to block an individual number.

And while it is not actually officially signaling to that company, hey, I am taking my consent back. But by blocking that single number, you are preventing it from communicating with you. If we can require companies, when you grant consent to say, I am going to consent to that one number, right.

And if they, if a bot granted it or you accidentally unintentionally grant it, at least it was pinned to that one number, and you can control the caller originating from that one number and revoke that consent.

So, if we can just change how we—change our policies about when you have got an entity and how many numbers it tries to rotate through to evade these tools that we have in our hand. You don't need generative AI. You just need to make sure that you pin

robo-operations, robo-communications to using a number which matches their identity as they communicate that with you.

Senator HICKENLOOPER. Interesting. Yes, great. Ms. Brown, in your testimony, you described how businesses use automated messages to reach their customers. So, when these bad actors flood an individual with robocalls, people lose their trust in answering the phone. The best example, I always—I have my phone.

If I were to call you, comes—I, you know, it doesn't give my number, because whether for whatever right or wrong reason, sometimes rarely a constituent or a journalist might decide they want to get a hold of me frequently.

So, I have, you know, caller ID blocked. No one will take my call. So, I have to send someone a text before they will take my call because they think that that is always going to be a robocall. Whereas now the robo guys are so smart that they never use it anymore.

I keep trying to convince even my family that they should accept blocked numbers, but they don't. Anyway, Ms. Brown, how would you think small businesses would benefit if we could reduce the volume of illegal or unwanted calls?

Ms. BROWN. Thank you for the question. I think small businesses are victimized by fraudulent and illegal calls in much the same way that Ms. Saunders was talking about consumers at the front end.

So, I do think the steps Congress has taken to prevent caller ID spoofing, to try and clean up the ecosystem, and some of the work that Josh and the Industry Traceback Group do is really important to try to instill or protect confidence in the calling ecosystem so people do want to pick up their phone.

Small businesses both make calls and receive calls, and I think everyone is benefited if there can be trust that who is calling you is who it purports to be and not an overseas scammer, for example.

Senator HICKENLOOPER. Yes. The small businesses I know are irate because they have to take every call, and so they are the ones that are constantly distracted at certain times of the day when the robocalls are coming in waves. Anyway, thank you all for taking time out of your busy schedules to be here. I yield back to the Chair.

Senator LUJÁN. Thank you so much, Senator Hickenlooper. Senator Rosen, you are recognized. Senator Rosen, we cannot hear you right now.

STATEMENT OF HON. JACKY ROSEN, U.S. SENATOR FROM NEVADA

Senator ROSEN. Oh. I am off mute. Can you hear me now?

Senator LUJÁN. Yes, we can, Senator. The floor is yours.

Senator ROSEN. Oh, perfect. Thank you. All right. Technology is great when it works. And sometimes technology is not so great when it gives you a million phone calls all at once. So, there you go.

Thank you, everybody, for being here today. And I am going to just get right into it on scams, of course, in Nevada. Because according to the FTC, in 2022 alone, Nevada had the third highest rate of fraud and the fifth highest rate of identity theft.

So, every year, millions of Americans, of course, we know, including many of my constituents, fall victim to these predatory robocallers. The scammers, they create elaborate schemes through robocalls.

They say they are calling from Government agencies or other entities attempting really just to convince people to provide their personal identifiable information or that they are legitimate.

And so, for example, Nathan is one of my constituents in Las Vegas. He is a veteran of the Air Force, the U.S. Air Force. He wrote to my office sharing about a spam call he received from the Veterans Benefit Center. They asked him to refinance his mortgage. He said at one point he was receiving 10 to 15 calls a day from this Veterans Benefits Center.

But thankfully, Nathan recognized the scam. Many others don't. And veterans like him who serve our country should not be targeted with these kinds of calls. It is unacceptable. We have to do more to protect all of our constituents and combat these criminal schemes.

So, Ms. Saunders, what advice would you give to Nevadans, and of course, to everyone, particularly in more vulnerable communities perhaps, like seniors and veterans, who are targeted by scammers and are impacted at, I would say, disproportionate rates?

Ms. SAUNDERS. We have—thank you for the question. We have one clear piece of advice to give all American subscribers until this problem has been solved. If you receive a call from anybody, unless you are absolutely positive you know—that you know the person that has called you, do not give access to your bank account or any other money to that caller.

If you receive a call from somebody purporting to be from the Veterans Administration and you want to make sure that your benefits are protected, then hang up, look up the number for the Veterans Administration or whoever it is that supposedly called you and call them directly.

But don't give—and we don't do that even when we receive solicitations from a charity that we believe in. We never, ever give over the phone payment information.

Senator ROSEN. Yes, that is a great advice, and we are going to have to keep putting it out there over and over again, so people are continuing to hear this message.

But Mr. Bercu, can you tell us a little bit about how companies are working together to ensure that people are aware of these scams? We have to get it out there again over and over to keep reminding people.

Scams like the ones that Nathan called this about. What are you doing to make sure your advocacy is reaching every corner of every state, urban and rural?

Mr. BERCU. Thank you for the question. The industry is very active educating their consumers and their customers. I think they all have information out there. But one of the other things is all voice service providers virtually today have protections in place too. They—not only STIR/SHAKEN, which we talked about, but all the major wireless carriers have blocking and labeling. So, there is actually a lot of work to directly protect their customers as well.

Senator ROSEN. Thank you. And speaking about customers, and now you are trying to make your workforce who is creating all these ways to protect consumers, workforce and technology, it is so important.

You know, as a former computer programmer, I have a unique understanding of both the benefits and challenges that technology presents. So, in this case, we have this great technology, but it allows for more sophisticated use of robocalls and robotexts. And hopefully on the same side, we have presumably enough resources to combat that.

So, Ms. Brown, law enforcement officers, they really need access to training and technology to talk about the more advanced scams, especially as we see AI start to play a role in these scam robocalls.

And so, based on your experience, what kind of technology and training do you think, you know, Congress can support to bolster these resources as these scams just get more and more vicious, I would say?

Ms. BROWN. Thank you for the question, Senator. You know, I haven't given a lot of thought to specific training for State and local law enforcement, but it makes me think back to the importance of the Department of Justice and that collaborative work that the State Attorneys General are already doing with the Federal Communications Commission and otherwise.

So, my perception is there are a lot of resources that are available, some of which are similar to what Ms. Saunders was talking about in terms of consumer facing. But I would expect that the Department of Justice, the Federal Trade Commission, can sort of dig into those resources and help State and local law enforcement.

But I will say the State Attorneys General have been very active on these issues, and I think they are uniquely positioned to help State and local law enforcement identify some of these more exotic, shall we say, scam attempts that my panelists were discussing.

So, I think it is a great area to think about, particularly if you have constituents who it sounds like may not be getting that kind of information and support.

Senator ROSEN. No. Especially as we deal with deepfakes and other things. And of course, we are just going to keep working on building out our STEM workforce and keep working to protect the consumers.

Mr. Chairman, thank you for this hearing. I yield back.

Senator LUJÁN. Senator Rosen, thank you so very much. I am going to recognize myself for some additional questions.

Mr. Rudolph, everyone is talking about AI in some degree and using it differently. Just yesterday, the Chairwoman of the FCC, Jessica Rosenworcel, proposed a new notice of inquiry that would take a closer look at how artificial intelligence impacts illegal and unwanted robocalls and texts.

Specifically, this would investigate how the Commission might use AI technologies to protect consumers under the Telephone Consumer Protection Act.

Now, YouMail specializes in stopping scam calls and texts, so thank you for that. How do you envision using artificial intelligence to protect consumers from robocalls and robotexts?

Mr. RUDOLPH. It is a great question. Thank you. I would almost make a joke that we are going to enter a Black Mirror episode and each of us will be protected by our own bot that is going to screen every inbound communication, and eventually we have got just all these telemarketing bots talking to all these consumer protection bots, and the polar ice caps melting for all the GPU's having to run that.

But that joke aside, one of the suggestions I had earlier was to use a large language model to go through robocall mitigation database filings and toss out all the ones that are junk. So LLMs can be trained pretty quickly to synthesize that data and understand the intent, and you know, what that robocall mitigation filing would—if it is even feasible to, you know, implement the controls at those providers.

If you look at the Herculean lift of enforcement, the same thing could be done where if you wanted to investigate a communication service provider and you were given logs from that provider or given internal communications or memos that, you know, discuss the policies or controls those providers implemented, an LLM could quickly, you know, process that data and come to an understanding of what was actually happening.

So, I would say, you know, we are really facing a problem of scaling enforcement labor to, you know, make industry compliant here, and that is a great place to deploy that technology.

Senator LUJÁN. I very much appreciate that response. And also, bringing attention to the line of questioning from Senator Markey around how so many are thumbing their nose at a requirement with the mitigation plan and submitting blank documents, documents that are intended to be rude, or menus, or whatever nonsense is also being submitted.

It shows that it is not working. That there is a loophole somewhere that has been created. That there is no attention to the prosecution side, if you will, or the requirements from a mitigation plan.

And using tools to identify where those are is going to be critically important to ensure that we are able to enforce the mitigation plan when someone is found to be doing this illegal activity. I also appreciate, Ms. Saunders, your response to several colleagues' questions about what could be done in the area of looking at where traffic is being carried.

Data that I have seen suggests that not all carriers may be knowingly doing this, but it seems to be that there is a smaller number of carriers that carry more of the calls. That is revenue. If someone is told, you are carrying these calls that are stealing billions of dollars of American people, and they do it over and over, and then they submit a mitigation plan that is a blank document, it is the cost of doing business.

I want to equate this to financial institutions in America who are laundering money for cartels. And the cost of doing business is paying a fine. Some really smart people created these loopholes. Well intentioned, but there is loopholes and people have learned to take advantage of them.

What I would hope is that we can all agree to the ending of those loopholes. I remarked on this when this committee, the Commerce

Committee, had a hearing on a rail derailment. Well-intentioned legislation, well-intentioned testimony, people working together, but when the rulemaking gets started, then there is all kinds of stuff submitted into the Federal registry.

A lot of them are loopholes that get codified into the rules creating loopholes. Loopholes can lead to problems, as well-intentioned as they may be for whoever is submitting them. I hope that we can pull back the curtains on this to stop this.

With the transition to telecommunications being digital, it is not analog—Mr. Bercu, you can trace this stuff back wherever it goes. Mr. Rudolph, YouMail can stop it because you know where it is coming from. It is digital. You can follow it.

So, why is this so hard? If the traffic is in a small area, let's work with them, either to create the technical capabilities for the small carriers to have those capabilities, but for the whole industry also to self-police, to say you are the problem, you need to stop this.

Because if a small carrier has an agreement with one of the major carriers in America, and they are knowingly doing this, when I look at 12 percent of the traffic that is coming from some of the bigger names in the country, stop it. And I am hoping that we can get there. So, I appreciate that, that line of questioning and those responses.

I will close with this particular question toward you, Ms. Saunders, around AI generated scam calls. Now, we also know there is an urgent need to mitigate risks and establish responsible guardrails around AI.

And we have seen many examples around here. Scammers are cloning people, children's voices. We heard the testimony from our colleagues with veterans or active military whose voices are being spoofed all to steal financial resources from families.

Now, Ms. Saunders, yes or no, do current laws and regulations around robocalls cover these types of AI generated scam calls?

Ms. SAUNDERS. The Telephone Consumer Protection Act has been found to cover robot generated scam calls and telemarketing calls, yes.

Senator LUJÁN. Would anyone else respond to that? Ms. Brown.

Ms. BROWN. And I think the view is the TCPA is well suited to adapt to that sort of new technology. And I was just going to commend to you a report that the Chamber put out on a bipartisan basis.

They have an AI Commission, and I think there is a lot to learn from the NOI that the Chairwoman of the FCC has kicked off about how all of this will play out. But I do think the TCPA reaches some of these voice cloned concerns.

Senator LUJÁN. Mr. Bercu.

Mr. BERCU. I concur.

Senator LUJÁN. Mr. Rudolph.

Mr. RUDOLPH. I think anybody who is doing voice cloning to make calls doesn't care about the TCPA. So, they are committing criminal acts and TCPA, they would ignore it.

Senator LUJÁN. I appreciate that. Ms. Saunders.

Ms. SAUNDERS. The problem is that the TCPA is not effective against scam calls. It is effective against telemarketing calls, but it is not effective against scam calls.

And the only way to stop the scam calls is to deal with the providers who are providing access to the communications network for those scammers. And we don't have a law like the TCPA that applies to the voice service providers, nor are we necessarily recommending that there be one.

So, Ms. Brown, you don't need to worry. But what we are recommending is that the FCC be encouraged or enabled, whichever is appropriate, to act much more quickly against those problem voice service providers that are inserting the bad callers—the bad calls into the network.

Senator LUJÁN. I appreciate that. I am concerned that it does not. I think it handles calls in one format, but I am concerned in this other space as well. And look, understandably, when it was written, this technology did not exist to the degree that it exists today.

One of the faults with many pieces of legislation is when it is thought up, and by the time it passes, technology has accelerated, you know, a generation or two ahead of what the well intentioned proposal was as well. But that is where the rulemaking bodies are supposed to keep up with what?s happening here.

And also, industry. When something bad is happening that cannot be self-policed, ask for help. How do we stop the nonsense? $39 billion being stolen in a year. That should rise to any prosecutor's attention. If the Department of Justice is not going to do this, then how do we find other partners that are willing to?

How do you work with the FCC such that if a fine is put forth and then there is not a prosecution, then what? And I will also say that if there is a small number of entities that are responsible for the majority of traffic, and they have been warned about it, and it continues, something needs to be done there because, again, it is the cost of business, it is revenue.

And if you can make $100 million and pay a $10 million fine, some people are willing to take that deal. And it is just not right, because who is at the end of this?

Ms. Saunders, do you have some thoughts on what Congress could be doing to protect Americans from AI generated scam calls and robotexts? And I will ask the rest of the panel to address that as well, and then we will close out the hearing.

Ms. SAUNDERS. I think that I have articulated it already. I think that the FCC is uniquely poised to be the prime policeman on the block regarding the voice service providers.

What I want to explain is that the reason the terminating providers who are all in agreement that these calls should not be processed, the reason they cannot stop them, they can't block them is because the scam calls are mixed with the legal calls, so it is impossible for them, for the terminating providers to identify them.

Senator LUJÁN. But Ms. Saunders, if I may interject. I am a former public utility commissioner.

So, while the calls may be mixed in, they can tell where the calls are originating, and then they also know if the investigators are doing their job, you are burying this traffic from, you know, Mr. John in whatever location, whether it is in the United States or in other part of the world.

Why are you carrying all this traffic where it appears that 90 percent of it is bad stuff as well?

Ms. SAUNDERS. Well, I am not sure that the terminating providers can always identify exactly where the calls are originating. They see—all they see is that the calls are coming from the upstream intermediate provider.

And so, the key is to somehow encourage all of the providers in the network to only carry legal calls or else it will cost them. And we provided in our testimony in the last section an example of how the legal callers can use their power in the marketplace to encourage their voice service providers to only carry their calls and thus isolate the illegal calls, which we think would enable the terminating providers to better identify them and block them.

Senator LUJÁN. Appreciate that. I am going to go to Mr. Bercu and I will come back to Ms. Brown. How are you able to follow the calls then, if—how do you know where they are coming from?

Mr. BERCU. So that is what our trace back process accomplishes. Because as Ms. Saunders said, often all a provider knows is who they got from, and our process does that. We just go hop, by hop, by hop. Who did you get the call from? Who did you get the call from? Until we find out exactly where it came from.

Senator LUJÁN. That is proprietary technology?

Mr. BERCU. It is our—we have a portal that all the providers log into and they do it in the portal. We have automation. If someone doesn't respond, they get shamed for not responding in time. They get warnings. The provider downstream gets shamed if they continue to take traffic from robocallers, and all this information is made available to the enforce.

Senator LUJÁN. Repeat that last part, Mr. Bercu. What happens if they take calls from folks that are responsible for robocalls or where they are known to come from?

Mr. BERCU. So, the way our—we designed our system, if providers upstream is the originator of the illegal robocalls we trace, the downstream provider knows that. They are put on notice that their upstream partner keeps giving them bad traffic. And again, all this information makes its way to the enforcement community.

Senator LUJÁN. So, based on that common carrier or whatever the agreement is between one carrier and another, your technology allows for those two entities to know that there is a problem with these fraudulent calls?

Mr. BERCU. Yes, absolutely. And we see, to Ms. Saunders' point, we see all the time carriers taking action. We see them fire their wholesale providers. The challenge is because it is an interconnected network, it is—we have—you know, I have heard from providers that said, OK, we got too much bad traffic from these providers and fired all of them. The calls still hit their network. It just was another hop or two that were added in between.

Senator LUJÁN. And Mr. Rudolph, with that being said, where traffic can be identified, YouMail can stop this from hitting a consumer, dramatically reduce, stop to protect people. Is YouMail also—is YouMail able to identify where it originates?

Mr. RUDOLPH. So as calls reach the consumer, right, we have got two very amazing ways to understand which communication pro-

viders were the originators or the gateway providers for those traced back.

If the call was not a test, using STIR/SHAKEN. And if it has a STIR/SHAKEN packet, basically with it, it is clear as day that these are the seven voice providers that are currently harboring that account that is making the loan calls, you know, as a—identifying as a VA or interrupting other centers—so, you know, if you ask me right now, you know, who are the providers who have these calls. We can look at STIR/SHAKEN and get a lot of that.

And then the ones we don't see the STIR/SHAKEN yet carry, the trace back process can illuminate that. What we are missing is the signal to industry, those specific calls are bad, knock those off, right.

The FCC has done that twice auto warranty calls and student loan calls. And now providers have a clear signal from the FCC, don't carry those. And what happens is, you know, trace back runs, or YouMail will directly contact a provider and say, hey, this call looks like it is committing fraud. Maybe you should knock it off. That account gets kicked off that provider and goes and finds a new home.

So, unless the entire ecosystem is notified, don't take this account on, someone is going to look at that new sign up and think, oh, that is revenue. I am going to take that new account on and kind of look the other way about whatever that account might be communicating.

Senator LUJÁN. What process is required to ensure the whole ecosystem knows about the one fraudulent call and the communication to the one company?

Mr. RUDOLPH. Can you say that again? Sorry.

Senator LUJÁN. What would be required to share that information that YouMail may be having with one carrier, or anyone maybe having with one carrier to say this called fraudulent, you should kick it—you should probably kick it off, so that it goes across the entire ecosystem.

Mr. RUDOLPH. So, we work regularly, every other week, with the FCC and we go through the prioritized calls that are on that hotlist of investigations. And we will provide that and those discussions about, hey, these are the providers that we are seeing that are carrying those calls presently.

Senator LUJÁN. Appreciate that. Ms. Brown.

Ms. BROWN. Do you want me to address AI, which I think is what you started with a little while ago?

Senator LUJÁN. In this space with AI, also given the responses associated with being able to narrow where there may be a fraudulent call with the carrier, is there something that could be done to share it within the ecosystem?

Is it something that the companies could adopt to share—and through that process? Is it something the FCC should be doing with existing authorities that this is just—this is what is going to happen every time that we see this, and it is proven that there is a fraudulent call. If you could touch in those three areas.

Ms. BROWN. Sure. I will do my best. Thank you, Senator. I am actually sort of optimistic and I think the Chamber would be that

AI will sort of juice up what the ITG and YouMail are already doing.

And I think, so that gives me optimism that those anti-fraud efforts and the ability to detect bad traffic is going to get better over time. And I think at a recent workshop the FCC held back in September with the National Science Foundation, they heard about that as well.

So that is kind of my response on the AI piece of this, or the AI approach. It sounded to me from what Mr. Rudolph and Mr. Bercu were saying, that the FCC is intimately involved in getting this information, I think it is maybe a question of scale, to address the issue that you were raising.

Again, maybe AI, maybe some additional technology can help there. I don't have visibility, whether it is a manual process or if it is really phone calls with the Enforcement Bureau, which it probably is, which makes me sad for the Enforcement Bureau staff.

But again, I think there is a reason to be sort of cautiously optimistic that maybe they haven't cracked the code, but there can be additional steps. And then if the FCC can be encouraged to do more of what it did in the auto warranty space and student loan space.

I think the report the FCC gave to Congress under the TRACED Act had some really remarkable data in it about the decrease in calls after they took those actions. So, I am sort of cautiously optimistic about that process working.

I don't see right now a need for new regulatory authorities to be given because it feels like that process is actually working fairly well, even if it is a little opaque. Sorry for that long answer.

Senator LUJÁN. Oh, I appreciate the response very much. Thank you all for being here today, and to all my colleagues for attending today.

This is important testimony and there is, as you all know, an immense interest with the American people in this space and immense frustration with the American people about what happens to them every minute of every day as well.

And I want to commend you for helping to solve this challenge, for helping consumers one at a time, for providing support to help the process, understand where and what is happening every day, looking at the ability of rules that exist, exploring those that may be needed to make things better in this space.

So, thank you so very much. And remaining challenge and a very complex issue. With that, I will close the hearing. And should members have additional questions for the witnesses for the record, I ask that they submit them to the Committee within two weeks, and witnesses will have an additional two weeks to respond. Thank you, everybody.

[Whereupon, at 11:51 a.m., the hearing was adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO MARGOT FREEMAN SAUNDERS

Innovation and Adoption

Robocallers are taking advantage of technological innovations to flood our phones with calls and texts. It seems to me that other forms of technological innovation—like machine learning and generative artificial intelligence– hold the most promise for combatting this flood of illegal robocalls.

Question 1. How can Congress and the FCC encourage telecommunications companies to embrace innovative technologies and use new tools responsibly to protect consumers from robocalls?

Answer. By creating incentives for telecommunications companies to protect consumers—either with the "carrot or the stick."

The carrot might involve the FCC establishing a system of public rewards, such as positive ratings for trustworthiness for those companies who have no history of transmitting illegal calls in the previous 12 months. Legal robocallers (such as banks, health care providers, and pharmacies sending desired alerts to consumers) could use this information to choose their originating voice service providers for their calls.

The stick should be clear and immediate consequences which are costly to the providers who persist after notice in transmitting illegal calls. These must be meaningful and not merely "the cost of doing business."

AI and Deepfake Calls

I recently heard about an alarming situation in my state. A family in Pierce County, Washington received a deepfake call, where a scammer used AI to spoof their daughter's voice saying that she had been in a car accident and that a man was threatening to harm her unless they wire $10,000. No family should have to face this.

Question 1. How can Congress empower consumers, regulators, and law enforcement to stay ahead of the increasingly sophisticated technologies scammers use?

Answer. As explained more fully in response to the question "How can Congress best ensure that the FCC uses its enforcement authority effectively?" We believe that in addition to close monitoring of the voice service providers who repeatedly transmit these dangerous scams after notice, and punishment Congress should authorize the FCC to suspend the ability of complicit voice service providers to transmit calls into the network. This is described more fully in Section II of NCLC's testimony. In addition, Congress should require the Department of Justice to pursue and prosecute the perpetrators of these scams.

Heightened Enforcement

Congress passed the TRACED Act in 2019 to enhance the FCC's enforcement authority and increase penalties for illegal robocallers. Since then, scam robocalls have dropped 50 percent, but they remain a serious problem.

It's true that, on paper, there appears to have been a 50 percent reduction in scam robocalls. However, this is a result of reclassification of calls that were previously classified as scam calls, and are now classified as telemarketing calls. Please see the illustration of this in the table on page 4 of *NCLC's testimony to this Committee on October 24, 2023.*[1]

As illustrated in that table, when the scam calls and telemarketing calls are combined, these calls peaked at more than 3 billion calls per month in September 2019. There were similar levels of these combined calls in March 2021. In September

[1] *https://www.commerce.senate.gov/services/files/92F8E35B-F203-49FD-BA53-E9F8816A19F2*

2023, the combined number of these unwanted calls was at 2 billion a month, but as recently as March 2023, the numbers had been as high as 2.5 billion.

Additionally, the FTC reports that while the *reports* of scams were lower in 2022 than the previous year, the *amount of losses* reported increased substantially to $8.8 billion.[2]

Last year, scam robocalls cost American consumers a total of $39 billion. This includes 1.1 million people in the State of Washington. Clearly, we can do more to crack down on these scams.

Question 1. The FCC already has civil enforcement authority over robocalls. How can Congress best ensure that the FCC uses its enforcement authority effectively?

Answer. As described in section II of NCLC's testimony, we recommend that the FCC establish a system to suspend complicit voice service providers after one verified notice that the provider has been transmitting illegal calls. In a nutshell, we are proposing that the FCC should be authorized to quickly remove the ability of complicit voice service providers to transmit calls into the U.S. telephone network. This can be accomplished by suspending these repeated offenders from the Robocall Mitigation Database. Below is an excerpt from the testimony that summarizes this recommendation.

> We believe that the FCC should be empowered to use immediate—but temporary—suspension[3] from its Robocall Mitigation Database as a mechanism to protect telephone subscribers from receiving illegal calls, pending investigations and due process determinations. This would prioritize protecting U.S. telephone subscribers from criminal scam calls over providing originating and gateway providers access to the U.S. telephone network.[4] Once a provider has been notified by any of the government enforcement agencies, or their service providers, that it has been found to be transmitting illegal calls, such notification should serve as legal notice that the next time it is determined to be transmitting illegal calls, it will be suspended from the RMD. These suspensions should be temporary and short-lived, but immediate, pending a due process review. The due process review would determine whether this latest finding that the provider was transmitting illegal calls was a mistake that will not be repeated, or whether it justifies permanent removal from the RMD.

Question 2. Are there additional tools that Congress should empower the FCC with to combat illegal robocalls?

Answer. In our 2022 Report "Scam Robocalls: Telecom Providers Profit,"[5] we also suggested that the FCC employ a more robust licensing system to police voice service providers that have a history of non-compliance with the FCC's rules. This would establish a simple method for the FCC to govern recalcitrant providers.

The VoIP providers that process the illegal robocalls are generally small, often simply one or two individuals with minimal investment or technical expertise who have set up a service in their home or other temporary quarters and offer services through online advertisements. *See* FCC 2021 Report to Congress, *supra* note 15, at 12 ("The Commission's experience tracing back the origins of unlawful call traffic indicates that a disproportionately large number of calls originate from Voice over Internet Protocol (VoIP) providers, particularly non-interconnected VoIP providers.

---

[2] *https://www.ftc.gov/business-guidance/blog/2023/02/ftc-crunches-2022-numbers-see-where-scammers-continue-crunch-consumers.* Regarding scams conducted over phone or text specifically, the FTC noted $830 million in consumer-reported scam losses in 2021 as compared with $1.13 billion in 2022; in the first three quarters of 2023 alone the FTC has already seen $922 million in reported consumer losses from text and phone call scams. *https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts*

[3] Suspension should result in legally effective removal from the RMD. This can be accomplished via a prominent notation that the provider's status is suspended. *See, e.g.,* In re Advanced Methods to Target and Eliminate Unlawful Robocalls *et al.,* Comments of ZipDX L.L.C., Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17–59, and Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17–97, at ¶64 (filed Dec. 7, 2021), available at *https://www.fcc.gov/ecfs/document/12080110629539/1* ("We would note that 'delisting' should not actually constitute complete removal from the database; rather, an entry should be retained so that it is clear to all others that the problematic provider has been explicitly designated as such. This will ensure that if (when) the problematic provider attempts to shift their traffic to a new downstream, that downstream will become aware of the situation before enabling the traffic.").

[4] Most, if not all, of the offending voice service providers are VoIP (Voice over Internet Protocol) services. VoIP is a technology that accesses the telephone network through the internet, and is commonly used by many large telecommunications providers in place of traditional landlines to provide service to residential and business customers. Often, the telephone service is paired with Internet access and cable television service.

[5] *https://www.nclc.org/resources/scam-robocalls-telecom-providers-profit/* at 32.

Moreover, the Industry Traceback Group has found that high-volume, rapid-fire calling is a cost-effective way to find susceptible targets, although it does not collect data about which robocall originators are VoIP providers.").

Just as states require testing and licenses before people are permitted to drive on public roads to protect the public from dangerous drivers, the FCC should require licenses, that must be renewed on a regular basis for all voice service providers. Repeated notices of non-compliance should be grounds for revoking a provider's license to transmit calls into the system.

Strengthening Rules

I understand that you have previously called for the FCC to strengthen its rules to address the marked rise in unwanted robocalls. Our robocall enforcement efforts cannot be successful without strong robocall rules in place.

Question 1. What can be done to modernize robocall rules?

Answer. The FCC has recently announced its intention to adopt a strong regulation governing consent for telemarketing rules.[6] Final approval and enforcement of this amended regulation "will prohibit abuse of consumer consent by" lead generator websites.

Similar actions should be taken to modernize the rules governing calls to lines registered on the Do Not Call Registry, such as—

a. Limiting the time for which a consumer's consent to be called should be considered (changing it from no time limit to 30 days), and clarify that once the consumer says "stop calling me" or anything similar that indicates a desire for the caller to stop calling.

b. Unequivocally stating that once a consumer revokes consent to a telemarketer calling on behalf of a seller, the seller is responsible for ensuring that the telemarketer reports that revocation immediately to the seller, who in turn must immediately inform any other telemarketers making calls on that seller's behalf that calls to that consumer must stop.

c. Establishing that a caller that fails to use the Reassigned Number Database to check that it is calling the person who provided consent for the call, cannot escape liability for placing that call under any of the Commission's rules.

d. Restoring meaningful restrictions on calls and texts sent using an automated telephone dialing system.

Question 2. What additional actions can the FCC take to stop illegal calls and texts?

Answer. As is described in *NCLC's testimony,* one of the primary reasons that terminating providers are unable to block scam robocalls is because complicit voice service providers mix the illegal calls with the calls from "legal callers." Legal callers are sending robocalls that consumers want and for which they have consented, such as medical appointment reminders, fraud alerts, and prescription refills.

The difficulties with reliably completing these wanted calls are apparently increasing. Legal calls are mixed with a torrent of illegal calls at shared originating and intermediating providers, causing legal calls to be tainted by illegal calls in the same call path. The result is that legal calls end up mislabeled or blocked by downstream providers seeking to protect subscribers from illegal calls.

We have proposed that the Commission facilitate leveraging the considerable marketplace power of these legal callers to assist in the efforts to eliminate dangerous and unwanted calls—scam and illegal telemarketing calls. If legal callers are armed with the information about how to avoid using the providers that are processing illegal calls, this would prevent the legal calls from being used to mask the illegal calls.

The sheer economic power of legal callers may be sufficient to force voice providers to stop transmitting illegal calls. A market-based approach like this would a) provide strong financial incentives to originating and intermediate providers to avoid transmitting illegal calls; b) facilitate the transmission of legal calls through call paths that would eliminate the likelihood that the calls would be labeled improperly or blocked by downstream or terminating providers; and c) supplement the other mechanisms created by the Commission intended to address illegal calls. *The foundation of a market-based approach is providing legal callers with the information that they need to keep their calls separate from illegal calls.* As explained in the testimony, this information is already available from private analytics-based platforms. The Commission need only lead the way.

---

[6] *https://docs.fcc.gov/public/attachments/DOC-398661A1.pdf*

STIR/SHAKEN Call Authentication

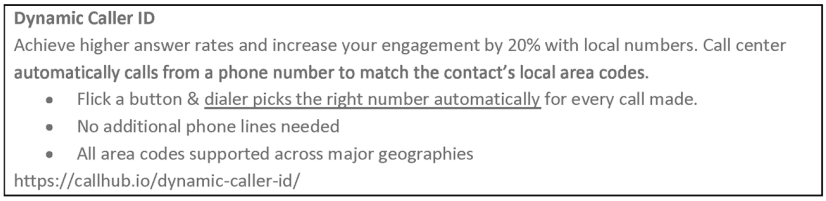
In 2019, Congress passed the TRACED Act to require phone carriers to adopt STIR/SHAKEN call authentication standards. These standards create a digital signature that identifies the calling party and allows phone carriers to verify calls, while weeding out calls from illegitimate sources.

While these standards have helped in the important fight against robocalls, they have certain limitations. For example, they will not work for all telephone calls. We have seen illegal robocallers change tactics, moving away from using fake phone numbers to buying real phone numbers that trick spam-blocking software into allowing the calls through.

Question 1. What is your assessment of STIR/SHAKEN?

Answer. A primary goal of the TRACED Act[7] was to facilitate the identification of callers so that illegal and unwanted calls can be blocked by either subscribers or downstream providers.[8] However, the temporary rental of telephone numbers by bad actor voice service providers who advertise to callers the availability of Dynamic Caller ID, or Direct Inward Dialing numbers (DIDs), completely undermines the effectiveness of even the most robustly enforced caller ID authentication methodologies. The identity and the real telephone number of the caller is functionally obscured when a caller uses a disposable number that is local to the called party.

Some telephone providers routinely rent telephone numbers or make "dynamic caller ID" available to callers to facilitate deliberate evasion of the FCC's requirements for callers to identify themselves properly. For example, one telephone provider—CallHub—advertises that its service can be deliberately manipulated to make calls appear to be from local numbers[9]—which they are clearly not, or this service would not be necessary:



Some VoIP providers openly advertise the use and the effectiveness of these services, emphasizing that even calls from international numbers will appear that they are from a local business:

> Is it possible to change an outgoing caller ID? Yes, *with the VoIP feature, dynamic caller ID, your business can display a local or toll free number instead of a long-distance or international number.*[10]

The use of rented telephone numbers just for the purpose of matching the area code to which the calls are directed, rather than matching the actual geographic source of the call, conflicts with several specific requirements imposed by Congress and the Commission designed to give called parties reliable and truthful information about the identity of callers. A fraudulent or scam caller that rents telephone numbers on a temporary basis for the purpose of displaying a deceptive caller ID violates 47 U.S.C.§ 227(e)(1)'s prohibition of misleading caller ID. When the calls are telemarketing calls, the use of rented numbers or dynamic caller ID also conflicts with 47 CFR § 64.1601(e), which requires telemarketers to transmit specific caller identification information regarding the seller or the telemarketer. This regulation serves no purpose if callers are permitted to rent telephone numbers that provide no information about the caller or seller whose product is subject to the call. This is illustrated by the advertisement on another website.

---

[7] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, Pub. L. No. 116–105, § 4(b), 133 Stat. 3274 (2019) [hereinafter "TRACED Act"].

[8] TRACED Act at § 7(b)(2).

[9] *https://callhub.io/dynamic-caller-id/* (emphasis added) (last visited June 5, 2023).

[10] *https://www.unitedworldtelecom.com/learn/what-is-a-dynamic-caller-id-for-voip/* (emphasis added) (last visited June 5, 2023).

Why Does Your Business Need a Dynamic Caller ID?
The main reason why businesses use or should consider using a dynamic caller ID is so they can increase the chances of calls being answered. Individuals are less likely to answer calls from "unknown" numbers or numbers they do not recognize as toll free or local.

With a customizable caller ID, you can choose which number to display. When calling specific local areas, you can display that area's local number or toll free number. In fact, this even increases the chances of receiving a call back because callers will be dialing a local or toll free number which does not incur high calling rates.

Contact centers, customer service teams, as well as sales and marketing teams can use this feature to reach more customers locally and internationally. The logic here is the customer will assume your business is local and will feel more comfortable doing business with you due to your location.

Callers use bulk rented numbers is to deceive the called party into believing the caller is local, to mask the caller's actual identity, and to avoid the "scam likely" analytics of terminating providers.

Applying the STIR/SHAKEN authentication closes one door to falsifying caller-IDs, while leaving another one wide open. While considerable progress on the spoofing front has been made,[11] the problem continues. Quoting from previous findings, the Commission has recently noted that it has received—"hundreds of comments from consumers . . . stating that they no longer answer their phone when it rings," and has concluded that "[i]t is obvious that the volume of unwanted calls is reducing the value of telephony to anyone who makes or receives calls. . . . Unwanted robocalls, for example, often are either delivered with inaccurate caller ID information deliberately designed to trick the called party into answering the telephone. . ."[12]

Even the most perfect and robust use of STIR/SHAKEN will not stop callers from hiding their real name, location, and telephone number unless the use of rented DIDs is also eliminated. Failing to eliminate the use of rented numbers while requiring strict compliance with STIR/SHAKEN requirements is like adding a deadbolt to a closed door to keep the flies out, while leaving a window wide open.

Question 2. If STIR/SHAKEN is not enough, what more do we need to effectively curb illegal robocalls?

Answer. Voice service providers should be prohibited from renting outbound numbers for short-term temporary use, with specific exceptions permitted for appropriate business reasons.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BEN RAY LUJÁN TO MARGOT FREEMAN SAUNDERS

Facebook v. Duguid

Question 1. How will the Supreme Court's ruling in *Facebook, Inc. v. Duguid et al.,* impact litigation brought under the TCPA?

Answer. It has effectively eliminated all challenges to automated live calls and non-telemarketing texts, as well as telemarketing texts made to cell phones that are used for business purposes.

Question 2. In *Duguid,* the Supreme Court reasoned that the narrow statutory design of the definition of the technology that constitutes an automatic telephone dialing system ("autodialer") under the TCPA was deliberately designed to address "nuanced problems." If Congress were to expand and redefine the technology that constitutes an autodialer, what would the definition need to include to protect Americans from unwanted robocalls?

Answer. We suggest that the new definition for ATDS should be along the following lines:

"(1) The term "automatic telephone dialing system" means equipment that—

---

[11] *See e.g.,* FCC Closes Gap in Caller ID Authentication Regime (Mar. 17, 2023), *https://www.fcc.gov/document/fcc-closes-gap-caller-id-authentication-regime-0.*

[12] *In re* Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, ACA International, the Edison Electric Institute, the Cargo Airline Association, and the American Association of Healthcare Administrative Management Petition for Partial Reconsideration, Enterprise Communications Advocacy Coalition Petition for Reconsideration, Order on Reconsideration and Declaratory Ruling, CG Docket No. 02–278 at ¶33 (Dec. 22, 2022), *https://www.fcc.gov/ecfs/search/search-filings/filing/12271082616240.*

a. produces a set of telephone numbers to be called; and

b. dials the set of numbers using automation or partial automation.

(2) "produce" means to select, create, or recreate from a file, database, or other form of data storage, or to generate using number generators;

(3) "automatic telephone dialing system" does not include any application that comes preinstalled with the operating system of any consumer device."

Question 3. The National Consumer Law Center (NCLC) submitted an amicus brief to the Supreme Court in support of Duguid. The NCLC cautioned that "unwanted automated calls significantly invade the privacy of Americans, diminish the usefulness of cellular telephones, and threaten public safety." How does narrowing the TCPA undermine commerce and telecommunications in America? Specifically, how will the post-*Duguid* narrowing of the TCPA impact small businesses and low-income Americans?

Answer. Narrowing the definition has led to the proliferation of unwanted texts to cell phones, as well as more unwanted and unconsented-to automated live calls. The only protection against unconsented-to texts or automated calls (that do not include a prerecorded voice) to cell phones apply only if the message involves telemarketing, and only if the cell phone is used for residential purposes, and only if the cell phone telephone number is registered on the Do-Not-Call Registry. However, there are no protections against unwanted and unconsented-to texts or automated live calls for cell phones used for business purposes.

Question 4. The Supreme Court reasoned that a more expansive definition of an autodialer could expand the TCPA's liability provisions and affect ordinary cell phone owners in the course of common place usage. If the TCPA definition of an autodialer were to be expanded, how would that impact American cell phone owners?

Answer. It would dramatically cut down on the number of unconsented-to texts received by American cell phone owners. Additionally, the definition that we propose ensures that calls from consumers using their cell phones would not be inadvertently included.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JOHN HICKENLOOPER TO MARGOT FREEMAN SAUNDERS

Traceback Transparency

The Industry Traceback Group (ITG) conducts thousands of tracebacks to find the source of illegal traffic by tracing each provider along the call path who helped facilitate the illegal call. However, raw traceback information is only released privately or on a case-by-case basis to law enforcement.

Question. Should raw traceback information be made available to the public? What are the benefits, and potential risks, of traceback information becoming public?

Answer. We have advocated that traceback information regarding the originating and/or gateway provider, as well as the first intermediate provider, be made available to the public. This would enable the world to see which providers are responsible for transmitting illegal calls.

The telephone industry argues that revealing the tracebacks publicly will reveal confidential contractual arrangements involving least-cost routing between providers. The issue is which is more important—protecting these contractual secrets or protecting consumers from the scam calls that these providers are transmitting, even after repeated notices that they are responsible for these calls.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. PETER WELCH TO MARGOT FREEMAN SAUNDERS

Question 1. What challenges does the FCC face in reducing unwanted and illegal calls?

Answer. We think the most significant challenges that the FCC faces are:

First, the lack of clear authority and instruction from Congress to move quickly to shut down the providers who are repeatedly transmitting the illegal calls and

texts into the U.S. telecommunications system, as I described in detail in Section II of the *testimony to this Committee.*[13]

And second, insufficient funding to hire more staff to deal with the problem.

Question 2. The STIR and the SHAKEN framework is slated to be fully implemented by December 31, 2023. How can STIR/SHAKEN protocols be improved before they are fully implemented?

Answer. Please see the response provided to the question on STIR/SHAKEN from Chairwoman Cantwell, above.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TED CRUZ TO MARGOT FREEMAN SAUNDERS

Cy Pres Awards

When class action award funds are unable to be awarded to class members directly, or are unclaimed by class members, courts will use *cy pres* awards and distribute those funds to nonprofit entities instead of class members. The National Consumer Law Center (NCLC) actively solicits and receives such *cy pres* awards in Telephone Consumer Protection Act (TCPA) class actions.[1] Given that most class actions result in class member claims rates of *well less* than 10 percent, these residual distributions could be substantial.[2]

Question 1. How much revenue has NCLC received from *cy pres* awards each year for the past five years (CY2019 to CY2023)?

Answer. NCLC has been determined to be an appropriate recipient of *cy pres* awards by many courts across the Nation over the past 5 years. From CY2019 through CY2023 (through 12/1/2023) the amount of *cy pres* awards we have received is:

2019—$2,471,054.58
2020—$5,139,211.54
2021—$1,892,346.33
2022—$4,329,220.91
2023—$3,645,940.60

Question 2. What percentage of NCLC's *cy pres* revenue was generated from TCPA class actions each year for the past five years (CY2019 to CY2023)?

Answer. Most class action cases involve multiple causes of action. The percentage of total *cy pres* revenue generated from class actions that involved a TCPA claim as one of the causes of actions (that we have been able to identify) each year for the past five years is: 2019—30 percent; 2020—7 percent; 2021—38 percent; 2022—44 percent; 2023—48 percent.

Question 3. What limitations exist on the use of any revenue NCLC receives from TCPA *cy pres* awards?

Answer. Limitations on the use of TCPA *cy pres* awards are determined by the court that enters the order approving the award in each case. NCLC abides by all court orders.

Question 4. Are these funds resulting from *cy pres* awards comingled with any other revenue streams?

Answer. *Cy pres* awards that are purpose-restricted by a court are not comingled with any other revenue streams.

---

[13] *https://www.commerce.senate.gov/services/files/92F8E35B-F203-49FD-BA53-E9F8816A19F2*

[1] For example, NCLC lists "ways to give" on its website, including through *cy pres* nominations (*NCLC—Cy Pres*). It features *cy pres* stories and successful nominations in its newsletter. "*NCLC—Consumer Impact Spring 2021"* lists over 60 successful nominators and "*NCLC—Consumer Impact Spring 2019*" mentions a TCPA *cy pres* award (though not the amount). NCLC is reported to be the designated beneficiary of TCPA class actions, including *Krakauer v. Dish Network* at $1,708,810. Other TCPA suits designate NCLC to receive any residual funds not distributed to class members and the final amounts NCLC receives are unclear.

[2] Fed. Trade Comm'n, *Consumers and Class Actions: A retrospective and Analysis of Settlement Campaigns,* at 11 (Sept. 2019), *https://perma.cc/CM66-ZVCX;* Consumer Financial Protection Bureau, *Arbitration Study,* at Section 8, page 30 (reporting a weighted average claims rate" in class actions of just 4 percent), *https://perma.cc/8AX5-AYWN; see also Mayer Brown Study* at 7 & n.20 (in the handful of cases where statistics were available, and excluding one outlier case involving individual claims worth, on average, over $2.5 million, the claims rates were miniscule: 0.000006 percent, 0.33 percent, 1.5 percent, 9.66 percent, and 12 percent), *https://www.mayerbrown.com/files/uploads/Documents/PDFs/2013/December/DoClassActionsBenefitClassMembers.pdf.*

Question 5. How has NCLC used revenue from TCPA *cy pres* awards each year for the past five years (CY2019 to CY2023)?

Answer. In the past five years, NCLC has used revenue from TCPA *cy pres* awards to support work to protect consumers from unwanted and dangerous calls and texts and, where permissible under the court order, to support our research, training, and advocacy on behalf of low-income and other vulnerable consumers who have been or are at risk of being abused, deceived, discriminated against, or denied access to justice.

This work includes advocacy before the Federal Communications Commission (FCC) to stop unwanted and dangerous calls and texts, especially those that defraud consumers. In the past several years our work has included the filing of *44 comments and ex parte notices* to encourage more effective protections against invasive and dangerous calls. These filings have been in multiple dockets, including but not limited to the TCPA docket.

During this time our advocacy has been instrumental in improved consumer protections against these calls and texts, including:

a. The *FCC's determination* that ringless voice-mail messages are covered under the TCPA, which protects consumer and business cell phone subscribers from having their voice mailboxes filled with unwanted robocalls.

b. The *FCC's new limits on non-telemarketing prerecorded calls* to residential lines that were previously exempt from any restrictions. These calls are now limited to only 3 unconsented-to calls a month; this particularly protects consumers from overzealous debt collection efforts.

c. Our *2022 Scam Call report* on the causes and consequences of the 1 billion plus monthly scam calls has received widespread attention, reinforcing the efforts we launched with our national partners to urge the FCC to apply more aggressive measures to block these calls. Some of the proposals that the FCC is now considering appear to be in response to many of the issues we raised. We have also done considerable *work to assist consumers* in recovering money stolen through scam robocalls and texts.

d. NCLC is also leading an effort to drastically reduce illegal telemarketing calls (currently over 1.2 billion monthly) by prohibiting lead generators and data brokers from trafficking in the consents that are used to justify these calls. The Federal Trade Commission has issued guidance supporting this position, and along with a dozen national partners we have filed *comprehensive comments* and held numerous meetings with the FCC, urging it to do the same. *Twenty-eight state attorneys general* have supported these efforts, as has *USTelecom, the trade association* for the telephone providers. Indeed, the FCC has *recently announced its intention* to implement many of our recommendations in an amended regulation that the FCC says will "prohibit abuse of consumer consent by" lead generator websites.

e. NCLC has testified before Congress on ways to limit dangerous and unwanted robocall multiple times, including before this Committee in 2016, 2018 and 2019, and before the House Subcommittee on Communications and Technology in 2019.

f. NCLC writes and publishes a treatise titled *Federal Deception Law,* which includes two chapters providing a detailed analysis of all significant TCPA decisions and FCC actions, updated regularly (most recently in early 2023).

g. NCLC provides multiple Continuing Legal Education (CLE)-eligible trainings to consumer lawyers each year on the intricacies of the TCPA and related regulations.

Our broader efforts to protect low-income consumers are documented on *www.nclc.org,* which includes thousands of pages of detailed reports, testimony, advocacy, and resources directed at achieving economic justice for people with low incomes. NCLC's research and advocacy helps protect every consumer who buys a house or a car, uses a credit card, opens a banking account, makes a payment, incurs a medical debt, obtains utility services, or takes out a student loan from unfair, abusive, and deceptive financial practices.

NCLC's work includes publishing comprehensive legal treatises, widely considered to be the Nation's leading source of consumer law analysis, which are often cited in judicial opinions by courts across the country, including the U.S. Supreme Court. The 21-volume Consumer Law Practice Series and the NCLC Digital Library are used over 35,000 times each month by attorneys working to detect and remedy illegal robocalls, obtain redress from scams and fraud, challenge arbitration clauses, clear credit reporting errors, protect consumers from abusive debt collection prac-

tices, use bankruptcy to obtain a fresh financial start, stop threatened foreclosures, and much more.

NCLC's expertise is often called upon by public officials, courts, attorneys, and other advocates focused on addressing the needs of low-income and other disadvantaged consumers. NCLC provides comprehensive continuing legal education on consumer law. More than 10,000 consumer attorneys, advocates, and service providers attend an NCLC conference or receive training from an NCLC attorney through a webinar or in-person training session each year.

Question 6. How does NCLC advocate and/or engage in activities designed to encourage and/or maximize the amount of *cy pres* awards provided to NCLC in TCPA actions?

Answer. NCLC encourages class action attorneys to consider nominating NCLC to receive *cy pres* awards in appropriate cases through occasional mailings, e-mails, newsletters, and mentions at relevant conferences and trainings. NCLC does not seek to "maximize" *cy pres* awards; our advocacy consistently supports the maximum distribution of settlement funds to class members.

Question 7. Has anyone who nominated NCLC for a *cy pres* award in a TCPA class action in the past five years (CY2019 to CY2023) received any payment, benefit, award or honorarium from NCLC because of, or in connection to, such nomination for or actual receipt of a *cy pres* award? If so, please describe any such payment, benefit, award, or honorarium received.

Answer. NCLC does not offer or issue any payment, benefit, award or honorarium "because of, or in connection to" nominations for or receipt of *cy pres* awards. We do provide some forms of non-monetary recognition to attorneys who nominate NCLC to receive *cy pres* awards, including lapel pins, plaques, and public expressions of appreciation for the attorney's work to protect consumers on nclc.org, at conferences, and/or in our bi-annual newsletter.

From 2019–2023, NCLC has issued 20 awards: five Vern Countryman Awards for consumer attorneys whose special contributions to the practice of consumer law have strengthened and affirmed the rights of low-income and other vulnerable consumers, and 15 Rising Star Awards to attorneys newer to practice who have made major contributions to consumer law within the past two years by trying or settling a case of great success and significance. Of these 20 individual attorneys, one award winner nominated NCLC for a *cy pres* award in a TCPA class action, and the award was based on that recipient's career accomplishments assisting low-income consumers. Award recipients receive a trophy and $500 in recognition of their lifetime achievements.

Provider Suspension Process

Question 1. In your written *testimony,* you advocated for the Federal Communications Commission (FCC) to immediately suspend a provider from the Robocall Mitigation Database if that provider transmits as few as two calls deemed to have been illegal by a government agency or a government contractor. Your proposed scheme seems like a two-strike system: You get one notification that a problem has occurred, and then if it happens again, you get an immediate suspension and have to cease all operations for 10+ days.

a. In your view, should a voice service provider be forced to cease all operations, sacrifice two weeks of revenue, and defend itself before the FCC if it merely lets just *two* illegal robocalls pass through its network?

Answer. No. The notifications and the suspensions we are proposing are only triggered by numerous (thousands, or tens of thousands) of similar calls transmitted through the same provider.

b. What evidence of wrongdoing should be required before the FCC takes such measures?

Answer. Repeated transmission of illegal calls after notification from a Federal or state enforcement agency, or a designated contractor of one of these agencies, that the provider is continuing to transmit illegal calls.

Question 2. Your proposal contemplates allowing a suspended provider to have a hearing before the FCC's Administrative Law Judge (ALJ) by the end of its 10-day initial suspension. However, there is currently only one ALJ working at the FCC. How will the hearing process move on "an expedited basis" as you describe?

Answer. If necessary, we propose that the FCC employ more ALJs to deal with these hearings. And, if more funding is necessary, we are advocating that Congress should allocate sufficient funds to the FCC to enable it take appropriate steps to stop these illegal calls.

Currently the illegal scam and telemarketing calls cause billions of dollars to be stolen annually by scam callers, and significant losses of time and privacy for almost

all telephone subscribers in the United States. These calls are also a primary contributor to overall denigration of the American telephone system. These costs surely provide sufficient justification for additional funding to the FCC to employ the necessary number of ALJs and other staff.

Question 3. If the hearing can take place immediately after the 10-day period, why do you believe the suspended voice provider will be ready by then?

Answer. As with the hearings that follow temporary restraining orders (TRO) issued pursuant to Rule 65(b) of Federal Rules of Civil Procedure, the 10-day period is for the benefit of the recipient of the orders to request that the TRO be lifted. If the provider requests an extension of time before the hearing, we doubt anyone would object.

a. Why is it a reasonable expectation for every voice provider to have sufficient in-house counsel or teams of lawyers on retainer that can spring into action, gather evidence, write briefs, and prepare arguments within ten days?

Answer. Not every voice provider would need these resources—only those providers whose practices either support or permit the illegal calls to continue after being given notice. The potential for suspension would create incentives for providers to comply with the law.

Additionally, it is highly unlikely that providers who receive these notices would be unaware that they are flouting the law. Indeed, it is more typical for repeated notices to be sent to complicit providers who ignore them and continue to transmit the illegal calls. This dynamic was described in a recent case brought by the Attorney General of Florida against a voice service provider for repeatedly transmitting illegal calls after notice: "Plaintiff alleges that Defendant was notified approximately 250 times of fraudulent calls it has transmitted, despite having this knowledge it continued to connect these calls, profited from these fraudulent calls, refused to implement a means to check for these robocalls, and the calls would not have connected but for Defendant's decision to allow them to transit its network." Office of the Attorney General v. Smartbiz Telecom LLC,—F.Supp.3d—, 2023 WL5491835116 at 4, (S.D.Fl. August 23, 2023).

Question 4. If a voice provider is wrongfully suspended—say, because the suspected illegal robocalls were actually legal, or because the initial notice of having transmitted illegal robocalls was never provided to them—would the provider have any recourse from the FCC for the wrongful suspension?

Answer. Just as with the current process for a court to issue a TRO, one prerequisite would be the requirement for specific facts and evidence of those facts to show that the calls continued after the required notification was given to the voice service provider. (*See* FRCP Rule 65(b)). We have not outlined every specific facet of the procedure, only the general outline. The expedited, *ex parte* process used for TROs is a well-developed process in the Federal and state courts, used to prevent irreparable injury, loss, or damage that would result if the complained-of acts were allowed to continue. We are recommending that the FCC be authorized to establish and pursue a similar process to cut down on these invasive and dangerous calls.

The original notifications should be based on verified information, using any one or several of the available service providers that identify the illegal calls. The FCC should only issue the suspension after ascertaining that the required notifications have been issued.

Question 5. If a voice provider was wrongfully suspended, could they recover damages for the ten days of lost revenue?

Answer. The answer to this question should be based on whether defendants in similar expedited processes (such as TROs issued under Rule 65)) may be entitled to such damages.

a. What about reputational damages they may suffer by being publicly suspended from the Robocall Mitigation Database?

Answer. Please see the answer to question # 5, above.

Lead Generators

Question 1. In your *oral testimony,* you stated: "Telemarketers routinely ignore [FCC] regulations and make . . . about a billion illegal telemarketing calls every month. Then they defend themselves from government and private enforcement by relying on specious consent agreements that were either completely fabricated or based on supposed consent agreements, sold and resold, and sold again by lead generators."

a. Yes or no. If a consumer provides express written consent to a lead generator to be contacted by other businesses, and then their information is sold either to an aggregator or directly to a seller of the good or service the consumer wanted, would you consider any subsequent phone call from such businesses to be illegal?

Answer. Yes. As we and numerous others have stated in comments filed with the FCC (see answers above), under the applicable rules for telemarketing calls made *with an artificial or prerecorded voice,* a lead generator can only collect consent for calls for one seller at a time in one agreement with the consumer. The *FTC has already declared that calls* made after consents for calls using prerecorded voice are traded are illegal under the Telemarketing Sales Rule.

Furthermore, as we and others have also explained in comments filed with the FCC, under the applicable rules for telemarketing calls and texts to *lines registered on the DNC Registry,* the agreement that is necessary to make those messages legal can only be entered into between the seller and the consumer. No lead generator can be involved unless it is an agent of the seller.

Question 2. In your *oral testimony,* you stated that the FCC should "eliminate [the] entire business model" of lead generation. Although there are bad actors within the industry, there are also legitimate companies, including small businesses, that rely on purchasing leads to grow their business and reach consumers who have given consent to be contacted. Could a categorical ban on lead generators harm these legitimate businesses?

Answer. We have not called for eliminating the lead generation industry, only the practice of selling consumers' purported consent for telemarketing calls. There is a distinction between purchasing leads with the contact information of consumers who are interested in particular products or services, and purchasing the consent agreements that are necessary for telemarketing calls to be considered legal under the FCC's regulations. I was only addressing the practice of lead generators of trading the agreements for consent, which we believe to be already illegal, but which the FCC's amendment to the TCPA regulations "unequivocally" makes illegal.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TED CRUZ TO MEGAN L. BROWN

FCC Robocall Forfeitures

Federal Communications Commission (FCC) Chairwoman Jessica Rosenworcel has sought additional authority to make up for the Department of Justice's (DOJ) failure to pursue Telephone Consumer Protection Act (TCPA) violations. While I understand the importance of recovering penalties and fines, I am concerned about giving this additional authority to the FCC. It raises separation of power concerns and could shift the FCC's focus away from pursuing bad actors.

Question 1. Can you please describe the implications of giving prosecution authority over forfeiture penalties to the FCC?

Answer. Authorizing the Federal Communications Commission (FCC) to pursue forfeitures directly in Federal court, instead of relying on the DOJ, would be an expansion of authority and change the role of the FCC's Enforcement Bureau. It may open the door to future expansions of broad direct prosecution authority to the FCC and other agencies. At a time when courts are looking skeptically at Federal agencies' general ability to both interpret and enforce statutes, Congress should not expand the FCC's ability to go straight to court without DOJ. To the contrary, many statutes rely on DOJ enforcement of other agency actions, which makes sense because DOJ is well positioned to prioritize enforcement, exercise prosecutorial discretion, and promote consistency in the positions of the United States before Federal courts. Putting a new responsibility on the FCC may require additional resources and is beyond the agency's procedural and substantive areas of expertise.

It is unnecessary to make such a fundamental change at this time. The FCC has been capably investigating and acting on abuses of the TCPA, the Truth in Caller ID Act, the TRACED Act, and its rules, including recent actions to address police misstatements and defects in the Robocall Mitigation Database (RMD).[1] As FCC Chairwoman Jessica Rosenworcel recently noted, in the last two years since passage of the TRACED Act, the FCC has "stopped more big robocall schemes than at any

[1] *See* Press Release, FCC Seeks to Remove Companies from Key Database for Non-Compliance with Anti-Robocall Rules, FCC (Oct. 16, 2023), available at *https://docs.fcc.gov/public/attachments/DOC-397737A1.pdf.* The FCC's press release discusses the issuance of 20 Enforcement Bureau orders to begin removing specified non-compliant voice service providers from the agency's RMD, due to their submission of allegedly deficient robocall mitigation plans. Their removal from the RMD would require all intermediate providers and terminating voice service providers to cease carrying the companies' traffic, these companies' customers would be blocked, and no traffic originated by these companies would reach the called party.

point in [the FCC's] history."[2] The FCC can continue to pursue bad actors, increase its efforts to clean up the RMD, communicate with industry when it identifies problematic traffic, and increase its collaboration with the agency's registered traceback consortium under the TRACED Act, the Industry Traceback Group. As the FCC itself has noted, when it sends clear messages to stop facilitating bad traffic, the results are impressive. For example, in a recent enforcement action targeting the bad actors behind more than 5 billion fraudulent auto warranty robocalls, FCC Chairwoman Rosenworcel noted that subsequent to its enforcement action, the volume of these calls fell by 99 percent.[3] In recent Senate testimony, Chairwoman Rosenworcel emphasized similar results in student loan scam calls, which were reduced by 88 percent.[4]

Given the ability of DOJ to go to court, there is no demonstrable need to fundamentally change the agency's relationship with the FCC and the courts. In fact, when Congress in the 1970s gave some direct litigating authority to the Federal Trade Commission, it was responding to demonstrated disagreement between the DOJ and the FTC that was affecting litigated cases.[5]

The prior "division of labor created problems when the FTC and DOJ disagreed on substantive areas of antitrust law and policymaking efforts and resulted in poor representation of the FTC's positions through filing delays, settlements that did not reflect the agency's policy goals, and even the refusal to file cases in the first place."[6] There is no apparent disfunction between DOJ and the FCC over collection of forfeitures, so it appears premature at best to expand the role of the FCC.

Question 2. Do you agree that we should focus on getting the DOJ to do its job rather than giving this power to an independent agency?

Answer. The Chamber agrees that it would be preferable to encourage the DOJ to prioritize the collection of FCC forfeitures and the pursuit of other claims—civil and criminal—against those who abuse the communications system to seek to defraud Americans. There are many ways the DOJ, using existing authorities, can investigate and prosecute bad actors and fraudsters, with the FCC and on its own. As I explained in my written testimony, Congress can do several things to encourage DOJ to take more action:

- Require DOJ to file an annual report with Congress explaining enforcement activity it has undertaken in the last calendar year to combat illegal robocalls and its handling of FCC referrals, including the pursuit of forfeiture amounts. This requirement would be similar to the TRACED Act's annual TCPA reporting requirement for the FCC and should require DOJ to explain if and why it has not pursued FCC referrals.
- Prioritize DOJ funds for investigations and enforcement actions against illegal robocallers.
- Require DOJ to establish a robocall enforcement and education office.

TCPA Abuse

Question 1. In your testimony, you point out that TCPA class action litigation filings are once again on the rise even in in the wake of *Facebook v. Duguid.*[7] Why is that and why should the public and lawmakers be concerned?

Answer. It appears that class action lawyers and plaintiffs are turning to other parts of the TCPA, and also that they continue to try to limit and undermine the

---

[2] *See* Statement of Chairwoman Jessica Rosenworcel, *Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17–59; Call Authentication Trust Anchor,* WC Docket No. 17–97; Seventh Report and Order in CG Docket CG 17–59 and WC Docket 17–97, Eighth Further Notice of Proposed Rulemaking in CG Docket 1759, and Third Notice of Inquiry in CG Docket 17–59 (May 18, 2023); available at *https://docs.fcc.gov/public/attachments/FCC-23-37A1.pdf.*

[3] Statement of Chairwoman Jessica Rosenworcel, *In the Matter of Sumco Panama SA, Sumco Panama USA, Virtual Telecom kft, Virtual Telecom Inc., Davis Telecom Inc., Geist Telecom LLC, Fugle Telecom LLC, Tech Direct LLC, Mobi Telecom LLC, and Posting Express Inc.,* File No.: EB–TCD–21–00031913, Forfeiture Order, FCC–23–64 (August 3, 2023) (*Sumco Panama Forfeiture Order*).

[4] *https://docs.fcc.gov/public/attachments/DOC-397034A1.txt*

[5] *See* S. Rep. No. 93–151, at 29 (1973) ("This section insures that the Commission will be able to represent itself in any civil proceeding involving the Federal Trade Commission Act. At the present time, the Commission must, in many situations, rely on the Department of Justice, which has been sluggish in the past in enforcing regulatory agency decisions in Federal courts.").

[6] Eliott Karr, *Independent Litigation Authority and Calls for the Views of the Solicitor General,* 77 Geo. Wash. L. Rev. 1080, 1091 (June 2009).

[7] *Facebook, Inc. v. Duguid,* 141 S. Ct. 1163 (2021).

decision in *Duguid.*[8] Post-*Duguid,* TCPA litigation has remained steady with the overall number of cases dropping slightly at first and gradually increasing.[9] Additionally, the plaintiffs' bar has used techniques to prolong litigation to the summary judgment stage instead of being dismissed at the pleadings stage, giving plaintiffs' attorneys leverage to coerce companies into massive settlements in a post-*Duguid* world.[10] Because of the statutory damages and near strict liability of the TCPA, it simply remains too attractive to class action lawyers.

The proliferation of TCPA class actions should be a concern for policymakers because they generate costly litigation and encourage settlements that may not reflect violations of the law but that greatly benefit lawyers. This is why the TCPA remains a lucrative specialty for the plaintiffs' bar. Because the TCPA operates as a strict liability statute, legitimate businesses that make a mistake can be caught in its cross hairs. And the threat of expensive litigation and enormous damages can lead companies to settle cases even where they have solid defenses and did nothing wrong. For example, even where a company claims it has adequate consent for the communication, it can be difficult to establish consent in early motions practice at the class certification stage. This means a defendant faces enormous litigation costs, creating a strong incentive to settle.

Fundamentally, this sort of punitive TCPA litigation environment does nothing to discourage the fraudsters and scammers that intentionally violate the law and are responsible for the overwhelming majority of illegal robocalls and texts.

Question 2. On October 24th, Ms. Saunders of the National Consumer Law Center *testified* that while she "understand[s] the frustration of the Chamber of Commerce with inappropriate class actions at the moment, the danger of class actions is also one of the prime ways that incentivizes sellers and callers to comply with the law."

a. Do you agree or disagree that the "danger of TCPA class actions" helps consumers and is effective in reducing illegal robocalls?

Answer. I disagree. The fear of TCPA liability chills legitimate and lawful communications campaigns and imposes additional burdens on companies. Legitimate American businesses have robust compliance programs to meet the demands of the TCPA as well as the Telemarketing Sales Rule and other requirements. And the calling ecosystem has extensive codes of conduct and programs that are built on consent and compliance. The bad guys, fraudsters, and criminals abusing our communications networks do not care about compliance and are not deterred by our laws or the threat of class actions. TCPA litigation ensnares legitimate U.S. businesses that already have robust compliance programs and ample incentive to comply with the law.

---

[8] *See, e.g., Borden v. eFinancial, LLC,* 53 F.4th 1230 (9th Cir. 2022) (rejecting attempt to distinguish *Duguid*); *Brickman v. Meta,* 56 F.4th 688 (9th Cir. 2022) (same). The U.S. Chamber participated as amicus in *Brickman,* and explained to the Ninth Circuit that "the TCPA plaintiffs' bar has continued after Duguid to bring putative class actions under the statute seeking exorbitant statutory damages. Like many TCPA plaintiffs since Duguid, Brickman makes an argument that relies heavily on a single sentence within a single footnote in Duguid—footnote 7. As a recent report released by the Chamber's Institute for Legal Reform explains, that footnote "has become the battleground in much of the post-Duguid TCPA litigation." Brief Amicus Curiae, United States Chamber of Commerce, *Brinkman v, Meta,* 9th Cir. No. 21–16785 (filed Apr. 18, 2022) *https://www.uschamber.com/assets/documents/U.S.20Chamber20Amicus20Brief20-20Brickman20v.20United20States2028Ninth20Circuit29.pdf* (citing U.S. Chamber Inst. for Legal Reform, Turning the TCPA Tide: The Effects of Duguid 13 (Dec. 2021), *https://institute forlegalreform.com/wp-content/uploads/2021/12/1323_ILR_TCPA_Report_FINAL_Pages.pdf*).

[9] Turning the TCPA Tide: The Effects of Duguid, U.S. Chamber Institute for Legal Reform (Dec. 2021), *https://instituteforlegalreform.com/wp-content/uploads/2021/12/1323_ILR_TCPA_Report_FINAL_Pages.pdf,* ("Between October 1, 2020 and March 31, 2021, 975 TCPA-related Federal cases were filed. Duguid was decided on April 1, 2021. In the six succeeding months, up to September 30, 2021, 674 TCPA-related cases were filed in Federal court—a decrease of roughly 31 percent."). According to data from Westlaw Litigation Analytics, more than 50 percent of the 2,640 TCPA cases in Federal court in 2022 and so far in 2023 have been class actions. In October 2023 alone, 64 percent of all TCPA lawsuits were class actions. (In Westlaw Analytics, we reviewed docket analytics under the "Experience" (Telephone Consumer Protection Act) tab for 1/01/2022 to 11/20/2023 to identify the total cases (2,640). We reviewed how many were class action (1,463). We also looked at the cases in the date range 10/1/2023-10/31/2023 (122) and reviewed how many were class actions (79) to determine that in October 2023 alone, 64 percent of TCPA lawsuits were class actions.) (last visited Nov. 20, 2023)).

[10] *Id.*

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO MEGAN L. BROWN

Question 1. The TRACED Act increased the FCC's ability to initiate enforcement actions against illegal robocallers who are intentionally violating the law by extending the statute of limitations from 1 year to 3 years, and it eliminated the citation requirement for such violations. Has this provision helped enable the FCC to stop illegal robocallers?

Answer. Yes, this part of the TRACED Act appears to have helped the FCC investigate and bring actions against illegal robocallers. The FCC has been bringing substantial enforcement actions since passage of the TRACED Act, the FCC appeared to have used this provision on at least three occasions. For example, on August 24, 2021, the FCC issued a Notice of Apparent Liability for Forfeiture (NAL) proposing a $5,134,500 fine against John M. Burkman, Jacob Alexander Wohl, and J.M. Burkman & Associates LLC for apparently making 1,141 unlawful robocalls to wireless phones without prior express consent in violation of the TCPA.[11] The FCC noted that this was the first case in which the FCC used the TRACED Act's authorization to issue an NAL for apparent TCPA violations without first issuing a citation.[12] The FCC appears to have leveraged this provision on at least two other occasions.[13]

Question 2. Does the FCC have the authority to revise the definition of an ATDS without a clear directive from Congress following the Supreme Court's decision in *Duguid*?

Answer. No. The Supreme Court's unanimous opinion definitively interpreted § 227(a)(1)(A) of the statute, defining what is required to constitute an autodialer. The Court held that "a necessary feature of an autodialer under § 227(a)(1)(A) is the capacity to use a random or sequential number generator to either store or produce phone numbers to be called." [14]

The FCC does not have authority the revise the statutory definition, as interpreted by the unanimous Supreme Court, nor should it attempt to do so on its own.

Question 3. Could you provide some examples of TCPA filings that you would categorize as litigation abuse?

Answer. There are so many cases that involve beneficial communications, as well as legitimate companies, non-profits and government actors. And in many instances, court rulings prevent speedy resolution of dispositive questions like whether there was consent or whether a call is for telemarketing. Because there is no cumulative limit to damages, plaintiffs' lawyers will continue to seek mind-boggling damages awards. Further, massive classes—such as a recent class certification of over one million people—encourage settlement even where a company has strong defenses. The Chamber provides a few examples:

- *Silver v. City of Albuquerque*[15]: The City of Albuquerque was sued after sending text messages to local residents during the COVID–19 pandemic, notifying them of the opportunity to engage in socially-distanced town halls. The City had to engage in substantial litigation over communications that were intended to help the community participate in local government.
- *Barton v. Serve All, Help All, Inc.*[16]: Serve All, Help All, a non-profit company that provides financial aid and assistance to those with housing needs, was sued by a serial *pro se* litigant for an automated phone call offering a Public Service Announcement for homeowners in default.
- *Eller v. Uber Technologies, Inc.*[17]: Plaintiff sued Uber after receiving text messages that, "Your Driver's License is expired, please head to the app to update it." Plaintiff alleges Uber failed to honor opt-out requests and makes a number of process-based claims about internal policy problems such as lack of sufficient training. Since this case was filed in September 2023, no merits briefing has taken place, but it appears this case will seek enormous damages and fees

[11] *See John M. Burkman, Jacob Alexander Wohl, and J.M. Burkman & Associates LLC,* Notice of Apparent Liability for Forfeiture, FCC 21–97 (Aug. 24, 2021).

[12] *Id.* at ¶ 2.

[13] *See e.g.,* Gregory Robbins; Interstate Brokers of America LLC; National Health Agents LLC, Notice of Apparent Liability for Forfeiture, FCC 22–16 (2022); *see also Thomas Dorsher, ChariTel Inc., OnTel Inc., ScammerBlaster Inc.,* Notice of Apparent Liability for Forfeiture, FCC–22–57 (2022).

[14] *Facebook v. Duguid,* 141 S. Ct. 1163, 1173 (2021).

[15] No. 1:22–CV–00400, 2023 WL 2413780 (D.N.M. Mar. 8, 2023).

[16] No. 3:21–CV–05338, 2023 WL 1965905, at *1 (W.D. Wash. Feb. 13, 2023), motion to certify appeal denied, No. 3:21–CV–05338–RJB, 2023 WL 2372904 (W.D. Wash. Mar. 6, 2023).

[17] No. 4:23–CV–03526 (S.D. Tex. Sept. 19, 2023).

($1500 per text for alleged knowing and willful conduct). It appears this case is on shaky ground. The plaintiff alleges this is a telemarketing text, but it does not appear to be, and it is not clear that the plaintiff followed the opt-out mechanism provided by the company.

- *Head v. Citibank, N.A.*[18]: Plaintiff sued a credit card company in a putative class action alleging that she received unsolicited calls about past-due credit card debt incurred by another person. Citibank argued that the Plaintiff "does not identify a single similarly situated person or phone number that received allegedly wrong number calls." Citibank argued against certification of a class action because, among other things, its internal "wrong number codes" are used for a variety of reasons, and do not necessarily indicate unconsented calls. The court disagreed and certified the class, reasoning that "[i]n light of the enormous rate at which Citibank places calls to delinquent accounts, it seems virtually impossible" that Citibank has not called "at least 40" non-customers, warranting class certification. This ruling is based on speculation but subjects Citibank to expensive litigation and burdensome discovery, delaying resolution and increasing the pressure to settle despite what appear to be meritorious defenses.
- *Hylton v. Titlemax of Virginia, Inc.*[19]: This is a reassigned number case, a type of TCPA case in which companies are sued for making communications to numbers that, unbeknownst to the company, were reassigned from someone who had provided consent to a new user who then sues for the mistake. The plaintiff, Hylton, received communications because Titlemax was trying to contact an individual who had the number prior to Hylton and had consented to calls with a pre-recorded message and agreed to inform Titlemax of any change in his provided number but failed to do so. After receiving calls, Hylton called Titlemax on five occasions, but did not inform Titlemax that she had received the calls on the number they thought belonged to another person nor requested that Titlemax stop calling Hylton's number. Though the defendant was not on notice of the reassigned number and had consent from the previous holder of the number, the court found that "neither the text of the TCPA nor the FCC's recent rulemaking supports the creation of a defense or exemption for those who can show that they reasonably relied upon their intended recipient's prior express consent when calling a reassigned number," and denied Titlemax's motion for summary judgement.
- *Wick v. Twilio, Inc.*[20]: Plaintiff accessed a website, Crevalor, which offered a nutrition supplement. To receive a free sample, the plaintiff submitted his name, address and cell phone number into a form on the website. Plaintiff was then directed to a webpage that provided pricing information. Plaintiff decided against continuing with the order and closed the webpage. Immediately after plaintiff submitted his information, defendant Twilio, which provides automated text messaging services, sent the plaintiff a text message stating: "Noah, Your order at Crevalor is incomplete and about to expire. Complete your order by visiting *http//hlth.co/xDoXEZ*." Plaintiff filed suit under the TCPA, alleging that the text constituted telemarketing. The Court disagreed, reasoning that "it is not telemarketing for the service or product provider to inform plaintiff how to complete" an order process . . . Because plaintiff consented to the communications at issue when he submitted his telephone number during the Crevalor order process, plaintiff fails to plead a TCPA violation." This case show how even valid defenses and consent cannot stop litigation of spurious claims that requires expensive defense costs for targeted companies.

Question 4. You list caps on attorneys' fees as a means to deter abusive TCPA litigation. What is your view on limiting the availability of class actions under the TCPA, which could also deter out-of-control attorneys' fees?

Answer. Limiting the availability of class actions under the TCPA would be an effective way to help reduce enormous attorney's fees. According to data from Westlaw Litigation Analytics, more than 50 percent of the 2,640 TCPA cases in Federal court in 2022 and so far in 2023 have been class actions. In October 2023 alone, 64 percent of all TCPA lawsuits were class actions. The class action vehicle is a major driver of TCPA litigation. The combination of statutory damages ($500 or $1500) multiplied across large numbers of purported class members creates a threat of crushing liability; this leads to large settlements, of which a third or more can go to the lawyers.

---

[18] 340 F.R.D. 145, 149 (D. Ariz. 2022).
[19] No. 4:21–CV–163, 2022 WL 16753869, at *1 (S.D. Ga. Nov. 7, 2022).
[20] 2016 WL 6460316, at *1 (W.D. Wash. Nov. 1, 2016).

The Chamber has long criticized the utility of the class action vehicle because it is often used to target large companies and exact enormous fee awards, with little direct benefit to class members (for example in coupon settlements) or consumers.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO JOSHUA M. BERCU

Heightened Enforcement

Congress passed the TRACED Act in 2019 to enhance the FCC's enforcement authority and increase penalties for illegal robocallers. Since then, scam robocalls have dropped 50 percent, but they remain a serious problem.

Last year, scam robocalls cost American consumers a total of $39 billion. This includes 1.1 million people in the State of Washington. Clearly, we can do more to crack down on these scams.

Question 1. How can we ensure that the partnerships between state law enforcement and the private sector effectively supplement what the FCC and the FTC do on a Federal level?

Answer. State enforcers are critical partners in the fight against illegal robocalls. The ITG works closely with attorneys' general offices from across the country, including Washington. States, like their colleagues at the FCC and FTC, are bringing more enforcement than ever before in large part based on ITG traceback data. For instance, earlier this year, 49 attorneys general sued one provider they deemed responsible for illegal robocalls based on traceback data.

Robocall Mitigation Tools

You spoke of the various types of robocall "mitigation tools" that providers are deploying, which help consumers block unwanted calls.

Question 1. Do the various tools you described work with all technologies and devices?

Answer. Providers have deployed a variety of tools to protect their customers, and most have different tools deployed at different layers of their network and operations. For instance, many providers block calls highly likely to be illegal within the network long before they reach the consumer. Sometimes they do so because the calls are purportedly from numbers on the ITG's Do Not Originate list, a list composed of government and enterprise numbers intended only for inbound calls and never used to make calls.

Providers also have deployed tools that block and label illegal and unwanted calls on a per-call basis. The tools can vary provider-to-provider and vendor-by-vendor, and implementation for wireline can differ from wireless. In addition to the tools deployed by providers and their partners, consumers can obtain over-the-top applications to supplement protections, such as from YouMail, Nomorobo, and Robokiller.

Question 2. How do we ensure that these mitigation tools can evolve quickly enough to counter scammers' changing tactics?

Answer. The tools deployed by providers rely on machine learning and other cutting-edge technologies and methods to detect scammers' latest tactics and address them. As I noted in my testimony, one challenge for providers and legitimate callers alike are bad practices of scammers like number rotation, designed specifically to evade blocking and labeling protections. More oversight and curbing of such practices will help to further isolate illegal calling from legal calling, helping to better mitigate the former while minimizing inadvertent blocking and labeling of the latter.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BEN RAY LUJÁN TO JOSHUA M. BERCU

Handset Operating Systems

Question 1. Fewer and fewer families subscribe to landline telephones, and the great majority of consumers receive robocalls and robotexts through handsets that use Apple iOS or Google Android. How do these handset providers work with STIR/SHAKEN to ensure call recipients have the best information about a call? Do Apple and Google participate in industry groups dedicated to limiting illegal and unwanted calls and texts?

Answer. Neither USTelecom nor the ITG works directly with Apple or Google on robocall or robotext mitigation applications, but it is my understanding that Apple and Google work closely with wireless carriers to continue to improve the customer experience.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN HICKENLOOPER TO JOSHUA M. BERCU

Artificial Intelligence

The Federal Communications Commission (FCC) is launching a proposed inquiry to examine how Artificial Intelligence (AI) can be used as a tool to detect robocalls and robotexts.

Question 1. How have members of U.S. Telecom utilized traditional AI/machine learning for both detecting robocalls and conducting traceback campaigns? Are members of U.S. Telecom exploring methods to detect AI-generated robocalls?

Answer. USTelecom members are at the forefront of deploying cutting-edge technology to protect their customers. Providers and their analytics partners have long relied on machine learning and other tools to detect and stop scammers' latest practices. Providers choose the technologies and methods most effective for that goal. As a general matter, providers and their analytics partners are focused on identifying patterns of bad calling activity based on numerous factors. Their tools often focus primarily on such patterns, and capture illegal robocall activity whether generated by AI or not.

Traceback Transparency

Industry Traceback Group (ITG) traceback information is only released to selected parties and not made publicly available. In November 2022, ITG stated in their public comments submitted for the Federal Communications Commission's (FCC) annual report to Congress that releasing raw traceback information to the public could be "misleading and harmful" without proper context.

Question 1. What steps is ITG taking to increase real-time transparency about scam calls to the public? Can generative AI be used in a virtual assistant to provide the necessary context to consumers such that they can easily digest raw traceback information?

Answer. The ITG relies on third parties, such as YouMail, Robokiller, and individual providers, for real-time information about ongoing scam call campaigns. The ITG's traceback data is limited to information about suspected illegal call examples and how those calls transited from provider to provider across the telephone network. Such information does not offer either beneficial or actionable information directly to individual consumers, but it is critical to enforcement. In that regard, last year, the ITG launched a portal to provide direct access to traceback data to the FCC and other Federal and state law enforcement agencies. The ITG also responds to hundreds of subpoenas from such agencies to support their enforcement efforts.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JOHN THUNE TO JOSHUA M. BERCU

Question. In your testimony, you mention that the registered traceback consortium established under the TRACED Act has been an effective tool for identifying illegal robocalls. Are there steps Congress should take to further advance industry efforts to crack down on illegal calls? How would the Robocall Trace Back Enhancement Act, legislation I led last Congress with Senator Markey, help bolster privately led efforts to trace illegal robocalls?

Answer. The Robocall Trace Back Enhancement Act would advance the ITG's efforts in combating illegal robocalls by extending liability protection to the ITG as the registered traceback consortium responsible for traceback. The legislation would allow the ITG to continue to be aggressive in disrupting illegal call flows through sharing of traceback-based data within the industry and with government entities by protecting the ITG as the registered consortium from frivolous lawsuits aimed at undermining the traceback process.

The ITG would also support Congress extending the consortium designation process to every three years. Under the TRACED Act, the registered traceback consortium must be designated by the FCC annually. The FCC's review and oversight are integral to confirming that the consortium operates in a neutral and non-discriminatory manner. Conducing the designation process on an annual basis, however, ties up the Commission's resources as well as those of the consortium. Those resources would be better dedicated to investments in advancing the fight again illegal robocalls.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO MICHAEL RUDOLPH

Innovation and Adoption

Robocallers are taking advantage of technological innovations to flood our phones with calls and texts. It seems to me that other forms of technological innovation—like machine learning and generative artificial intelligence– hold the most promise for combatting this flood of illegal robocalls.

Question 1. How can Congress and the FCC encourage telecommunications companies to embrace innovative technologies and use new tools responsibly to protect consumers from robocalls?

Answer. The biggest current challenge meriting Congressional and FCC assistance to combat illegal robocalls and robotexts is assisting in the adoption of effective, innovative technologies.

Presently, telecommunication companies are *not incentivized* to solve these problems as solving the problems not only costs time, and resources, but the eventual outcome is lost revenue from the now missing robocommunications.

Robocalls are introduced into the phone network because the "chain of trust" has been broken, and a telecommunication company has allowed a nefarious, bad acting account or other telecommunication company to enter the network and bring along unwanted, unlawful communications.

At present, telecommunication companies, being profit-driven enterprises, seek to maximize revenue. Maximizing revenue means carrying as many robocalls as reasonably possible while signaling to investigators and enforcement that "just enough" mitigation effort is applied and a conveying "just enough" responsiveness to investigative demands.

For example, take recent evidence from the public record in the Florida Southern District Court from Office of Attorney General, State of Florida vs Smartbiz Telecom LLC (1:2022cv23945). Document 50–32 contains 18 pages of invoices of a provider accused of being a conduit of millions of unlawful robocalls. The very first invoice indicates that the provider earned $140,063 of revenue in 1 month via 1 relationship for 96 million calls, or $0.0015 per call. Documents for this case further include 444 pages of traceback e-mails received by this telecommunication provider for 261 traceback notifications starting in 2020. In just one route of this provider's business, approximately 814 million calls from July 2022 through June 2023 generated $1.22 million in revenue.

US Telecom recently indicated that the average traceback travels 6.1 hops [1] which could then be applied to form an approximate "industry revenue model" for 814 million such calls by using the .0015/call rate and 10 percent wholesale margins. In total for the six provides involved, 814 million similar calls generate $5.7M in telecommunications revenue, with $720,000 for the final provider servicing the call recipient.

Hop 1	Hop 2	Hop 3	Hop 4	Hop 5	Term (Hop 6)
$1.22M	$1.10M	$988K	$889K	$800K	$720K

The current state in industry for innovative solutions that identify which accounts and partners carry these calls faces tremendous resistance if a telecommunications company can achieve sufficient robocall mitigation compliance by simply responding to individual incident reports (direct or via traceback) and taking down individual numbers on accounts as they are reported rather than seek to exterminate all similar traffic from their networks. The decision to not adopt comprehensive solutions not only saves the provider from paying for the cost of those solutions, but also allows the provider to retain as much revenue from allowing the remaining unreported, uninvestigated, unlawful traffic to continue transiting their networks.

In 2002, the Sarbanes-Oxley Act was passed with votes of 423–3 and 99–1 that mandated certain practices in financial record keeping and reporting for corporations. Minimal or non-existent detection, investigation and mitigation controls at communications companies are predominantly responsible for the plague of robocommunications. Present reductions have only been achieved due to FCC orders [2] that create a no-tolerance policy for certain topical robocalls and then follow it up

[1] *https://docs.fcc.gov/public/attachments/DOC-390423A3.pdf*

[2] *https://www.fcc.gov/document/robocall-enforcement-order-all-us-based-voice-service-providers*

orders with direct evidence, outreach and enforcement to eliminate the traffic exhaustively throughout the telephone network.

If communication platforms servicing unlawful robocommunication operations were subjected to regular assessments similar to those within Section 404 of Sarbanes-Oxley requiring management and external auditors to report on the adequacy of a company's internal controls (and to also improve deficient controls, even if that meant losing material revenue), it would dramatically shift the risk/revenue balance throughout industry with new standards for conduct, tolerance and accountability.

As the problem is rooted in functions balancing risk with revenue, it is not solved without further Congressional action to change the balance of the equation where providers seek to eliminate the risk rather than protect revenue.

AI and Deepfake Calls

I recently heard about an alarming situation in my state. A family in Pierce County, Washington received a deepfake call, where a scammer used AI to spoof their daughter's voice saying that she had been in a car accident and that a man was threatening to harm her unless they wire $10,000. No family should have to face this.

Question 1. How can Congress empower consumers, regulators, and law enforcement to stay ahead of the increasingly sophisticated technologies scammers use?

Answer. This particular scam is one of the most difficult ones to stay ahead of, as it:

- Uses a phone number that appears as unknown to the recipient
- Uses a convincing "deep fake" voice of someone the recipients knows and cares about
- Explains the rational for using a suspicious, unrecognized number is part of the reasoning for the crisis requiring sending money

Technology innovators thrive in a continuous effort to stay ahead of the scammers, but are certainly only permitted to innovate solutions within the confines provided by Google on Android devices and Apple on iOS devices.

The scam perpetrator in this case may:

- be using a VOIP number obtained from a CPaaS platform
- have walked into an actual store and obtained a phone or plan
- may be using an "over the top" (*i.e.,* "burner") phone number app they downloaded (perhaps even for free)

Presently, companies like YouMail possess data that indicate the origination and history of the number. If the scammer is saying they "have borrowed a friend's phone", there is data to refute this and indicate that the number is recently acquired and could indicate details for the source and geography. If allowed by Google or Apple, this information could be displayed alongside the call so the recipient could "check the facts".

YouMail, as a device installed app on Android or Google, enables individuals to link their address book data. In many cases, because so many people do not answer calls from unknown numbers, this particular scam leaves a voice-mail message. YouMail transcribes every voice-mail message left for its users and does "extract" the identity the caller provided for themselves (*i.e.,* "Hi, this is your grandson, Mike. . ."). YouMail can use this content to provide a live warning or caution indicator to the recipient that provides more details on the call origination and educates the customer live at the time of interacting with the call and reduces the chance the call is returned, or a subsequent live call from that number is answered.

Ultimately, this particular communication was criminal, and law enforcement must apprehend the criminal parties behind the call. By partnering with law enforcement, YouMail has enabled identification of the parties operating scams such as these using same-day, live data and domestic threat actors can be pursued by enforcement while and in-network countermeasures can be put in place at cooperating network providers for communications originating from outside the U.S.

Heightened Enforcement

Congress passed the TRACED Act in 2019 to enhance the FCC's enforcement authority and increase penalties for illegal robocallers. Since then, scam robocalls have dropped 50 percent, but they remain a serious problem.

Last year, scam robocalls cost American consumers a total of $39 billion. This includes 1.1 million people in the State of Washington. Clearly, we can do more to crack down on these scams.

Question 1. How can we ensure that the partnerships between state law enforcement and the private sector effectively supplement what the FCC and the FTC do on a Federal level?

Answer. YouMail partners directly with many State Attorneys General offices to monitor, investigate, disrupt and enforce laws against robocall operations. YouMail thanks the State of Washington for its active role and partnership investigating certain robocall campaigns over the past few years and its participation in the multi-state Anti-Robocalling Task Force.

YouMail has provided data indicating the robocall reduction since the passage of the TRACED Act directly ties to state and Federal efforts to investigate and shut down the highest volume robocall operations—such as the robocalls impersonating the Social Security Administration, offering extended warranties or providing student loan assistance. YouMail presently applies investigative resources to track several thousand active robocall campaigns each month for directly classifying and stopping these calls from harming YouMail users directly. Additionally, YouMail works to provide evidence to state and Federal investigative and enforcement resources but observes those resources only have bandwidth to investigate a few dozen of these active campaigns at a time. YouMail has observed certain states (North Carolina, Ohio, Florida, Indiana, Vermont, Washington) have taken more active roles in the Anti-Robocalling Task Force. If each state would contribute resources proportional to its population affected by robocalls, current investigative and enforcement impacts would be increase significantly and more active robocommunication threats could be investigated and disrupted.

Robocommunications that are criminal or unlawful require an appropriate amount of policing to prevent and deter. State enforcement can operate with greater agility than Federal enforcement, particularly when issuing CID or subpoenas on robocommunications operations, but the amount of criminal or unlawful activity it can pursue is proportional to the number of real people that have those responsibilities set as their weekly priority within their respective offices.

In simpler terms, there are not enough state and Federal police proportional to rising crime occurring via the telephone network and digital communication platforms.

Robocall Mitigation Tools

You spoke of the various types of robocall "mitigation tools" that providers are deploying, which help consumers block unwanted calls.

Question 1. Do the various tools you described work with all technologies and devices?

Question 2. How do we ensure that these mitigation tools can evolve quickly enough to counter scammers' changing tactics?

Answer. It should be reinforced that not all robocalls are scams. YouMail has partnered with certain states to review direct consumer complaint data and tie those consumer complaints to the calling campaigns or even the exact call made related to that complaint. Generally, the majority of robocall complaints received by a State are "grey area telemarketing" rather than true criminal-intent scams. Further scoping this to complaints received by a State that are criminal in nature identifies hundreds of threat actors operating at lower volumes.

YouMail operates as a bridge between consumers receiving communications on their devices, their mobile network operators, the communication networks in between the originator and recipient, any business or entity that may have been impersonated and finally state and Federal enforcement agencies with committed resources to combatting these communications.

YouMail presently works from an evidence capture perspective on both Android and iOS devices and can relay this data through to enforcement resources that same hour/same day. However, some phone carriers do not allow consumers to use a service such as YouMail to become the 'answering service' for their calls. Engaging a solution like YouMail directly on your device as a consumer also potentially suffers from a fair amount of friction to 'activate' it successfully depending on the willingness of the handset maker or the carrier to allow third-party solutions.

There are significant "boxes of evidence" that have yet to be opened up for agile detection and enforcement. For example, consumers can report unwanted SMS to their carrier by sending it to "7726" or tapping "Report Junk". Presently this data resides within each carrier to evaluate or improve its own analytics (as a competitive enabler) and does not leave that carrier's databases for broader consumer protection or benefit. Both Apple and Google have material live intelligence of communication threats (particularly via iMessage and RCS) and consumers have no convenient method to indicate they are willing to also grant independent security appli-

cations (*i.e.,* YouMail, McAfee, Aura, Gen/Norton, etc) access to this threat data for direct consumer benefit.

Encouragement for the carriers and platforms/operating systems to make changes that would allow consumers to share their reports and to share threat intelligence improves the collective response time of industry to identify threats as they are occurring and implement countermeasures that enhance consumer safety and security.

STIR/SHAKEN Call Authentication

In 2019, Congress passed the TRACED Act to require phone carriers to adopt STIR/SHAKEN call authentication standards. These standards create a digital signature that identifies the calling party and allows phone carriers to verify calls, while weeding out calls from illegitimate sources.

While these standards have helped in the important fight against robocalls, they have certain limitations. For example, they will not work for all telephone calls. We have seen illegal robocallers change tactics, moving away from using fake phone numbers to buying real phone numbers that trick spam-blocking software into allowing the calls through.

Question 1. Your testimony notes that STIR/SHAKEN currently has insufficient resources to carry out the investigative and enforcement efforts needed to stop illegal robocalls. What can Congress, the FCC, and providers do to address this resource gap and other limitations?

Answer. From an industry-wide perspective, effective robocommunication mitigation is achieved through joint efforts of all parties when live communications evidence captured at the consumers' device is available that same day (or as soon as possible thereafter) to be used for committed investigative and enforcement resources combatting those particular communications. In the cases of vehicle warranty spam and scam calls, and student loan spam and scam calls, prioritized investigation and elimination of those calls met with success in "short circuiting" the calls as they reached consumers, disrupting those calls at their point of origination and identifying the parties behind those calls. Scaling this formula for success with additional state, Federal and private resources so the capacity to mitigate dozens to hundreds of active campaigns rather than just a few is essential to have "eyes on all the present tactics".

Communication networks have evolved into digital streets that some consumers travel more often than real, physical streets. Threats and crime have followed opportunity to these streets as they are less protected, policed and understood. As private enterprises, communication providers pursue their self-interests and revenue goals and do not bear substantial obligations to protect the general public in the same manner as state or Federal agencies. There are state-specific robocommunications attacks occurring in states without any material state resources to police the threat. There are nation-wide attacks with an expanding but still resource-constrained FCC to stay abreast of every robocommunications campaign every month. Based on active participation in joint efforts in 2021–23, total funding by states and Federal agencies for robocommunications investigation, mitigation and enforcement relies on the work of 15–20 individuals, many who balance other non-robocommunications matters in their monthly responsibilities. With several thousand robocommunication campaigns active each month, the ratio of threat to nationwide individual reacting to the threat is between 300:1 and 500:1.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BEN RAY LUJÁN TO MICHAEL RUDOLPH

Handset Operating Systems

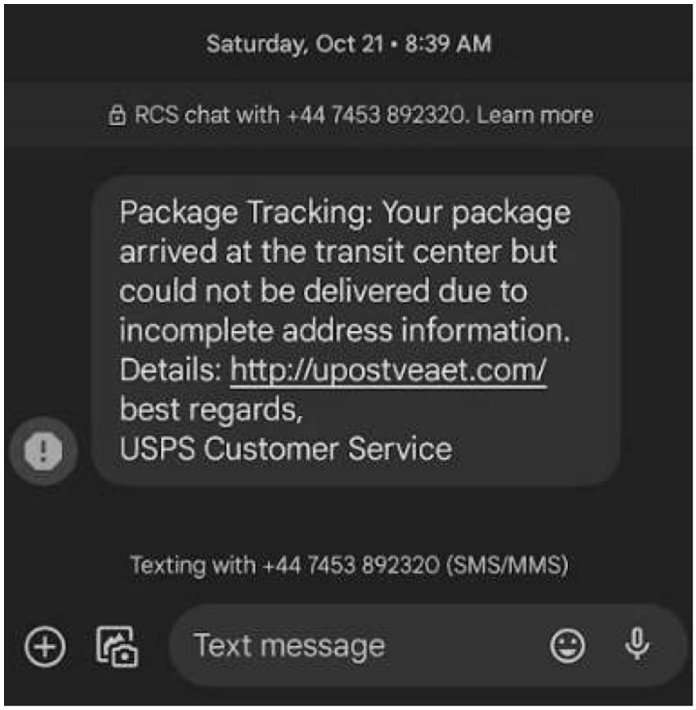
Question 1. Fewer and fewer families subscribe to landline telephones, and the great majority of consumers receive robocalls and robotexts through handsets that use Apple iOS or Google Android. How do these handset providers work with STIR/SHAKEN to ensure call recipients have the best information about a call? Do Apple and Google participate in industry groups dedicated to limiting illegal and unwanted calls and texts?

Answer. As the handset platform/operating system providers, Apple and Google can play significant roles in combatting illegal and unwanted calls and texts.

Since there is such an expansive amount of unwanted communications, it's possible to meet twenty people who complain about an unwanted or illegal call or text and for each of those twenty individuals, stopping their particular unwanted communication requires a different approach. Depending on the scam and the approach,

further success has dependencies on both technology but also policy and regulatory change

As one example, package delivery scams have evolved from using SMS messaging to instead use iMessage or RCS messaging:



If the recipient of most of these recent messages looks closely, while they may have been perceived as an SMS message, it may show an indication that the message was an "iMessage" or "RCS chat". The way RCS or iMessage work is they send the messages over the data channel of your carrier (Verizon, AT&T, T-Mobile, etc) so those mobile carriers cannot do anything to identify nor stop that message from reaching your device. From their origination point, they are encrypted and travel through your data connection (and not SMS or voice channels) and only upon reaching the recipient device, are decrypted. Thus, any assumption that a carrier or app-based solution can address these unwanted or illegal communications is false as any solution depends on Google or Apple providing such visibility or capabilities to touch that message.

With regards to handset providers working with STIR/SHAKEN to assist call recipients, the most common indication that there is some perceivable benefit to a call recipient is the "green checkmark" next displayed next to an incoming call on Android devices. Google has provided the most access to the "verification status" of a call which is essentially asking "was the call signed properly?"). This small window of access is possible via a "getCallerNumberVerificationStatus" method made available to developers in Android 11 developer APIs[3] in 2020 but has evolved little since. iOS13, released in 2019, or newer devices will show similar information, but in the call log after the call has completed rather than when the call is actively presented on the device to make an answering decision.

Joint investigation efforts by YouMail, major banks and law enforcement has typically found that the "green check mark" is often utilized by threat actors to make their calls appear more legitimate, rather than an indication of trust. Specifically, bank imposter calls will obtain real numbers that carry authentic STIR/SHAKEN data through to display the "green check" on the consumer device.

---

[3] *https://developer.android.com/reference/android/telecom/Call.Details#getCallerNumberVerificationStatus()*

Industry has long benefited from innovative companies that can assist consumers with problems such as these, but at present neither Android nor Apple make it easy for third-parties to augment an incoming or historical call with valuable, assistive information. As an example, in partnership with several banks, YouMail knows exactly which numbers are used by those banks to originate their legal voice calls or SMS messages and could use this intelligence to indicate to a consumer that an incoming or previous communication with content claiming to be the bank from a number outside this known set of numbers is very highly likely an impersonation of that bank with a clear consumer warning rather than an obtuse "Scam Likely" warning.

At present, neither Apple nor Google play material, active roles in these groups or trade associations where network providers, banks or enforcement agencies convene on robocall/robotext matters. Given the unique data they collect from the handset devices or consumer reports using features like the 'Report Junk' ability on an Apple device, they possess highly valuable intelligence that can be a leading indicator of major threats targeting Americans. Carriers, banks, consumers and other organizations can benefit from these signals to put countermeasures in place as well as educate consumers to threats before and during their rise rather than days later. However, this intelligence is also a tremendous competitive advantage for companies to use in order to compete with one another, so there are factors contributing to minimal, if any, intelligence sharing in industry.

Minimal access to enhance consumer safety is provided by Apple and Google devices for third-party innovators, and often what little is provided has major hurdles that introduce friction into providing the solution for consumers. YouMail is fortunate enough to have over 13 million registered U.S. users in its decade of directly providing safe communication solutions to U.S. consumers, but faces many challenges in its end-users getting setup correctly due to consumers needing to jump in and out of the app in order to manage settings at the operating system level outside of the app itself. It would be transformative if Android and Apple made it easier for consumers to leverage innovative solutions directly that give them more control over which communications they allow to reach them and how they are allowed to do so.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. PETER WELCH TO MICHAEL RUDOLPH

Question 1. FCC Chairwoman Jessica Rosenworcel has expressed interest in exploring how generative artificial intelligence might be used to stop robocall and robotext scams.

a. How is generative AI being explored to combat robotext scams, and what potential advantages does it offer for identifying and blocking fraudulent text messages?

b. Are there ethical or privacy concerns associated with using generative AI to filter or create text messages, and how can these concerns be addressed?

c. As Congress considers potential legislative responses to emerging AI technologies, what steps—if any—should it take to protect consumers from generative AI scams, while preserving the ability of Federal regulators and industry to innovate?

Answer. Artificial Intelligence (AI), Machine Learning (ML) and Natural Language Processing (NLP) have long been used to analyze and identify communications, using both behavior of senders/numbers (volume, reach, frequency), the communication content carried by those senders/numbers, or to analyze individual consumer complaints about senders/numbers.

Advances by ChatGPT, Large Language Models (LLMs), Generative AI and Discriminative AI have brought a lot of attention to their potential as tools to combat fraudulent communications. YouMail is just one of many companies using generative and discriminative AI to analyze text message content to separate lawful messaging from illegal messaging. The more powerful, modern models require less development resources to effectively and accurately perform these tasks that can follow threat actor messaging campaigns over time as they impersonate multiple institutions. They can evaluate conversations that otherwise look like personal communications and observe indications of potential social engineering, and alert customers to concerns about that communication (if allowed to by the handset manufacturer). AI-assisted evidence collection has been and continues to be provided by YouMail directly and regularly to many state and Federal enforcement agencies for action against specific topical, prioritized threats.

AI scanning personal communications is a slippery slope when it comes to ethical or privacy concerns. As an example, your Internet provider could scan every single file you download without your knowledge and decide which files arrive on your computer unaltered or potentially decide to block those outright. Or, as a consumer you could choose which utilities you trust to perform this job for you and enable/disable them as you control them outright (*i.e.,* anti-virus software such as that by McAfee, Microsoft or Norton). The same slippery slope exists for communications—voice calls and messaging such as SMS. Consumers have a variety of use cases where some folks may be extremely susceptible to social engineering scams and want their inbound communications to essentially be limited to trusted, close acquaintances. Small businesses, like a plumber or electrician, may want every potential call or message coming through to their business line since every communication could be an essential lead for their business that day or week.

In essence, utilities and filtering powered by generative or discriminate AI are not unlike virtual robotic assistants you could choose to employ at your discretion, and you could select the one that is most appropriate for your needs. 2020–2030 will see science fiction is no longer far from reality where your incoming communications can be screened by artificial intelligence where each embodiment of AI behaves slightly differently depending on how it has been trained or programmed.

There are certainly concerns in a future if consumers rely on an unseen AI presence operating at the handset or within the network (or multiple networks in tandem) that is unknown with questions over how they have been tuned to filter or block communications that are in a 'grey area'. Consider political communications that travel systems with AI models that consider them as 'potentially scam' for one political party and 'not spam' for the other political party. Any time any filtering is performed for a consumer, they should be able to control who performs the filtering and ideally consumers would select solutions that transparently show them what they were protected from (*i.e.,* in a spam folder or quarantine folder) so the audiences of those solutions can be held accountable for the standards those consumers expect from them. This provides consumers with the choice to select aggressive or passive systems to use as their defenses. YouMail provides many settings to its end-users to decide how its AI-enabled solutions classify and treat incoming calls and messages and ultimately consumers can always visit their 'Spam folder' to see if these settings need to be changed because they want more or less calls like the one they are viewing. Similarly, YouMail does believe any solution given such a power to act as a barrier or shield to communications should be one that consumers have total control of choice and configuration in how it works for them.

As Congress considers legislative responses, it is presently too early to provide a definitive recommendation on steps it should take. One of the challenges with generative AI is that it has evolved to a point that it is extremely difficult to distinguish from a real person when authoring text or audio content. While a text message or audio file could be examined and a likelihood assigned that it may have been created by generative AI, investigative and enforcement efforts need to reach higher levels of certainty by collecting hard evidence that generative AI was utilized by threat actors (*i.e.,* finding logs of sessions with LLMs on the threat actor devices).

Congress should continue to encourage efforts like the FCC's recent Notice of Inquiry [4] on November 16 2023. Even if this NOI produces few response filings by December 18, 2023, Federal agencies charged with protecting consumers from unsafe communications benefit from increased encouragement to apply resources and take quick action against rapidly evolving threats causing harm. Representatives can of course direct additional funding to their respective destinations, at the state and Federal level, which will not only enable more personnel to police and enforce laws against these unlawful communications, but also stimulate innovation in solutions used by these personnel to achieve this policing and enforcement at better scale.

○

[4] *https://www.fcc.gov/consumer-governmental-affairs/fcc-launches-inquiry-ais-impact-robocalls-and-robotexts*