STOPPING ILLEGAL ROBOCALLS AND ROBOTEXTS: PROGRESS, CHALLENGES, AND NEXT STEPS

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

JUNE 4, 2025

Serial No. 119–22

Published for the use of the Committee on Energy and Commerce
govinfo.gov/committee/house-energy
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
60–677 PDF WASHINGTON : 2025

COMMITTEE ON ENERGY AND COMMERCE

BRETT GUTHRIE, Kentucky
Chairman

ROBERT E. LATTA, Ohio
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
RICHARD HUDSON, North Carolina
EARL L. "BUDDY" CARTER, Georgia
GARY J. PALMER, Alabama
NEAL P. DUNN, Florida
DAN CRENSHAW, Texas
JOHN JOYCE, Pennsylvania, *Vice Chairman*
RANDY K. WEBER, SR., TEXAS
RICK W. ALLEN, Georgia
TROY BALDERSON, Ohio
RUSS FULCHER, Idaho
AUGUST PFLUGER, Texas
DIANA HARSHBARGER, Tennessee
MARIANNETTE MILLER-MEEKS, Iowa
KAT CAMMACK, Florida
JAY OBERNOLTE, California
JOHN JAMES, Michigan
CLIFF BENTZ, Oregon
ERIN HOUCHIN, Indiana
RUSSELL FRY, South Carolina
LAUREL M. LEE, Florida
NICHOLAS A. LANGWORTHY, New York
THOMAS H. KEAN, JR., New Jersey
MICHAEL A. RULLI, Ohio
GABE EVANS, Colorado
CRAIG A. GOLDMAN, Texas
JULIE FEDORCHAK, North Dakota

FRANK PALLONE, JR., New Jersey
Ranking Member
DIANA DEGETTE, Colorado
JAN SCHAKOWSKY, Illinois
DORIS O. MATSUI, California
KATHY CASTOR, Florida
PAUL TONKO, New York
YVETTE D. CLARKE, New York
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan
MARC A. VEASEY, Texas
ROBIN L. KELLY, Illinois
NANETTE DIAZ BARRAGÁN, California
DARREN SOTO, Florida
KIM SCHRIER, Washington
LORI TRAHAN, Massachusetts
LIZZIE FLETCHER, Texas
ALEXANDRIA OCASIO-CORTEZ, New York
JAKE AUCHINCLOSS, Massachusetts
TROY A. CARTER, Louisiana
ROBERT MENENDEZ, New Jersey
KEVIN MULLIN, California
GREG LANDSMAN, Ohio
JENNIFER L. MCCLELLAN, Virginia

PROFESSIONAL STAFF

MEGAN JACKSON, *Staff Director*
SOPHIE KHANAHMADI, *Deputy Staff Director*
TIFFANY GUARASCIO, *Minority Staff Director*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

GARY J. PALMER, Alabama
Chairman

TROY BALDERSON, Ohio, *Vice Chairman*
H. MORGAN GRIFFITH, Virginia
NEAL P. DUNN, Florida
DAN CRENSHAW, Texas
RANDY K. WEBER, SR., TEXAS
RICK W. ALLEN, Georgia
RUSS FULCHER, Idaho
MICHAEL A. RULLI, Ohio
BRETT GUTHRIE, Kentucky (ex officio)

YVETTE D. CLARKE, New York
Ranking Member
DIANA DEGETTE, Colorado
PAUL TONKO, New York
LORI TRAHAN, Massachusetts
LIZZIE FLETCHER, Texas
ALEXANDRIA OCASIO-CORTEZ, New York
KEVIN MULLIN, California
FRANK PALLONE, JR., New Jersey *(ex officio)*

C O N T E N T S

STOPPING ILLEGAL ROBOCALLS AND ROBOTEXTS: PROGRESS, CHALLENGES, AND NEXT STEPS

WEDNESDAY, JUNE 4, 2025

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, D.C.

The subcommittee met, pursuant to notice, at 10:15 a.m., in room 2322, Rayburn House Office Building, Hon. Gary Palmer (chairman of the subcommittee) presiding.

Members present: Representatives Palmer, Balderson, Griffith, Dunn, Crenshaw, Weber, Allen, Fulcher, Rulli, Guthrie (ex officio), Clarke (subcommittee ranking member), DeGette, Tonko, Trahan, Fletcher, Ocasio-Cortez, Mullin, and Pallone (ex officio).

Also present: Representatives Joyce and Pfluger.

Staff present: Ansley Boylan, Director of Operations; Jessica Donlon, General Counsel; Sydney Greene, Director of Finance and Logistics; Brittany Havens, Chief Counsel; Megan Jackson, Staff Director; Sophie Khanahmadi, Deputy Staff Director; Alex Khlopin, Clerk; John Lin, Senior Counsel; Sarah Meier, Counsel and Parliamentarian; Joel Miller, Chief Counsel; Chris Sarley, Member Services/Stakeholder Director; Joanne Thomas, Counsel; Matt VanHyfte, Communications Director; Aurora Ellis, Minority Law Clerk; Austin Flack, Minority Professional Staff Member; Waverly Gordon, Minority Deputy Staff Director and General Counsel; Tiffany Guarascio, Minority Staff Director; Will McAuliffe, Minority Chief Counsel, Oversight and Investigations; Constance O'Connor, Minority Senior Counsel; Christina Parisi, Minority Professional Staff Member; Harry Samuels, Minority Counsel; and Caroline Wood, Minority Research Analyst.

OPENING STATEMENT OF HON. GARY J. PALMER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ALABAMA

Mr. PALMER. Good morning, and welcome to today's hearing entitled "Stopping Illegal Robocalls and Robotexts: Progress, Challenges, and Next Steps."

All of us have personal experiences with unwanted robocalls and robotexts. Some are merely annoying, but others have devastating consequences. For example, in March, the FCC warned consumers about scam robocalls targeting older Americans, and the Department of Justice announced that it charged 25 individuals for participating in the same scam that defrauded Americans out of more

than $21 million in more than 40 States. The scammers made phone calls pretending to be an individual's grandchild who needed money for bail after being arrested, or pretended to be the grandchild's attorney and were told that they could not speak to anyone about the arrest. This is one of the many heartbreaking examples of scams perpetrated on Americans by illegal robocallers and bad actors.

According to recent estimates, in April of 2025, nearly 2,000 robocalls were placed to U.S. consumers every second. Spam and scam calls make consumers feel threatened, fearful, and distrustful of legitimate calls. As more and more Americans ignore calls from unknown numbers, they miss important calls. Moreover, fraud perpetrated against Americans by illegal robocalls costs an average of $25 billion annually, primarily affecting those who cannot afford such losses.

We are also seeing a lot of unwanted and scam robotexts and AI-generated phone calls and text messages, including voice clones and deepfakes. According to the FCC, consumer complaints about unwanted text messages increased 500-fold between 2015 and 2022. Americans are frustrated, and understandably so.

In 2019, the bipartisan Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence, or TRACED, Act was enacted to help reduce the flood of illegal robocalls. The TRACED Act allowed the FCC and law enforcement to impose stricter penalties for intentional violations of the Telephone Consumer Protection Act, or TCPA, improved adoption of technical solutions like STIR and SHAKEN call authentication framework, and established a Federal interagency working group to combat illegal robocalls. As a result, U.S. telecommunications carriers have made progress implementing STIR/SHAKEN into their networks.

This framework authenticates that phone calls are coming from legitimate phone numbers, which helps reduce the number of spoofed and illegal robocalls. Generally, to operate within the U.S., voice service providers must now implement robocall mitigation programs and file these plans in their STIR/SHAKEN compliance certifications in the robocall mitigation database overseen by the FCC. Moreover, in July 2020, the FCC recognized the USTelecom Industry Traceback Group as the single registered consortium to conduct private led traceback efforts that identified the source of an illegal robocall. The FCC has also taken measures to address the growing burden of unwanted and scam robotexts and abused AI technologies.

Specifically, in March 2023, the agency adopted regulations targeting scam robotexts. In addition, industry actors have partnered with Federal agencies to launch new programs such as robotext tracing. Lastly, in August, the FCC proposed rules to protect consumers from AI-generated robocalls and robotexts.

These are steps in the right direction, and I applaud the coordination we have seen thus far. While the TCPA has provided many useful tools, the TCPA's private right of action has given rise to class-action lawsuits focused on minor infractions rather than the bad actors responsible for placing illegal robocalls, and it has not reduced the number of illegal robocalls or improved consumer protection.

In addition, STIR/SHAKEN implementation among smaller carriers has been delayed, and bad actors have exploited these providers' reliance on legacy infrastructure. Moreover, a majority of illegal robocalls and robotexts originate overseas, making them hard to trace. Because these bad actors are outside the jurisdiction of U.S. law enforcement, they are challenging to combat.

Finally, the FCC must grapple with emerging technologies and navigate the best way to create appropriate guard rails for these technologies, while simultaneously continuing to support innovation. We will always have robocalls and robotexts because not all of them are illegal. Many are used for legitimate purposes by U.S. businesses and public entities. But we must continue finding ways to combat the unwanted communications.

I want to thank our panel of witnesses for joining us. I look forward to a robust discussion to understand the current landscape of illegal robocalls and robotexts plaguing U.S. consumers and businesses, so we can work together to identify and address remaining challenges.

[The prepared statement of Mr. Palmer follows:]

Chairman Gary Palmer
Opening Statement - Subcommittee on Oversight and Investigations
"Stopping Illegal Robocalls and Robotexts: Progress, Challenges, and Next Steps"
June 4, 2025

Good morning, and welcome to today's hearing entitled "Stopping Illegal Robocalls and Robotexts: Progress, Challenges, and Next Steps."

All of us have personal experiences with unwanted robocalls and robotexts. Some are merely annoying, but others have devastating consequences. For example, in March, the FCC warned consumers about scam robocalls targeting older Americans, and DOJ announced that it charged 25 individuals for participating in the same scam that defrauded Americans out of more than $21 million in more than 40 states. The scammers made phone calls pretending to be an individual's grandchild who needed money for "bail" after being "arrested," or pretended to be the grandchild's "attorney," and were told they could not speak to anyone about the "arrest." This is one of the many heartbreaking examples of scams perpetrated on Americans by illegal robocallers and bad actors.

According to recent estimates, in April 2025, nearly 2,000 robocalls were placed to U.S. consumers every second. Spam and scam calls make consumers feel threatened, fearful, and distrustful of legitimate callers. As more and more Americans ignore calls from unknown numbers, they miss important calls. Moreover, fraud perpetuated against Americans by illegal robocalls costs an average of $25 billion annually, primarily affecting those who cannot afford such losses.

We are also seeing a lot of unwanted and scam robotexts, and AI generated phone calls and text messages, including voice clones and deepfakes. According to the FCC, consumer complaints about unwanted text messages increased 500-fold between 2015 and 2022. Americans are frustrated and understandably so.

In 2019, the bipartisan Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence—or TRACED Act—was enacted to help reduce the flood of illegal robocalls. The TRACED Act allowed the FCC and law enforcement to impose stricter penalties for intentional violations of the Telephone Consumer Protection Act, or TCPA;

improved adoption of technical solutions, like the STIR/SHAKEN call authentication framework; and established a federal interagency working group to combat illegal robocalls.

As a result, U.S. telecommunications carriers have made progress implementing STIR/SHAKEN into their networks. This framework authenticates that phone calls are coming from legitimate phone numbers, which helps reduce the number of spoofed and illegal robocalls. Generally, to operate within the U.S., voice service providers must now implement robocall mitigation programs and file these plans and their STIR/SHAKEN compliance certifications in the Robocall Mitigation Database overseen by the FCC. Moreover, in July 2020, the FCC recognized the U.S. Telecom Industry Traceback Group (ITG) as the single registered consortium to conduct private-led traceback efforts that identify the source of an illegal robocall.

The FCC has also taken measures to address the growing burden of unwanted and scam robotexts and abused AI technologies. Specifically, in March 2023, the agency adopted regulations targeting scam robotexts. In addition, industry actors have partnered with federal agencies to

launch new programs, such as robotext tracing. Lastly, in August, the FCC proposed rules to protect consumers from AI-generated robocalls and robotexts. These are steps in the right direction, and I applaud the coordination we've seen thus far.

While the TCPA has provided many useful tools, the TCPA's private right of action has given rise to class-action lawsuits focused on minor infractions, rather than the bad actors responsible for placing illegal robocalls and it has not reduced the number of illegal robocalls or improved consumer protection.

In addition, STIR/SHAKEN implementation among smaller carriers has been delayed and bad actors have exploited these providers' reliance on legacy infrastructure. Moreover, a majority of illegal robocalls and robotexts originate overseas making them hard to trace. Because these bad actors are outside the jurisdiction of U.S. law enforcement, they are challenging to combat.

Finally, the FCC must grapple with emerging technologies and navigate the best way to create appropriate guardrails for these technologies while simultaneously continuing to support innovation.

We will always have robocalls and robotexts because not all of them are illegal. Many are used for legitimate purposes by U.S. businesses and public entities, but we must continue finding ways to combat these unwanted communications.

I want to thank our panel of witnesses for joining us. I look forward to a robust discussion to understand the current landscape of illegal robocalls and robotexts plaguing U.S. consumers and businesses so we can work together to identify and address remaining challenges.

I now recognize the Ranking Member of the Subcommittee, Ms. Clarke, for her opening statement.

Mr. PALMER. I now recognize the ranking member of the subcommittee, Ms. Clarke, for her opening statement.

OPENING STATEMENT OF HON. YVETTE D. CLARKE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Ms. CLARKE. Thank you, Mr. Chairman, and I thank our panel of witnesses for appearing before us today.

Americans are tired of hundreds of unwanted calls and texts they receive every year from scammers attempting to steal their hard-earned money. In 2023, Americans lost over $25 billion to phone-based scams. These criminals target the vulnerable and kind-hearted by pretending to be law enforcement, Medicare, or even relatives in order to scam them out of hard-earned money. Enough is enough.

For years, there has been a bipartisan effort to address this issue. In 2019, Democrats and Republicans came together to pass the Pallone-Thune TRACED Act, giving the Federal Government greater enforcement ability and the authority to implement a call authentication framework and force phone carriers to improve the traceback of illegal calls.

Under the Biden administration, the Federal Communications Commission created the Robocall Response Team that has assisted in cutting off providers who facilitate illegal robocalls. And last year, Ranking Member Pallone led a Democratic package to close the loophole scammers rely on to target Americans. Committee Democrats are now working on updates to strengthen that package.

Unfortunately, the Trump administration and congressional Republicans are retreating from the fight against illegal robocalls and robotexts. Just last week, President Trump released his 2026 budget proposal, in which he recommends cutting $42 million and firing 83 people from the Federal Trade Commission. By the Trump administration's own definition, the mission of the FTC is to protect the public from unfair or deceptive business practices, including unlawful telemarketing and robocalls. How can we expect the Federal Government to do more to protect Americans when the Trump administration is firing the very people whose job it is to enforce the law?

Right now, law enforcement in all 50 States and the District of Columbia are combating robocalls. A bipartisan group of 40 State attorney generals wrote to Congress to say that their State laws regulating artificial intelligence help prevent spam phone calls and texts. But just a few weeks ago, Republicans on this committee voted for a reconciliation package that includes a 10-year moratorium on enforcement of State and local AI laws that these State attorney generals are opposed to. This provision stops States in their tracks from doing important work when we have not yet provided a Federal solution.

I think my Republican colleagues forget they are not the only elected officials in this country. State legislators and law enforcement work in tandem every day to stop these harassing robocalls and texts, and you should not stand in their way.

Stopping robocalls and texts will require dedicated employees at every level of government. Congressional Republicans should not

hamstring the efforts of State and local enforcement, and President Trump should not slash and burn the budgets and staff of Federal agencies, all of which are dedicated to serving the American people. We in Congress have a duty to our constituents. Committee Democrats are here to prioritize the will of the people who put us in these chairs, not prove our loyalty to Donald Trump.

If my Republican colleagues honestly want to stop illegal robocalls and robotexts, let's work together to support the Federal employees and agencies that work, instead of tearing them down.

Having said that, I thank you, and I yield back, Mr. Chairman.

[The prepared statement of Ms. Clarke follows:]

Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Subcommittee on Oversight and Investigations Ranking Member Yvette Clarke

Hearing on "Stopping Illegal Robocalls and Robotexts: Progress, Challenges, and Next Steps"

June 4, 2025

Thank you, Mr. Chairman. Americans are tired of the hundreds of unwanted calls and texts they receive every year from scammers attempting to steal their hard-earned money. In 2023, Americans lost over 25 billion dollars to phone-based scams. These criminals target the vulnerable and kind-hearted by pretending to be law enforcement, Medicare, or even relatives in order to scam them out of hard-earned money. Enough is enough.

For years there has been a bipartisan effort to address this issue. In 2019, Democrats and Republicans came together to pass the Pallone-Thune TRACED Act, giving the federal government greater enforcement ability and the authority to implement a call authentication framework and force phone carriers to improve the traceback of illegal calls. Under the Biden Administration, the Federal Communications Commission created the Robocall Response Team that has assisted in cutting off providers who facilitate illegal robocalls. And last year, Ranking Member Pallone led a Democratic package to close the loopholes scammers rely on to target Americans. Committee Democrats are now working on updates to strengthen that package.

Unfortunately, the Trump Administration and congressional Republicans are retreating from the fight against illegal robocalls and robotexts. Just last week President Trump released his 2026 budget proposal, in which he recommends cutting 42 million dollars and firing 83 people from the Federal Trade Commission. By the Trump Administration's own definition, the mission of the FTC is "to protect the public from unfair or deceptive business practices," including unlawful telemarketing and robocalls. How can we expect the federal government to do more to protect Americans when the Trump Administration is firing the very people whose job it is to enforce the law? Right now, law enforcement in all 50 states and the District of Columbia are combatting robocalls. A bipartisan group of 40 State Attorney Generals wrote to Congress to say that their state laws regulating artificial intelligence help prevent spam phone calls and texts. But just a few weeks ago, Republicans on this Committee voted for a reconciliation package that includes a 10-year moratorium on enforcement of state and local AI laws that those State Attorney Generals are opposed to. This provision stops states in their tracks from doing important work when we have not yet provided a federal solution. I think my Republican colleagues forget they are not the only elected officials in this country. State legislators and law enforcement work in tandem every day to stop these harassing robocalls and texts, and you should not stand in their way.

Stopping robocalls and texts will require dedicated employees at every level of government. Congressional Republicans should not hamstring the efforts of state and local law

enforcement and President Trump should not slash and burn the budgets and staff of federal agencies, all of which are dedicated to serving the American people.

We in Congress have a duty to our constituents. Committee Democrats are here to prioritize the will of the people who put us in these chairs, not prove our loyalty to Donald Trump. If my Republican colleagues honestly want to stop illegal robocalls and robotexts, let's work together to support the federal employees and agencies doing that work instead of tearing them down.

I yield back.

Mr. PALMER. The Chair now recognizes the chairman of the full committee, Mr. Guthrie, for 5 minutes for an opening statement.

OPENING STATEMENT OF HON. BRETT GUTHRIE, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF KENTUCKY

Mr. GUTHRIE. Thank you, Chairman Palmer, and I thank the Ranking Member Clarke. I thank you for holding this hearing. A lot of times, when we are back from our breaks away from home, people in DC ask us, "What are you hearing back home?" And I will tell you, I mean, of all the things going on in Washington, DC, one of the number-one things I hear is robocalls.

And I was sitting with a good friend of mine who is a little older, and just chatting with him for about an hour during the break. And I bet his phone rang four or five times. And each one was a robocall. So this is important. It is important to the American people. And it is not just because of the annoyance, it is because of the people that get ripped off with these people. And there are over 52 billion robocalls, and that is 4 billion calls a month, an average of 13 calls per person.

At the outset, I would like to state that many robocalls are both legal and necessary. Robocalls are used to convey public service announcements and emergency messages. They are used for announcing school closures and providing reminders of upcoming appointments and payments. These are the calls that we want.

But a large number of robocalls are illegal and are used to defraud, harass, and deceive customers. We have all received calls where someone on the other end of the line pretends to be IRS or Treasury and attempts to offer student loans or debt relief and sell insurance, or claims to be a bank or a credit card company. According to one survey, American victims of fraud lost an average of $450 to phone scams that prey on trust and exploit vulnerabilities. This exploitation is despicable, and the impact on victims is tragic, and many have lost their entire life savings. And we know this must stop.

And thankfully, in 2019, the committee passed the bipartisan bicameral legislation which President Trump signed into law, the Pallone-Thune TRACED Act, to combat the epidemic of illegal robocalls. And I was proud to vote for that. The TRACED Act is an important law that provides the FCC and its partners with greater enforcement authority to hold illegal robocallers and bad actors accountable.

Since the enactment of the TRACED Act, the FCC has used this authority to issue additional rules as well as civil and criminal penalties under the Telephone Consumer Protection Act. As a result, we have seen a downward trend in the prevalence of illegal robocalls.

In addition, the FCC continues to mandate the voice service providers implement STIR/SHAKEN, caller ID authentication technology, and provide robocall mitigation plans to the robocall mitigation database. Furthermore, in 2020, USTelecom's Industry Traceback Group, or ITG, was recognized as the single private consortium to trace back the origins of suspected illegal robocalls, helping us to stop these calls at their source. All together, we have

seen some great work done by our Federal agencies and their industry partners.

However, despite these strides forward, illegal and scam robocalls persist. We are even seeing a significant increase in unwanted scam and robotexts, which include messages alerting consumers to act on undeliverable packages and unpaid tolls, to name a few examples.

Complicating these issues are new developments in artificial intelligence, including voice cloning and deepfake technologies to impersonate individuals and generate scam phone calls and texts. Just last month, the FBI issued a warning about a malicious messaging campaign targeting government officials and their acquaintances by sending AI-generated voice messages impersonating senior U.S. officials to gain access to their data.

As challenges evolve, so too must solutions. The Committee on Energy and Commerce has been at the forefront of leading discussions, understanding challenges, and developing solutions to address issues with new technologies, and we will continue to do so throughout this Congress. Notwithstanding the complex landscape illegal scam robocalls and robotexts pose for customers, legitimate businesses, Federal agencies, and their partners, I am optimistic that Republicans and Democrats will continue to work together to develop commonsense, bipartisan solutions to protect the American people from these fraudsters.

And I want to thank the witnesses for being here today. Thank you for taking your time to be here. And I look forward to your testimonies. And I will yield back.

[The prepared statement of Mr. Guthrie follows:]

Chairman Brett Guthrie Opening Statement
Subcommittee on Oversight and Investigations
Stopping Illegal Robocalls and Robotexts: Progress, Challenges, and Next Steps
Wednesday, June 4, 2025 – 10:15 AM ET

Chairman Palmer, thank you for holding this important hearing. Illegal and scam robocalls are a constant source of annoyance and harm to millions of Americans. According to recent analysis, last year Americans received over 52 billion robocalls—that's over 4 billion calls each month and an average of 13 calls per person.

At the outset, I'd like to state that many robocalls are both legal and necessary. Robocalls are used to convey public service announcements and emergency messages. They are used for announcing school closures and providing reminders of upcoming appointments and payments. These are calls we want. But a large number of robocalls are illegal and are used to defraud, harass, and deceive consumers.

We've all received calls where someone on the other end of the line pretends to be from the IRS or the Treasury, attempts to offer student loans or other debt relief, sell health insurance, or claims to be from a bank or credit card company trying to alert you to "fraud" or "unauthorized activity" on your account. According to one survey, American victims of fraud lost an average of $450 to phone scams that prey on trust and exploit vulnerabilities. This exploitation is despicable and the impact on victims is tragic. Many have lost their entire life savings. This must stop.

Thankfully, in 2019, this Committee passed bipartisan, bicameral legislation, which President Trump signed into law—the Pallone-Thune TRACED Act—to combat the epidemic of illegal robocalls, which I was proud to support.

The TRACED Act is an important law that provides the FCC and its partners with greater enforcement authority to hold illegal robocallers and bad actors accountable. Since the enactment of the TRACED Act, the FCC has used its authority to issue additional rules, as well as civil and criminal penalties under the Telephone Consumer Protection Act (TCPA). As a result, we're seeing a general downward trend in the prevalence of illegal robocalls.

In addition, the FCC continues to mandate that voice service providers implement STIR/SHAKEN caller ID authentication technology and provide robocall mitigation plans through the Robocall Mitigation Database. Furthermore, in 2020, USTelecom's Industry Traceback Group, or ITG, was recognized as the single private consortium to trace back the origins of suspected illegal robocalls, helping us stop these calls at their source. Altogether, we have seen some great work done by our federal agencies and their industry partners.

Despite these strides forward, however, illegal and scam robocalls persist. We are even seeing a significant increase in unwanted and scam robotexts, which include messages alerting consumers to act on "undeliverable packages" and "unpaid tolls," to name a few examples.

Complicating these issues are new developments in artificial intelligence (AI), including voice cloning and deep fake technologies, to impersonate individuals and generate scam phone calls and texts. Just last month, the FBI issued a warning about a malicious messaging campaign targeting government officials and their acquaintances by sending AI-generated voice messages impersonating senior U.S. officials to gain access to their data.

As challenges evolve, so too must the solutions. The Committee on Energy and Commerce has been at the forefront of leading discussions, understanding challenges, and developing solutions to address issues with new technologies, and we will continue to do so throughout the Congress.

Notwithstanding the complex landscape illegal and scam robocalls and robotexts pose for consumers, legitimate businesses, federal agencies, and their partners, I am optimistic that Republicans and Democrats will continue to work together to develop common sense, bipartisan solutions to protect the American people from these fraudsters.

I want to thank the witnesses for being here today and I look forward to hearing your testimonies. I yield back.

###

Mr. PALMER. I thank the gentleman

The Chair now recognizes the ranking member of the full committee, Mr. Pallone, for 5 minutes for an opening statement.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. Thank you, Mr. Chairman.

Combating the surge of unwanted robocalls and robotexts has been a priority of mine for years. And, as I appreciate Chairman Guthrie saying, in 2009, I led passage of the TRACED Act. And this law has helped protect Americans from predatory and annoying robocalls and gave Federal agencies better tools to fight back against fraudsters.

Despite these steps, Americans are still continuously bombarded by unwanted calls and texts that are not only annoying but cause real harm through fraud and scams. Technological advancements have supercharged fraud and made it easier and less expensive for scammers to make massive numbers of robocalls, to spoof caller ID information in order to hide a caller's true identity. They also use artificial intelligence to trick consumers to thinking they are talking to a relative in financial trouble, or to a trusted business offering assistance.

Now, Americans received over 52 billion robocalls in 2024, which is nearly 200 calls for every American adult. Scams targeting seniors are especially rampant and take many forms, including calls or texts claiming to be from grandchildren or law enforcement or Medicare, all aimed at bilking money from the senior citizen. And robotexts are increasingly problematic, using automated text messages that trick recipients into clicking damaging links, providing personal or financial information, or paying for fraudulent items or services.

And Congress has to continue to update the authorities we have given both to the FTC and the Federal Communications Commission to crack down on robocalls. We must also consider legislation focused on robotexts and provide our consumer protection agencies with adequate funding and staffing to hold bad actors accountable.

The TRACED Act gave the FCC increased authority to require carriers to implement a call authentication framework, and stepped up enforcement action against bad actors and directed carriers to develop better tools to protect their customers. But as technology evolves, fraudsters are finding new ways to scam Americans and abuse loopholes.

So last Congress, I led a Democratic effort that would expand antirobocall protections and provide explicit protections against robotexts. And our bill also would have closed loopholes exploited by scammers, combated the use of AI for scams, and alleviated the robocall-blocking technology for consumers. My colleagues and I are working on updates to strengthen that package, and I am sure today's testimony will help inform our thinking on how to better protect consumers from unwanted robocalls and robotexts.

Now, I am sure there is uniform agreement on this committee that it is important to put an end to harassing and illegal robocalls and robotexts. But I have to say that actions by the Trump admin-

istration do threaten our efforts to do just that. There is a regular effort to undermine—essentially what is happening is the Trump administration and, of course, the House Republicans, you know, are cutting funding and staff from the very entities that protect consumers. And, you know, this is all to give the big tax breaks to billionaires who do not need them.

And the problem is that, while law enforcement and State governments have been active in combating robocalls and on working with industry to find technical solutions to address robocalls, last month the House Republicans supported the reconciliation bill that included a 10-year moratorium on State and local enforcement of their own AI laws.

So if this Big Tech effort becomes law, it could stop State attempts to develop innovative solutions to prevent illegal robocalls and texts. And I think it compromises America's financial well-being and hamstrings States who are working to keep their citizens safe.

Federal consumer protection agencies are vital components of this fight against the robocalls and robotexts. But since taking office, President Trump has attempted to remove Senate-confirmed FTC Commissioners, reduce FTC and FCC staff, and that cripples these two important agencies' efforts to protect consumers. And Democrats have advocated for stronger authority and resources for both the FTC and the FCC, and for sensible guardrails to ensure consumer safety is at the forefront of strong enforcement by Federal, State, and private partners. But House Republican budgets that have all these cuts, they are basically underresourcing these agencies and the staff that would actually use the tools we have given them to fight against robocalls.

So, you know, I have to say, you know, obviously, this is not the way to protect consumers. And, you know, I always worry—and I am almost out of time, Mr. Chairman, but I just worry that, you know, whether it is the SUPPORT Act that is on the floor this week or it is your efforts to talk about the need to address robocalls and texts, if you do not have the resources, if you do not have the staff, and the money is cut for these agencies, then it is not going to be effective, no matter what we do as an authorizing committee. And I am going to continually point that out because I think it is important.

I yield back, Mr. Chairman.

[The prepared statement of Mr. Pallone follows:]

Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Ranking Member Frank Pallone, Jr.

Hearing on "Stopping Illegal Robocalls and Robotexts: Progress, Challenges, and Next Steps"

June 4, 2025

Combating the surge of unwanted robocalls and robotexts has been a priority of mine for years. In 2019, I led the passage of the Pallone-Thune TRACED Act. This law has helped protect Americans from predatory and annoying robocalls and gave federal agencies better tools to fight back against fraudsters.

Despite these steps, Americans are still continuously bombarded by unwanted calls and texts that are not only annoying but cause real harm through fraud and scams. Technological advancements have supercharged fraud and made it easier and less expensive for scammers to make massive numbers of robocalls, to "spoof" caller ID information in order to hide a caller's true identity. They also use artificial intelligence (AI) to trick consumers into thinking they are talking to a relative in financial trouble or to a trusted business offering assistance.

Americans received over 52 billion robocalls in 2024—which is nearly 200 calls for every American adult. Scams targeting seniors are especially rampant and take many forms including calls or texts claiming to be from grandchildren, or law enforcement, or Medicare – all aimed at bilking money from the senior citizen.

Robotexts are increasingly problematic, using automated text messages that trick recipients into clicking damaging links, providing personal or financial information, or paying for fraudulent items or services.

Congress has to continue to update the authorities we've given both the Federal Trade Commission and the Federal Communications Commission to crackdown on robocalls. We must also consider legislation focused on robotexts, and provide our consumer protection agencies with adequate funding and staffing to hold bad actors accountable.

The TRACED Act gave the FCC increased authority to require carriers to implement a call authentication framework, stepped up enforcement action against bad actors, and directed carriers to develop better tools to protect their customers.

As technology evolves, however, fraudsters are finding new ways to scam Americans and abuse loopholes. Last Congress, I led a Democratic effort that would expand anti-robocall protections and provide explicit protections against robotexts. Our legislation would have also closed loopholes exploited by scammers, combated the use of AI for scams, and alleviated the cost of robocall-blocking technology for consumers. My colleagues and I are working on

updates to strengthen that package and I am sure today's testimony will help inform our thinking on how to better protect consumers from unwanted robocalls and robotexts.

While I'm sure there is uniform agreement on this Committee that it is important to put an end to harassing and illegal robocalls and robotexts, actions by the Trump Administration threaten our efforts to do just that. Republicans are regularly undermining efforts to address these threats, cutting funding and staff from the very entities that protect consumers, all to give giant tax breaks to billionaires who don't need them.

While law enforcement and state governments have been active in combating robocalls and on working with industry to find technical solutions to address robocalls, last month House Republicans supported the GOP Tax Scam that included a 10-year moratorium on state and local enforcement of their own AI laws. If this giant giveaway to Big Tech becomes law, it could stop state attempts to develop innovative solutions to prevent illegal robocalls and texts. It compromises Americans' financial well-being and hamstrings states who are working to keep their citizens safe.

Federal consumer protection agencies are vital components in the fight against robocalls and robotexts. But, since taking office, President Trump has attempted to illegally remove Senate-confirmed FTC Commissioners from their positions and has reduced FTC and FCC staff, crippling these two important agencies' efforts to protect consumers.

Democrats have advocated for stronger authority and resources for the FTC and FCC and for sensible guardrails to ensure consumers' safety is at the forefront of strong enforcement by federal, state, and private partners. But House Republicans have proposed budgets with devastating cuts to already under-resourced agencies. This is not the way to protect consumers.

And with that I yield back the balance of my time.

Mr. PALMER. I thank the gentleman.

That concludes Member opening statements. The Chair would like to remind Members that, pursuant to the committee rules, all Members' written opening statements will be made part of the record.

We want to thank our witnesses for being here today and taking time to testify before the subcommittee. You will have the opportunity to give an opening statement followed by a round of questions from the Members.

Our witnesses today are Joshua Bercu, executive director for Industry Traceback Group and senior vice president of USTelecom; Ms. Sarah Leggin, vice president of regulatory affairs for CTIA; Mr. Stephen Waguespack, president of the Institute for Legal Reform and senior vice president of the U.S. Chamber Federation, State and local advocacy, at the U.S. Chamber of Commerce; and, finally, Mr. Ben Winters, director of AI and data privacy for the Consumer Federation of America.

We appreciate you being here today, and I look forward to hearing from you.

You are aware that the committee is holding an oversight hearing and, when doing so, has the practice of taking testimony under oath. Do any of you have any objection to testifying under oath?

Seeing no objection, we will proceed.

The Chair advises you that you are entitled to be advised by counsel pursuant to House rules. Do you desire to be advised by counsel during your testimony today?

Seeing none, please rise and raise your right hand.

[Witnesses sworn.]

Mr. PALMER. Seeing the witnesses answered in the affirmative, you are now sworn in and under oath, subject to the penalties set forth in title 18, section 1001 of the United States Code.

You may be seated.

With that, we will now recognize Mr. Bercu for 5 minutes to give an opening statement.

STATEMENTS OF JOSHUA M. BERCU, EXECUTIVE DIRECTOR, INDUSTRY TRACEBACK GROUP, AND SENIOR VICE PRESIDENT, USTELECOM; SARAH LEGGIN, VICE PRESIDENT, REGULATORY AFFAIRS, CTIA; STEPHEN WAGUESPACK, PRESIDENT, INSTITUTE FOR LEGAL REFORM, SPECIAL COUNSEL, U.S. CHAMBER OF COMMERCE; AND BEN WINTERS, DIRECTOR OF AI AND PRIVACY, CONSUMER FEDERATION OF AMERICA

STATEMENT OF JOSHUA M. BERCU

Mr. BERCU. Chairman Palmer and members of the subcommittee, thank you for the opportunity to testify today. Congress's leadership in passing the TRACED Act and maintaining strong oversight remains critical to ensuring that industry and government act with urgency to address this top consumer concern. Your commitment remains vital to sustain the vigilance, innovation, and coordination needed in our continued and evolving fight against scam calls.

I am Josh Bercu, executive director of the Industry Traceback Group, or ITG, which is the FCC-designated traceback consortium under the TRACED Act, and senior vice president at USTelecom.

Let me start with the bottom line: The TRACED Act worked. When Congress passed the TRACED Act, robocall complaints were nearing a crisis point, doubling at the FTC from 1.7 million in 2014 to nearly 4 million in 2019. Today, they are down more than 70 percent. FCC complaints are down 77 percent. That's real progress. It did not solve everything, but we now have tools and a mandate to fight back.

Over the past 6 years, we have built a framework that makes it harder and riskier for bad actors and criminals to infiltrate our networks. But it is neither hard nor risky enough, and the threat is evolving. Fraud losses are rising, not because of mass robocalls but because of targeted, more sophisticated scams. We have gone from fishing with dynamite to precision strikes. And that demands a more agile defense.

That is where traceback has come in. Since its inception, the ITG has conducted over 20,000 tracebacks. We help identify who's behind illegal calls, whether it is a robocall campaign, a spoof threat to a high school, or a scam impersonating a bank. Our work supports law enforcement and drives action.

When a rural high school in West Virginia received a threatening call, we worked with providers to trace the call path within hours, helping police confirm the call was not actually made locally, and safely reunite families.

The tools Congress empowered are as essential now as ever. Call blocking and labeling stops millions of illegal calls every day. Call authentication has made it far harder for bad actors to spoof numbers at scale. And pursuant to the TRACED Act, FCC rules now require all providers to know where their traffic comes from and take action when it is identified as unlawful, including through our tracebacks. The threat is evolving, so we need to keep evolving with the threat.

The good news? We're not starting from scratch. Here are three things we think Congress can do to help:

One, build a unified national scam strategy. We need a national strategy and a central Federal coordinator or task force to unify efforts, eliminate silos, and give industry a clear point of contact. That strategy should include international cooperation, including on traceback. We also need to treat call-based scams for what they are: crime. And it's crime that can only be fully stopped through cross-border criminal enforcement.

Two, strengthen the tools that work. Let's reinforce the existing framework, extend the FCC's traceback designation cycle, and provide narrow immunity so we can plan, invest, and act decisively without being distracted or deterred by an annual administrative process or the risk of nuisance lawsuits. We've also worked on new tools to explore other aspects of unlawful calling campaigns and, with congressional backing, they could become permanent and powerful parts of the tool set.

Three, unleash and promote cross-sector collaboration. Some of the most meaningful progress we've made has come from collaboration. We've launched a pilot with banks and carriers to trace

spoofed numbers pretending to be the banks, a model of the cross-sector collaboration we need more of.

But barriers can get in the way. Right now, providers may hesitate to share intelligence simply because rules and risks are not clear. A narrowly scoped safe harbor could change that, clarifying that sharing information to prevent fraud is not only allowed but encouraged. Blame will not stop fraud, but partnerships can. The TRACED Act was a turning point, but we need to keep adapting and fighting back.

Thank you for your leadership. I look forward to your questions.

[The prepared statement of Mr. Bercu follows:]

Prepared Testimony of Joshua M. Bercu
Executive Director, Industry Traceback Group
Senior Vice President, Policy, USTelecom — The Broadband Association
Before the House Energy & Commerce, Oversight and Investigations Subcommittee
Hearing on "Stopping Illegal Robocalls and Robotexts: Progress, Challenges, and Next Steps"

I. Introduction

Chairman Palmer, Ranking Member Clarke, Chairman Guthrie, Ranking Member Pallone, and Members of the Subcommittee:

Thank you for the opportunity to testify today and reflect on the progress we've made — and the challenges we still face — six years after the TRACED Act became law. Congress' leadership in passing the TRACED Act and maintaining strong oversight remains critical to ensuring the industry and government act with urgency to address this top consumer concern. Your commitment remains vital to sustaining the vigilance, innovation, and coordination needed in our continued and evolving fight against scam calls.

I'm Josh Bercu, Executive Director of the Industry Traceback Group, or ITG, and Senior Vice President of Policy at USTelecom — The Broadband Association. For nearly ten years, USTelecom has led the ITG, which has served as the designated registered traceback consortium since the enactment of the TRACED Act. We've spent the last several years scaling our work while partnering with federal and state enforcement agencies, innovating to meet a constantly shifting threat, and building the operational foundation to help identify and disrupt illegal calls.

The headline is this: the TRACED Act worked. It created an evolving framework that now enables disruption of illegal calling campaigns, better accountability, and targeted enforcement. The result is a communications ecosystem where it is meaningfully harder and riskier for bad actors to reach American consumers.

The reality, however, is that no single law or tool can solve all of our challenges. Fraud losses are growing as tactics are evolving. Today's fraudsters are using automation and deception to launch smarter, more targeted attacks that can do just as much if not more harm.

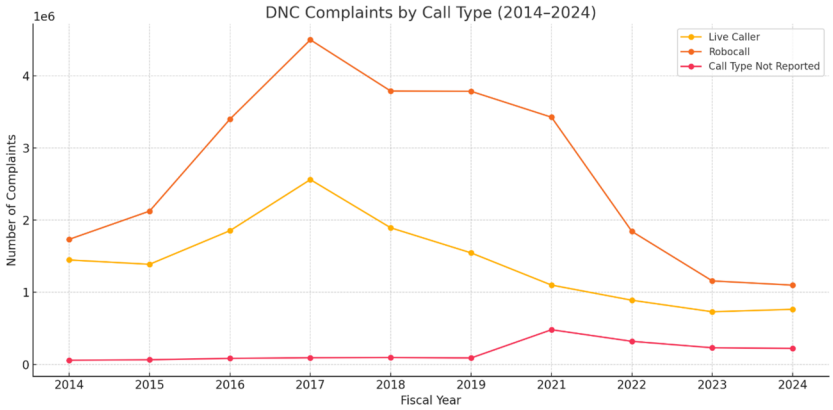
The good news is that the TRACED Act gave us a framework designed to evolve — if we keep investing in the tools that work.

II. TRACED Act Scorecard: Improved Tools Delivering Real Progress

So how well is that framework working? The numbers tell a compelling story. When Congress passed the TRACED Act in late 2019, illegal robocalls were nearing a crisis point. Robocall complaints at the FTC had more than doubled from about 1.7 million in 2014 to 4.5 million in 2017, and stayed just shy of 4 million prior to the TRACED Act's passage. The robocalls leading to these complaints were typically high-volume campaigns that predominantly used spoofed

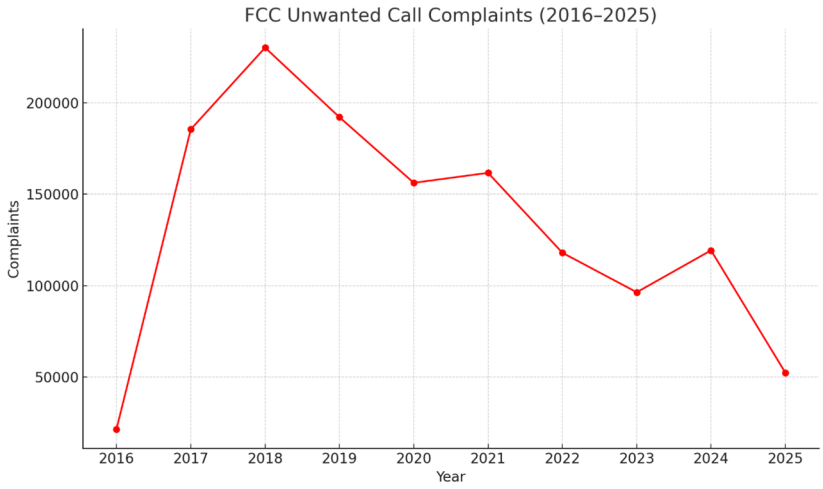
numbers, and automated and prerecorded voice messages at their core. Past illegal robocall campaigns were part of large-scale "fishing with dynamite" scams or illegal telemarketing schemes that exploited regulatory gaps and weaknesses in the phone network.

As of today, those complaints have declined by more than 70%.



Source: FTC Do Not Call Complaint Data

And it's not just the FTC data telling that story. FCC complaints about unwanted calls peaked in 2018 at over 230,000. As of 2025, they are down more than 77%.



Source: FCC Unwanted Call Complaint Data

Scam robocalls are also down significantly from their March 2021 peak, according to data from YouMail, with 2025 volume of scam robocalls about 50% lower.

These reductions represent real and measurable progress, even while volumes remain too high — a challenge that demands continued vigilance across industry and government.

The progress demonstrates how an adaptive, public-private model can scale to meet evolving threats, while also powering meaningful enforcement by agencies like the FCC, FTC, DOJ, and state attorneys general.

Although the TRACED Act didn't create the preceding industry-led initiatives such as traceback, call authentication, and the other tools now widely deployed across the network, as those efforts were already underway, it supercharged them. It gave the FCC new tools and helped align industry and government around a shared strategy. More importantly, it gave that strategy staying power. And today, that's what allows us to scale the defenses that work.

These tools provide a critical layer of consumer protection:

- **Call blocking and labeling**. Thanks to analytics engines and provider-side investments, millions of illegal and unwanted calls are blocked each day before they ever ring on a consumer's phone. Labeling tools have also become an essential part of the defense model, warning consumers in real time when calls may be fraudulent or spam.
- **Caller ID authentication through STIR/SHAKEN.** Since its deployment, we've seen a reduction in large-scale spoofing campaigns. It is far harder today to get a spoofed call to a consumer than it was when the TRACED Act was enacted.
- **Robocall Mitigation Database (RMD).** Authentication is just part of the new accountability framework. The FCC's RMD, combined with the agency's know-your-customer and know-your-upstream-provider requirements, has been instrumental. Providers now have an affirmative obligation to understand where their traffic comes from and to act if and when they learn it's unlawful. This, combined with the FCC's ability to delist noncompliant providers from the Robocall Mitigation Database or direct others to block their traffic — cutting them off from the phone network — gives real teeth to the regime.
- **Traceback.** Giving formal status to this tool under the TRACED Act has been indispensable. It transformed a voluntary industry initiative into a formal public-private partnership function. Since the law's passage, the FCC has designated the Industry Traceback Group as the official consortium six consecutive times, reinforcing the central role the ITG plays in combatting illegal calls. That work has grown dramatically in scope, speed, and impact, as described in more detail below.

None of this progress would have been possible without significant industry investment and innovation — not just in new technologies like call authentication and call analytics, but also in operational infrastructure and cross-sector collaboration. The industry has committed time,

resources, and expertise to support a layered defense model, develop scalable mitigation tools, and partner with law enforcement agencies, analytics firms, and other industries. These efforts are not just reactive; they reflect a proactive, long-term commitment to safeguarding consumers in an increasingly complex threat environment.

Six years after the TRACED Act was signed into law, the tools it empowered — like traceback, robocall mitigation, call authentication, and call blocking — are now key components of the anti-robocall toolkit. Together with aggressive enforcement, these tools are delivering real results.

III. Traceback: A Nimble Tool in a Shifting Landscape

In this shifting threat landscape — where attacks are more targeted and harder to identify — traceback has proven uniquely effective and adaptable. Over the past six years, it has become a scalable and flexible way to identify unlawful callers and disrupt illegal calling campaigns.

Consistent with the framework established in the TRACED Act, the ITG operates a neutral process that pieces together a call path across sometimes half a dozen or more providers. We begin with a suspicious call, sourced by analytics engines, honeypots, or referrals from law enforcement or industry. We then request upstream provider information one hop at a time through a semi-automated process. Because each provider knows only who sent them the call, this step-by-step process is essential to uncover the origin. And when we do, we're able to identify not only the call's origin but also the responsible entity. What once took months, we now do in a matter of hours or days.

What makes traceback so effective is its flexibility. We trace a wide range of call types — from traditional scam robocalls, to lead generation campaigns relying on falsified consent, to live voice phishing (vishing) attacks, school threats, and telephone-denial-of-service (TDoS) attacks.

Since the ITG's inception, we have conducted over 20,000 tracebacks, representative of billions of suspected illegal calls. Our data has supported enforcement by the DOJ, FCC, FTC, and state attorneys general. Just as importantly, the majority of completed tracebacks result in the originating provider taking action, including terminating the customer responsible.

And the impact is not abstract — it's real. Just last month, we were contacted by the West Virginia State Police following a threat to a rural high school. The threatening call was anonymous, and law enforcement lacked the information to identify which provider to contact. Normally, in cases like this, we direct law enforcement to the public safety teams that carriers maintain — they're better equipped to handle and respond to urgent threats. But in this case, there wasn't enough data to make that handoff. So we launched a traceback, worked with providers in the call path, and identified the originating provider and the calling number. Within hours, we connected law enforcement with the right contact. The ITG's efforts helped them to quickly determine the call wasn't local, enabling local enforcement to safely clear the school and safely reunite students with their families.

With respect to consumer financial losses, the ITG is also piloting a project with several major banks and carriers to identify when a bank's number has been spoofed, launch tracebacks based on that data, and help identify other potential victims. The pilot has already shown real impact, and we believe it can serve as a model for enhanced cross-sector collaboration — demonstrating how the ITG and traceback can evolve to meet new and ever-changing threats.

Given that illegal robocalls are global in scope and sometimes originate from overseas, international coordination is another essential frontier. The ITG has identified roughly 2,000 voice service providers from 75 countries in traceback. We are actively engaging with industry and regulators abroad to explore alignment around traceback and related fraud mitigation strategies. These discussions have provided valuable insight into how other jurisdictions are confronting the same challenges, often perpetrated by the same bad actors. This kind of global coordination is not just beneficial — it is increasingly necessary to meet a global threat.

IV. The Modern Threat Landscape

But success breeds adaptation. And while we've cut off many of the old attack vectors, today's threats are resilient, more obfuscated, and far more personal. The illegal call problem isn't static — it's evolving.

For example, some bad actors have adapted by shifting to "number rotation," where they rapidly cycle through thousands of real, assigned telephone numbers and use each number just once or twice to avoid triggering detection systems. It's a cat-and-mouse game, and while consumers benefit from the protections in place, legitimate callers sometimes find their calls misidentified, and fraudsters still find ways to break through. These bad actors have also adjusted their tactics to exploit some elements of the RMD. They use shell company networks to onboard with U.S. providers using throwaway domains and misleading credentials to appear legitimate and domestic. In some cases, they even impersonate legitimate providers. Once detected, they quickly abandon their existing shell company and reappear under a new name. The intent is clear: inject traffic, vanish, and reset. While the RMD provides a foundation for identifying these entities, we need faster, more decisive action to take down entire networks — and prevent them from resurfacing under a different LLC the next day.

While scam robocalls have declined, fraud has not. It's shifted.

Today's fraudsters aren't blasting millions of calls impersonating the Social Security Administration. They're shifting from high volume to high impact by targeting specific individuals often with live calls, stolen data, and finely tuned deception. They spoof bank numbers and pose as fraud teams. They script emotional appeals. They impersonate loved ones, local officials, or public safety agencies. And they don't need volume to succeed just the right target. They rely on maliciously building trust with the victim and they use that trust to steal their money, information, and peace of mind.

These scams — including those that begin through channels and platforms outside the voice network — are driving the 25%-30% increase in fraud losses last year, depending on whether you look at FBI or FTC data. That rise isn't driven by robocalls. It's driven by increasingly targeted and sophisticated fraud.

This evolving threat is an increasing focus for the ITG. The number of tracebacks we conducted involving targeted, live scam calls more than doubled last year — rising from 607 in 2023 to over 1,400 in 2024. As the threats evolve, the ITG is evolving too – just a few years ago, we weren't specifically tracing these types of calls.

Spoofing remains part of the criminal fraudster's playbook, even as overall volumes decline. We continue to fight spoofed calls impersonating banks, government agencies, and emergency services. These aren't meant to flood the network — they're meant to reach individuals at moments of heightened vulnerability and prompt them to act before they think.

SIMBoxes add another layer of complexity. These devices are deployed domestically and allow scammers to simulate thousands of unique mobile phone identities. To a carrier, they usually look like thousands of individual callers rather than one high-volume source, making them harder to prevent. They enable bad actors to place large volumes of calls from within the U.S. — even when the real perpetrators are sitting in call centers abroad.

But there's a silver lining. SIMBox operations are more expensive and effort-intensive than simple VoIP-based attacks — and they typically require someone physically present in the United States. That adds friction to the scam. And it gives us something much more valuable: someone we can more easily put in handcuffs. We've begun working successfully across the industry and with law enforcement partners to share information — and turn that intelligence into enforcement.

Meanwhile, AI is further blurring the line between robocalls and live scams. Criminals and other illegal callers can now use AI voice tools that mimic human interaction — pausing, laughing, apologizing, or asking how your day is going. These cheap and convincing tools are already being used by criminals and other bad actors. While STIR/SHAKEN and analytics can stop some of this activity, the core challenge remains: a growing volume of targeted, sophisticated attacks that are harder to detect, and often more damaging.

We do not sit by while criminal bad actors adapt. Rather, we are constantly evolving our own tactics and methods to counter them. But the industry is not law enforcement. Strengthening the public-private partnership in this space is one of the best ways the U.S. government can assist us.

V. What Congress Can Do

The reality is this: fraud evolves quickly, and regulation moves slowly. We cannot legislate or regulate our way out of every new scam tactic. That's not a sustainable model. What we need is a

framework that is nimble, targeted at the actors actually causing harm, and supportive of tools that work.

There are five things Congress can do that would make a difference.

- **Establish a national strategy for scams with a central scam coordinator at the federal level.** We need a unified, whole-of-government approach that elevates scams as a policy and enforcement priority. A designated lead or task force would provide industry a clear point of contact, improve coordination, eliminate silos, and drive faster, more consistent action against evolving threats.
- **Increase support for and prioritize criminal enforcement.** Most of the actors we identify in tracebacks on are not confused marketers. They're criminals or other malicious actors — often operating transnationally — who care little for compliance and are not deterred by fines. Prioritizing resources for training, prosecution, and investigations and expanding cross-border enforcement coordination will help deliver real deterrence.
- **Reinforce the traceback framework.** Congress should extend the FCC designation cycle from one year to five**.** The current process consumes substantial resources, both for the agency and for the consortium, and introduces uncertainty that complicates long-term investment. Congress should also provide targeted immunity for the registered consortium from nuisance lawsuits — not from accountability, but from litigation designed to undermine the traceback process and divert resources.
- **Support complementary tools like trace-forward and number trace.** Trace-forward helps identify who is on the other end of a scammer's callback number, even when call-forwarding or masking tools are used. Number trace uncovers how bad actors obtain and rotate through real phone numbers at scale. The ITG already conducts trace-forwards and is designing a number trace pilot, but neither of these efforts are endorsed in law or regulation to date — but they should be.
- **Provide a safe harbor for improved fraud prevention and detection.** Right now, privacy regulation can inhibit telecom providers from using and, where appropriate, sharing data that could help identify and stop fraud. A well-scoped safe harbor could unlock collaboration across the internet ecosystem to better prevent consumer harm and accelerate threat detection.

VI. Conclusion

The TRACED Act wasn't the end of the robocall problem — and it wasn't meant to be. But it gave us the structure we needed to respond with speed, creativity, and coordination. Thanks to that structure, we're seeing significant progress. Calls are being blocked. Bad actors are being identified. And enforcement agencies are acting faster and with greater precision than ever before.

At the same time, fraud is getting worse. It's more targeted, more convincing, and more scalable. Law enforcement needs targeted, well-coordinated resources to respond at scale and protect American consumers and businesses. And that makes our continuing work even more important.

The good news is we're not starting from scratch. We have the tools. We have the partnerships. And we have the commitment — across industry and government — to keep fighting back. What we need is the continued support of Congress to ensure we can adapt as fast as the threat does.

Thank you for your time, and I look forward to your questions.

Mr. PALMER. The Chair now recognizes Ms. Leggin for 5 minutes for your testimony.

STATEMENT OF SARAH LEGGIN

Ms. LEGGIN. Chairmen Palmer and Guthrie, Ranking Members Clarke and Pallone, and members of the subcommittee, on behalf of CTIA and the wireless industry, thank you for the opportunity to testify today.

CTIA commends the committee for its leadership in protecting Americans from the scourge of illegal and unwanted robocalls and robotexts. Consumers rely on wireless more than ever for voice calls and text messaging. As reported last year, Americans devoted nearly 2.4 trillion minutes to voice calls, and they exchanged more than 2.1 trillion text messages. And texts have a 98 percent open rate, evidencing just how much consumers open and read and trust their texts.

Unfortunately, bad actors know how much consumers value and rely on wireless voice and text messages. As they have increased their deceptive efforts, we have increased our efforts and our success in combating them. So today, first, I want to talk about how we are working to stop robocalls, and then I will turn to the similar but different challenges we face when it comes to robotexts.

First, on robocalls, we appreciate the committee's actions through the TRACED Act to provide the FCC with new tools to combat illegal robocalls. Under this framework, the wireless industry is helping lead the way in advancing consumers' control over the voice calls they receive. Although automated calls from your pharmacy, school, or charity can be helpful and enhance consumer welfare, too many of them are intrusive and a consumer pain point.

In response, the wireless industry has built a range of defenses against illegal and unwanted robocalls. We spearheaded the development of STIR/SHAKEN authentication framework, led the way in implementing it, as the TRACED Act directed. In addition, wireless providers and their partners have launched a variety of powerful tools to regain consumer control over the calls they receive. These include know-your-customer practices, innovative call blocking, tracing back illegal robocalls to identify bad actors, and robust robocall mitigation programs.

Wireless providers black label or identify over 45 billion scam calls every year while also working hard to make sure that legitimate calls are completed. Thanks to these efforts, robocall complaints reached a 6-year low last year. And we look forward to continuing progress there.

Now, turning to text messaging. Wireless text messaging is one of the most popular and trusted forms of communication among American consumers today. The wireless industry and our partners in the messaging ecosystem work really hard to keep it that way. To do so, we use proactive, multilayered measures that include tools like up-front vetting and verification, sophisticated machine learning and AI for filtering and blocking, and consumer reporting, all balancing the need to protect consumers and ensure that legitimate texts go through.

As just one metric, wireless providers blocked over 55 billion texts last year while at the same time delivering trillions of legiti-

mate texts. And we are always evolving our techniques to leverage the latest technology and meet new challenges. We complement these tools with best practices that offer industry-led guidance to honor consumer preferences focused on consent while supporting legitimate communications. The best practices are adopted throughout the messaging ecosystem and were recognized by a coalition of consumer advocate organizations as a critical element in protecting consumers and the messaging platform from bad actors.

Notwithstanding all these efforts, bad actors continue to try to exploit consumers' trust by spamming and scamming them. So to better target those bad actors, CTIA launched the Secure Messaging Initiative, or the SMI, to convene the texting ecosystem to help identify scam activity and refer it to law enforcement for investigation. Through the SMI, we've already traced over 172,000 robotexts and made over a dozen referrals to our law enforcement partners at the FCC, FTC, DOJ, and 50-State attorney general enforcement task force. These focused on scams like student loans, government and bank impersonation, package delivery, and more. Collectively, these efforts are helping to stop scammers and maintain consumer trust in text messaging.

Collaboration with our government partners is key to continued success, and we support the administration's efforts to protect consumers. Chairman Carr at the FCC has made cracking down on illegal robocalls a top priority, and we support this effort. And we acknowledge Ranking Member Pallone's Do Not Disturb Bill with the goal of combating consumer fraud.

Finally, we encourage Congress to take steps to support action against the bad actors behind illegal robocalls and robotexts. Many agencies are working hard to fight consumer fraud but lack the personnel or resources to bring cases. To help out, Congress could have agencies report on their current consumer fraud resources and actions and leverage that information to prioritize support. With more resources at the Federal and State levels, Congress can help take bad actors off the field and stop illegal robocalls and robotexts at the source.

Thank you for the opportunity to testify today. We look forward to working with you all to protect consumers from intrusive and illegal robocalls and robotexts.

[The prepared statement of Ms. Leggin follows:]

Testimony of

Sarah Leggin
Vice President, Regulatory Affairs
CTIA

on

Stopping Illegal Robocalls and Robotexts: Progress, Challenges, and Next Steps

Before the

U.S. House of Representatives Committee on Energy & Commerce
Subcommittee on Oversight & Investigations

June 4, 2025

Chairmen Palmer and Guthrie, Ranking Members Clarke and Pallone, and Members of the Subcommittee, on behalf of CTIA and the wireless industry, thank you for the opportunity to testify today.

CTIA commends the Energy and Commerce Committee for its leadership in protecting Americans from the scourge of illegal and unwanted robocalls and robotexts. Thanks to this Committee's actions, the TRACED Act provided the Federal Communications Commission ("FCC") with new tools to combat illegal robocalls. Under this framework, the wireless industry is helping lead the way in advancing consumers' control of the voice calls they receive. And with your support, the wireless industry is combatting billions of spam and scam text messages each month using innovative solutions that are helping prevent bad actors from corrupting the trusted environment of text messaging. We balance these steps with our ongoing support for legitimate calls and messages to help ensure that consumers get the communications they want.

Consumers rely on wireless more than ever before for voice calls and text messaging. As reported last year, Americans devoted nearly 2.4 trillion minutes to voice calls, and they exchanged more than 2.1 trillion text messages, or more than 67,000 messages every second – and texts have a 98 percent open rate, evidencing how much consumers read and trust their texts. Unfortunately, bad actors know how much consumers value and rely on wireless voice and text messages. As they have increased their deceptive efforts, we have increased our efforts and our success in combatting them. As just one example, wireless providers blocked

over 55 billion scam and spam texts in 2024, while at the same time ensuring trillions of legitimate texts go through.

Of course, there is more to do. And working together with Members of this Committee, the FCC, the Federal Trade Commission ("FTC"), the Department of Justice ("DOJ"), state attorneys general, and our partners throughout the voice and text messaging ecosystems, we are making headway in fighting bad actors and maintaining consumer trust in voice services and text messaging.

The Wireless Industry is Helping to Lead the Fight Against Robocalls.

Although automated calls from banks, pharmacies, airlines, schools, and others can enhance consumer welfare, too many automated calls are intrusive. We all know the type – a call that comes with a robotic or familiar voice and an enticing offer or one that tries to scam us into disclosing personal data. These calls are consumer pain points.

In response, wireless providers spearheaded the development of the STIR/SHAKEN framework years ago and led the way in implementing it, consistent with the directives of the bipartisan TRACED Act. As this Subcommittee is aware, STIR/SHAKEN helps identify callers and reduce caller ID spoofing as a key part of the industry's multipronged defense against illegal and unwanted robocalls. Congressional adoption and the FCC's implementation of the TRACED Act ensured this framework is now a critical component throughout voice networks, and STIR/SHAKEN has been a key step to restoring consumer trust in voice services.

Complementing STIR/SHAKEN, wireless providers and their ecosystem partners launched a range of powerful tools to regain consumer control over the calls they receive. These include robust know-your-customer practices, innovative call-blocking, tracing back illegal robocalls to identify bad actors, and robust robocall mitigation programs. AT&T's ActiveArmor, for example, features automatic fraud and spam call blocking and is included free with its plans. T-Mobile offers a variety of tools including Scam ID and Scam Block as well as a free Scam Shield app to help consumers identify and stop unwanted calls. Verizon engages in network-level blocking of highly-suspect traffic based on analytics and also offers Call Filter, an enhanced call labeling and blocking service, at no charge. In fact, wireless providers block, label, or identify over 45 billion scam calls each year while also working hard to ensure legitimate calls are completed. The FCC has recognized the success of these solutions and encouraged all voice service providers to take similar actions, using powerful analytic tools to complete legitimate calls while increasingly blocking illegal calls.

CTIA and its wireless partners are embarking on the next generation of call authentication – Branded Calling. We know that the majority of calls from unknown numbers are not answered today, and consumers are more likely to answer and engage with a call if they know the brand name of the caller. CTIA has developed a branded calling solution that leverages the STIR/SHAKEN framework to deliver trusted visual information to consumers' smartphones that helps assure them that a call is coming from a verified source. This solution is called Branded Calling ID™ – or "BCID™." BCID™ delivers verified,

robust, and secure identity information including: (1) caller display name (*e.g.*, "Home Depot"); (2) call logo; and (3) call reason (*e.g.,* "Order Ready for Pickup"). With trusted, branded caller information, consumers can make more informed choices about whether to pick up the phone, reducing the risk of being bothered by spam or scam calls.

Notwithstanding all of the solutions discussed above, we know that bad actor robocallers will continue to find ways to call consumers. To that end, wireless providers are key partners in USTelecom's Industry Traceback Group ("ITG") to identify, block, or take enforcement actions against bad actors. CTIA's member companies and their partners across the voice ecosystem also continue to work to ensure that overseas counterparts take effective measures to mitigate foreign-originated illegal robocalls. Providers balance these steps with efforts to ensure that legitimate calls, including public safety calls, are protected.

These efforts have yielded promising results. In fact, according to ITG's latest report, "[t]raceback-powered enforcement [has] led to sharp declines in numerous illegal robocall campaigns." Robocall complaints to the FTC have also decreased steadily, reaching a six-year low in 2024. We are proud of this progress.

The Wireless Industry Is Committed to Maintaining Consumer Trust in Text Messages.

Today, wireless text messaging is one of the most popular and trusted forms of communication among American consumers. Americans exchanged 2.1 trillion text messages in 2023, and 90 percent of Americans use their phones to text at least monthly. The consumer trust that the wireless industry has built is why messaging boasts a 98% "open rate." This is

much higher than email, with a 20 percent open rate and 6 percent response rate. As these stats show, consumer trust in wireless text messaging remains high, and the wireless industry works collaboratively and innovatively to keep it that way.

As a result, CTIA and its member companies understand the importance of investing in proactive, multi-layered measures that include sophisticated tools, industry best practices, and public-private partnerships to protect consumers from spam and scam text messages.

At the outset, it is important to note that consumers' positive assessment of text messaging stems in part from the fact that messaging does not carry the same regulatory burdens as voice services. In contrast to voice services, where common carrier regulations impeded voice service providers from blocking unwanted robocalls, text messaging operates in a light-touch regulatory regime that has enabled wireless providers to be nimble and innovative in crafting solutions to protect consumers from a flood of spam and scam text messages. Wireless providers have not been forced to seek a government agency's permission to block or take action against illegal text messaging and bad actors; they do so proactively and aggressively to the benefit of consumers. And this has worked exceedingly well.

Wireless providers successfully prevent billions and billions of spam text messages from ever reaching consumers each year. In 2024 alone, wireless providers blocked more than 55 billion scam and spam robotexts. And blocking is only one part of the broader

effort to make sure the wireless industry's playbook evolves to keep up with bad actors' changing tactics.

First, wireless messaging technologies and up-front vetting and verification practices help thwart bad actors before they can even send scam or spam text messages. As a threshold protection, wireless messaging technologies require valid originating information, such as a legitimate telephone number. As a result, number spoofing has not plagued text messaging as it has with robocalling. Instead, impersonation scams – where bad actors try to trick consumers into thinking that a trusted entity like their bank is contacting them – have been more prevalent. To address this issue, wireless providers and their ecosystem partners require businesses and other message senders to disclose information about themselves and their campaign before they can send high volumes of text messages. This process has helped to weed out and prevent many bad actors from blasting out mass spam text messages.

Second, many different entities help make messaging work, both with respect to innovating messaging platforms and consumer protection. The messaging "pie" is expanding, including not only SMS/MMS text messaging offered by wireless providers, but also new platforms, like over-the-top ("OTT"), online and app-based messaging platforms, and recently-launched Rich Communications Service ("RCS"). Unfortunately, that also means that bad actors have more ways to target consumers, and their ambitions are not limited to any particular technology platform. This means all messaging providers – including RCS, OTT,

and online platforms – are part of the team effort to prevent spam messages and deter bad actors from targeting consumers through messaging.

Next, CTIA's *Messaging Principles & Best Practices* for the messaging ecosystem offers industry-led guidance to vindicate consumer preferences, while supporting innovative, legitimate communications. The *Best Practices* are widely adopted throughout the messaging ecosystem and focus on the key tenet of consent: Consumers should have control over the texts they receive, with the ability to opt-out at any time. Through these and other principles, including those addressing privacy and security, the *Best Practices* help prevent consumers from receiving unwanted messages while promoting innovation that allows consumers to get the messages they do want.

CTIA is gratified that its efforts were recently recognized by a coalition of six national consumer advocate organizations:

> [T]exting currently remains a valuable and trusted method of communication in the United States, largely because of the best practices developed by CTIA and adopted by its members and their partners. . . . [T]he entire texting ecosystem would be a disaster if fewer industry-developed restrictions against unwanted texts were applied.[1]

CTIA continues to update the *Messaging Principles and Best Practices* – for example clarifying who qualifies as a non-consumer sender to help ensure all types of entities understand what guidance applies to them as they set up their messaging campaigns.

Wireless providers and their messaging partners also deploy vast security and fraud prevention teams using the latest innovative technologies, machine learning and AI, and other spam mitigation tools to protect consumers through real-time analysis and other

defense solutions. To enhance these protections, wireless providers have set up a common means for consumers to report unwanted text messages – 7726 (SPAM) – and partner with Apple and Google to make it easier for consumers to "Report Junk" directly through the wireless messaging applications that are built into most of our wireless phones. Wireless providers use this reported data to constantly evolve spam mitigation tools in real-time and keep pace with the constantly changing tactics of bad actors. And when wireless providers receive complaints about texts with suspicious URLs or domains, their teams investigate the website to determine if the link is intended to support fraudulent efforts. If so, wireless providers can share that link with Google's Safe Search list so it can be blocked by most internet browsers.

The wireless industry and their messaging partners are constantly evolving and enhancing their tools, including by responsibly leveraging AI in myriad applications throughout the wireless ecosystem to prevent fraud, robocalls, and robotexts, strengthen cybersecurity, and more. CTIA and its member companies are mindful of both the benefits and risks of AI, and they are incentivized to strike the right balance in promoting innovative uses while fighting bad actors. We support the Administration's efforts to accelerate AI innovation through its AI Action Plan and AI R&D Plan, Congress' efforts to avoid a patchwork of state legislation on AI, as well as the FCC's bipartisan decision last year establishing clear guidance on the use of AI that has already helped the FCC and industry protect consumers from bad actors using AI voice-generating tools that fall within the scope of the TCPA. We

look forward to further developments like these that promote AI innovation rather than regulations focused on addressing AI-enabled robocalls and text messages.

Notwithstanding all of these tools, bad actors continue to seek out ways to get spam and scam text messages through to consumers. To complement industry tools and best practices, CTIA launched the Secure Messaging Initiative ("SMI") to help the FCC, FTC, DOJ, and other law enforcement agencies identify and go after bad actors. The SMI leverages the additional information available in the texting ecosystem (i.e., not just phone number and provider name) that is not accessible in the voice context to help identify suspected bad actors and refer those to law enforcement for investigation. SMI participants also share suspected spam and scam messages and techniques to more rapidly and effectively shut down spam activity, while targeting the senders of unwanted or fraudulent messages.

Through the SMI, we have already traced over 172,000 robotexts and made over a dozen referrals for enforcement actions to our partners at the FCC, FTC, DOJ, and the 50-state attorneys general enforcement task force. Collectively, these efforts are helping to enhance efforts to stop scammers and maintain consumer trust in wireless text messaging.

Congress, the FCC, the FTC, DOJ, and other authorities can contribute to this fight by encouraging industry efforts to coordinate and facilitate broad-based sharing information about bad actors through CTIA's SMI. And enforcement authorities like the FCC, FTC, DOJ, and state AGs should continue to "throw the book" at those that seek to harm consumers through illicit messaging. As noted above, the wireless industry is coordinating with federal

and state authorities to stop bad actors who may be violating these rules. And government and industry alike have a role to play when it comes to educating consumers to protect themselves and encouraging broader adoption of industry best practices, including CTIA's *Messaging Principles and Best Practices* and industry vetting and monitoring tools, that enable the wireless industry to identify and stop bad actors.

CTIA and the wireless messaging ecosystem remain vigilant in seeking to combat scam and spam messaging, and we are pleased there was a nearly 40% drop in consumer complaints about text messages to the FCC and the FTC between 2021 and 2023. Collaboration and information sharing across the wireless messaging ecosystem, cross-sector partners, and law enforcement agencies will help us continue to maintain consumer trust in wireless messaging by targeting bad actors and thwarting their evolving tactics.

Congress Should Consider Ways to Boost Efforts to Fight Robocalls and Robotexts.

The TRACED Act was landmark legislation that has encouraged the adoption of innovative technologies and solutions that are having positive results. CTIA offers a few suggestions on how this Committee can build on this positive framework to address the enduring problem of robocalls and robotexts.

First, we support the Administration's efforts to do more to protect consumers and our voice and text networks. As Chairman Carr noted in his first Commission-level action as Chair, "[c]racking down on illegal robocalls will be a top priority at the FCC,"[2] and we support this

effort. Second, we share the goal of cracking down on consumer fraud, as reflected in Ranking Member Pallone's *Do Not Disturb Act*.

Finally, we value our partnerships with law enforcement and encourage Congress to take steps to promote more action against the bad actors behind illegal robocalls and robotexts. Many agencies are working to fight consumer fraud, but many lack the personnel or resources to bring cases. Congress could have agencies report on their current consumer fraud resources and actions and leverage that information collection to identify areas that could use more support. With more resources for enforcement at the federal and state levels, Congress can help take more bad actors off the field and stop illegal robocalls and robotexts at the source.

* * *

The wireless industry is proud of our efforts to reduce the volume of illegal robocalls and prevent spam and scam text messages from reaching consumers. We know there is more work to do to protect consumers, and with the support of this Committee, the wireless industry can continue to lead in mitigating efforts by bad actors.

Thank you for the opportunity to testify today. We look forward to working with you to continue to protect consumers from intrusive and illegal robocalls and robotexts.

---

[1] Letter from Margot Saunders, Senior Counsel, National Consumer Law Center, to Marlene Dortch, Secretary, FCC, CG Docket No. 21-402 et al., at 2 (filed Mar. 6, 2024).

[2] Press Release: First Commission-Level Vote Under Chairman Carr Proposes A Nearly $4.5 Million Fine Stemming From Apparently Illegal Robocall Scheme (Feb. 4, 2025), https://docs.fcc.gov/public/attachments/DOC-409354A1.pdf.

Mr. PALMER. The Chair now recognizes Mr. Waguespack for 5 minutes for your testimony.

STATEMENT OF STEPHEN WAGUESPACK

Mr. WAGUESPACK. Thank you, Chairman Palmer, Ranking Member Clarke, and members of the subcommittee. My name is Stephen Waguespack, and I serve as president of the U.S. Chamber of Commerce's Institute for Legal Reform, more commonly known as ILR. The ILR is a division of the Chamber whose mission is to champion a fair legal system that promotes economic growth and opportunity. We believe that an effective legal system is critical to helping both customers and business owners. Thank you for the opportunity to testify today about the robocalling landscape and how American businesses are protecting consumers.

There are four main points I would like to cover in today's hearing.

Number one, legitimate businesses support and are helping to lead efforts to crack down on illegal and abusive robocalls and robotexts. Businesses have every incentive to ensure that consumers continue to trust these communications. The illegal calls and texts that seek to defraud U.S. consumers begin with bad actors exploiting the reputation and good will of trusted American brands.

For example, one in three businesses report being impersonated by scammers, with 13 percent reporting a switch in brands due to this deception. According to 2024 data from Hiya, 45 percent of consumers have received a call from someone impersonating a legitimate business, and 70 percent of businesses report getting a similar attack. Beyond reputational damage, fraudulent calling and texting schemes also degrade consumers' trust in these types of communications, making it difficult for businesses to engage with their customers. That's why many companies are proactively helping regulators trace these bad actors and going on the offensive by fighting back directly against them.

For example, Marriott International brought its own trademark lawsuit against malicious robocallers and scored significant legal victories over both foreign and U.S.-based defendants, while DirecTV also secured a total of $8 million in judgments and broad, permanent injunctions. The private sector is also devising innovative technologies, such as analytics-powered software, while partnering with the government through programs like the Industry Traceback Group and Secure Messaging Initiative in tackling illegal and abusive robocalls.

Number two, more legislation will not solve the problem. Fraudulent and abusive robocalls and robotexts are already illegal. Congress must ensure that its already substantial efforts to curb these activities bear fruit by encouraging Federal agencies to make illegal robocalls and robotexts an enforcement priority. As the Chamber has previously urged, lawmakers should push DOJ to prioritize enforcement against these bad actors and report annually to Congress on their efforts.

There is optimism that focus on this topic could be welcomed by the DOJ, as we have seen the FCC and FTC utilizing tools like the traceback program to increase the focus on bad actors.

Number three and most critically, the TCPA's private rights of action provisions continue to fuel abusive litigation against American businesses. This difficult operating environment hurts both businesses and consumers and is undermining the proactive efforts by this Congress to address the very real problem of scammers. The private right of action provisions in the TCPA make it more challenging for legitimate businesses and organizations to send and for consumers to receive good calls and texts, such as appointment reminders, notifications about school closures, and other communications that consumers want. At the same time, it does not deter bad calls and texts, such as fraudulent and harassing communications that originate from bad actors.

It is critical that Congress distinguish between these two types of calls and limit the ability of a handful of aggressive plaintiff firms to dominate the market for these suits. Congress should also encourage the FCC to simplify TCPA regulations to boost compliance, ensure certainty for legitimate businesses, and focus on addressing bad actors.

Fourth and finally, Congress could utilize the precedents set in other Federal and State statutes to limit the abuse of private rights of action found within TCPA by implementing, one, reasonable damage caps; two, clear safe harbor provisions; three, limits on unreasonable attorney fees; and, four, mandatory disclosure of any usage of third-party litigation financing, known as TPLF, in these TCPA cases to ensure consumer rights are protected. The business community wants to end illegal robocalls and robotexts to foster a safe and trustworthy communications ecosystem for businesses and their consumers.

As Congress considers paths forward, the enforcement should be a top priority of all Federal agencies, and Congress should consider reforms to prevent legitimate businesses from being ensnared in abusive TCPA litigation.

Thank you for your work to date on this topic, and to the subcommittee for the opportunity to discuss these important issues. I look forward to answering your questions. Thank you.

[The prepared statement of Mr. Waguespack follows:]

Statement of Stephen Waguespack

President, Institute for Legal Reform & Special Counsel, U.S. Chamber of Commerce

U.S. House Energy & Commerce Committee, Subcommittee on Oversight and Investigations

Stopping Illegal Robocalls and Robotexts: Progress, Challenges, and Next Steps

Thank you Chairman Palmer, Ranking Member Clarke, and members of the Subcommittee. My name is Stephen Waguespack, and I am the President 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—and are helping to lead—efforts to crack down on illegal and abusive robocalls and robotexts 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 and robotexts bear fruit by encouraging federal agencies—and particularly the Department of Justice ("DOJ")—to make illegal robocalls and robotexts an enforcement

priority.

- ***Third***, the Telephone Consumer Protection Act's ("TCPA") private rights of action continue to fuel abusive litigation against American businesses. This difficult operating environment hurts businesses and consumers. It makes it more difficult for legitimate businesses and organizations to send, and for consumers to receive, good calls and texts—such as appointment reminders, notifications about school closures, and other communications that consumers want; at the same time, it does not deter bad calls and texts—such as fraudulent and harassing communications that originate from bad actors. It is critical that Congress distinguish between these two types of calls. Congress should also encourage the Federal Communications Commission ("FCC") to streamline and modernize TCPA regulations to boost compliance, ensure certainty for legitimate businesses, and focus on addressing bad actors.

- ***Fourth***, Congress 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.

Chamber members around the country share Congress's concerns about the damage that scam calls and texts are causing and are committed to working with Congress to root out these schemes at the source and hold perpetrators responsible.

Like consumers, legitimate businesses suffer harm at the hands of robocall and robotext fraud

and scams. The illegal calls and texts that seek to defraud U.S. consumers begin with bad actors exploiting the reputation and good will of trusted American brands. Indeed, legitimate businesses face the serious risk from illegal robocalls of dilution of their brand through impersonation fraud. For example, "1 in 3 businesses" report having "had their name used by an impersonator making scam calls."[1] This fraud carries serious consequences for businesses: 13% of consumers "have since switched brands after receiving an impersonation call."[2]

Beyond reputational damage, fraudulent calling and texting schemes also degrade consumers' trust in the voice and text messaging networks, making it difficult for businesses to engage with their customers. American consumers are the life-blood of commerce, and successful and trusted businesses avoid practices that customers revile. In stark contrast, the bad actors behind the deluge of illegal robocalls and robotexts simply ignore the law, ultimately inflicting financial harm to consumers, and severely tarnishing legitimate brands through impersonation fraud.

In short, the business community abhors the perpetuation of illegal and abusive robocalls and robotexts. Because of significant harms to consumers and businesses from robocall and robotext scams, companies are proactively going on the offensive by fighting back against the bad actors behind these calls and texts. For example:

- Marriott International has directly fought back by bringing its own trademark lawsuit against malicious robocallers and their facilitators, and in a significant legal victory, obtained judgments, consent orders, or settlements against all six of the U.S.-based

[1] State Of The Call 2023, Hiya, at 9, *available at* https://www.hiya.com/state-of-the-call (updated June 2023).

[2] *Id.* at 10.

defendants. Marriott also secured $8 million judgments against two foreign defendants that unlawfully used its trademarks in more than 66 million robocalls between 2018 and 2022.[3]

- DIRECTV also filed two federal lawsuits against fraudsters who were targeting existing or potential DIRECTV customers with imposter robocalls.[4] The company ultimately secured a total of $8 million in judgments, and broad permanent injunctions against the entities and individuals behind these deceptive robocalls targeting American consumers.

- Other companies have been actively deploying other efforts to address illegal robocalls and robotexts. For example, the American Bankers Association ("ABA") launched an industry-wide consumer education campaign involving more than 2,000 banks from across the nation called "Banks Never Ask That."[5] The campaign is designed to educate consumers about the persistent threat of phishing scams, and "turn[] the tables on the bad guys by empowering consumers with the tools they need to spot bogus bank communications."[6] The ABA recently reported that one participating bank experienced a

[3] *See* Press Release, Marriott International, Marriott International Secures Legal Victory Against Fraudulent Robocall Operators (Oct. 4, 2024), https://news.marriott.com/news/2024/10/04/marriott-international-secures-legal-victory-against-fraudulent-robocall-operators. *See also*, *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).

[4] *See DIRECTV, LLC v. Synmatix, LLC et. al.*, No. 1:22-CV-02817 (D. Md. Nov. 1, 2022); *DIRECTV, LLC v. WNK Associates, Inc. et. al.*, No. 6:22-CV-00423 (E.D. Tex. Nov. 1, 2022).

[5] *See Banks Never Ask That* (2024), American Bankers Association, https://www.banksneveraskthat.com/about/.

[6] *Id.*

94% decline in customer losses to fraud after implementing the campaign.[7]

- Companies are devising innovative technologies to ward off illegal robocalls and robotexts, such as analytics-powered software,[8] and the private sector is partnering with the Government in tackling illegal and abusive robocalls. The Industry Traceback Group ("ITG") is a group of "companies from across the wireline, wireless, [Voice over Internet Protocol] VoIP, and cable industries" that "collaborate to trace, source, and ultimately, stop illegal calls."[9] The ITG has conducted more than 17,000 tracebacks since its creation[10] 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."[11] And just last month, the ITG stated that it is coordinating with voice service providers and financial institutions to conduct a pilot program to source examples of spoofed bank calls for traceback and identification of their sources. Importantly, this effort has enabled banking institutions to more quickly identify customers impacted by

[7] Marlee Ribnick, *How one bank's 'stop and think' message slashed customer fraud losses*, ABA Banking Journal (May 20, 2025) https://bankingjournal.aba.com/2025/05/how-one-banks-stop-and-think-message-slashed-customer-fraud-losses/.

[8] *See* Lance Whitney, *Stop the Madness: How to Block Spam Calls and Robocalls*, PC Mag (Feb. 28, 2025), https://www.pcmag.com/how-to/block-robocalls-and-spam-calls.

[9] *See Industry Traceback Group*, https://tracebacks.org/.

[10] Industry Traceback Group Ex Parte, *Enforcement Bureau Requests Information on the Status of Private-Led Traceback Efforts of Suspected Unlawful Robocalls*, EB Docket No. 20-195, DA 25-261, at 1 (May 1, 2025), https://www.fcc.gov/ecfs/document/1050176246723/1.

[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.

fraudulent scams.[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-spearheaded approach.[14]

- Finally, on the robotexting front, CTIA has launched its Secure Messaging Initiative ("SMI"), which is an industry-led program aimed at protecting consumers from unwanted or illegal text messaging spam. The goal of the SMI is to rapidly and effectively shut down spam activity and help enforcement agencies target bad actors that send unwanted or fraudulent messages.[15] Through this partnership, the wireless industry has delivered 10 referral packages to law enforcement partners at the FCC, the Federal Trade Commission ("FTC"), and the state Anti-Robocall Litigation Task Force, which these enforcers can use to bring charges against spammers and shut them down.[16]

---

[12] USTelecom Ex Parte, *Enforcement Bureau Requests Comments on Selection of Registered Traceback Consortium*, EB Docket No. 20-22, at 2 (May 22, 2025) https://www.fcc.gov/ecfs/document/1052278229960/1.

[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).

[15] *CTIA Secure Messaging Initiative*, CTIA, https://www.ctia.org/ctia-secure-messaging-initiative.

[16] *Wireless Industry Achieves Milestones in Tracing Robotexts*, CTIA (Sept. 16, 2024), https://www.ctia.org/news/wireless-achieves-milestone-in-tracing-texts.

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

II. CONGRESS SHOULD ENSURE THAT PROSECUTING FRAUDSTERS IS A PRIORITY.

A. Fraudulent And Abusive Robocalls And Robotexts Are Already Illegal.

More legislation will not stop the illegal and abusive robocalls and robotexts that we are seeing today. The TCPA and its implementing rules prohibit calls made using autodialed and artificial or prerecorded voices to consumers' cell phones unless the consumer consents or the call is otherwise permitted (*e.g.*, calls made for emergency purposes).[17] And the FCC has extended the TCPA's coverage to text messages, prohibiting autodialed text messages sent without a called party's consent.[18] The TCPA also establishes a number of other robust protections for consumers with respect to telemarketing and solicitation calls and texts—regardless of the technology being used to communicate.[19] 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."[20] Congress delegated to the FTC the authority to

---

[17] 47 U.S.C. § 227(b)(1)(B), (2)(B); 47 C.F.R. § 64.1200(a).

[18] In the 2003 TCPA Order, the FCC determined that text messages constitute "calls" under the TCPA. *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order, CG Docket No. 02-278, at ¶ 165 (2003). *See also Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Declaratory Ruling and Order, CG Docket No. 02-278, WC Docket No. 07-135, at ¶ 107 (2015) ("Glide raises the issue of whether SMS text messages are subject to the same consumer protections under the TCPA as voice calls. We reiterate that they are.").

[19] *See, e.g.*, 47 C.F.R. § 64.1200 (c)-(d).

[20] 47 U.S.C. § 227(e).

"implement and enforce a national do-not-call registry,"[21] 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.[22] The TSR also prohibits deceptive and abusive telemarketing tactics and can be a powerful tool to go after bad actors.[23]

Illegal robocallers and robotexters also face serious potential criminal penalties, including through the wire fraud statute, which 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.[24] In addition, the TRACED Act imposes criminal fines of $10,000 per violation of the prohibition on fraudulent call spoofing.[25] 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.[26]

Beyond this, there are robocall and robotext mitigation requirements already on the books. For example, the FCC adopted a Report and Order in March 2023 that requires providers to block text messages that appear to originate from phone numbers on a reasonable do-not-originate list, which are text messages that are highly likely to be illegal.[27] And a second rule already in effect requires mobile providers to either establish a point of contact for text message senders or ensure

---

[21] 15 U.S.C. § 6151.

[22] 16 C.F.R. § 310.4(b)(1)(iii)(B).

[23] *Id.* §§ 310.4, 310.5.

[24] 18 U.S.C. § 1343.

[25] 47 U.S.C. § 227(e)(5)(B).

[26] 18 U.S.C. § 501.

[27] *Targeting and Eliminating Unlawful Text Messages; Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket Nos. 21-402, 02-278, Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2744, 2751, ¶ 16 (2023).

that its aggregator partner or blocking contractor establish a point of contact to inquire about blocked texts and resolve complaints regarding erroneous blocking.[28]

Even with this existing robust body of legislation, fraudsters continue to violate the many laws on the books without penalty.

B. There Has Been Some Enforcement Progress.

Thankfully, we have seen some progress in combatting the bad actors responsible for illegal robocalls. As the FCC's most recent report to Congress detailed, the agency pursues forfeitures for tens—and sometimes hundreds—of millions of dollars against the biggest robocalling operations targeting Americans.[29] Among these enforcement actions is the largest forfeiture in the agency's history: $299 million levied against a group of businesses that placed one billion fraudulent robocalls.[30] The FCC also took action to protect consumers from scam robotexts associated with student debt, issuing a Consumer Alert in conjunction with four state Attorneys General warning consumers about an uptick in scam messages related to federal student loan debt relief.[31] The FTC is also active, having settled a lawsuit in 2024 with a VoIP that funneled

[28] 47 CFR § 64.1200(r).

[29] FCC Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information, FCC, at 4-5 (Dec. 27, 2024), https://docs.fcc.gov/public/attachments/DOC-408475A1.pdf ("2024 FCC Robocall Report").

[30] *Id.* at 5.

[31] Consumer Advisory, Fed. Commc'ns Comm'n, FCC & State Attorneys General Warn Consumers of Increased Risk of Student Loan Debt Scam Robocalls and Robotexts (June 30, 2023), https://docs.fcc.gov/public/attachments/DOC-394832A1.pdf (Student Loan Robocall Advisory).

"hundreds of millions of illegal robocalls through its network."[32] The settlement, among other things, bans the company from providing VoIP services to any company that "does not have an automated procedure to block calls that display invalid Caller ID phone numbers or that are not authenticated through the FCC's STIR/SHAKEN Authentication Framework."[33]

As highlighted above, businesses are supplementing these federal enforcement efforts. As the FCC notes in its 2024 TRACED Act Report to Congress,[34] the ITG's traceback efforts "have continued to grow" over the last four years.[35] The ITG "initiated 3,737 tracebacks [in 2023]—345 more than were conducted in 2022."[36] The ITG identified 699 U.S. and foreign-based providers in 2023, and of those 699 providers, 270 had not previously been identified; "85% of completed tracebacks resulted in an originating provider warning or terminating the caller."[37]

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

---

[32] 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; Press Release, FTC, XCast Labs Will Be Banned from Supporting Illegal Telemarketing Practices to Settle FTC Charges It Assisted and Facilitated in Sending Hundreds of Millions of Illegal Robocalls (Jan. 2, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/xcast-labs-will-be-banned-supporting-illegal-telemarketing-practices-settle-ftc-charges-it-assisted.

[33] Press Release, FTC, XCast Labs Will Be Banned from Supporting Illegal Telemarketing Practices to Settle FTC Charges It Assisted and Facilitated in Sending Hundreds of Millions of Illegal Robocalls (Jan. 2, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/xcast-labs-will-be-banned-supporting-illegal-telemarketing-practices-settle-ftc-charges-it-assisted.

[34] 2024 FCC Robocall Report.

[35] *Id.* at 24.

[36] *Id.*

[37] *Id.*

Despite all of this activity—including headline-grabbing FCC forfeiture orders—the federal government needs to do more to hold bad actors accountable, particularly those perpetrating fraud on Americans from overseas. A lack of historical DOJ enforcement presents the biggest obstacle at this time, though we are hopeful that will improve.

DOJ has not been pursuing in court the forfeiture orders adopted by the FCC. The FCC recently reported that in 2023, DOJ did not "collect[] forfeiture penalties or criminal fines for violations of [the TCPA]."[38] This was a missed opportunity for DOJ and one we hope the new leadership at the Department will vigorously pursue in the near future.

Nor has DOJ historically taken its own 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,[39] DOJ has not previously appeared to have made material prosecutions a

[38] *See* 2024 FCC Robocall Report at 5.

[39] 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.

high priority, which is particularly disappointing when it comes to recidivist robocall abusers.[40]

As the Chamber has called for in prior testimony, lawmakers 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.[41]

- 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.

---

[40] *In the Matter of Sumco Panama SA et al.*, Forfeiture Order, File No. EB-TCD-21-00031913, FCC 23-64, ¶ 12 (Aug. 3, 2023) ("*Sumco Panama Order*") ("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.").

[41] 47 U.S.C. § 227(h).

III. THE TCPA'S PRIVATE RIGHTS OF ACTION CONTINUE TO BE THE SOURCE OF ONGOING LITIGATION ABUSE, WHICH DOES NOT ADDRESS THE URGENT ISSUE OF COMBATTING BAD ACTORS, AND THE FCC SHOULD MODERNIZE ITS TCPA REGULATIONS.

Although the TCPA has generally helped protect consumers, the same cannot be said for its private rights of action. Those provisions are 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 Court's 2021 decision in *Facebook v. Duguid*[42] would significantly improve the situation, well-meaning businesses continue to be harassed by harmful and opportunistic TCPA settlement demands and lawsuits. This ultimately harms the ability of consumers to utilize modern communications tools and access innovative services.

A. Not All Automated Communications Are Bad.

Ultimately, any discussion of robocalling, robotexting, and the TCPA must distinguish between legitimate and lawful communications versus abusive scam communications. 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."[43] Such a distinction is critical. Consider some

[42] *Facebook, Inc. v. Duguid*, 592 U.S. 395 (2021).

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

of the ways in which legitimate 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."
- "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." [44]

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."[45] 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 email being the least requested method of contact."[46]

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

---

[44] *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, 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*").

[45] *Id.* at 8085 (quoting Letter from Elizabeth P. Hall, Vice President, Office of Government Affairs, Anthem, Inc., to Marlene H. Dortch, FCC, CG Docket No. 02-278, at 5 (filed Apr. 6, 2015)).

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

"commercial" in nature.[47] In striking down part of the TCPA as unconstitutional in 2020, the Supreme Court confirmed that robocalls constitute speech protected by the First Amendment.[48]

In sum, there are many beneficial robocalls and robotexts that provide customers with timely, convenient, and desirable information. The Chamber urges policymakers 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 inhibit 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 litigation, including class-actions, burdening how businesses reach their customers, while doing little to stop truly abusive robocalls or robotexts and protect consumers.[49] This litigation cash cow has become a major obstacle,

---

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

[48] *See Barr v. Am. Ass'n of Pol. Consultants, Inc.*, 591 U.S. 610, 620 (2020) (plurality) ("The law here focuses on whether the caller is *speaking* about a particular topic." (emphasis in original)); *id.* at 637 (Sotomayor, J., concurring) (concluding that relevant provision of the TCPA unconstitutionally burdened "robocall speech" (internal quotations omitted)); *id.* at 649 (Gorsuch, J., concurring) ("no one doubts the TCPA regulates speech").

[49] *See, e.g.*, Expanding Litigation Pathways: TCPA Lawsuit Abuse Continues in the Wake of Duguid, U.S. Chamber Institute for Legal Reform (Apr. 2024), https://instituteforlegalreform.com/wp-content/uploads/2024/04/ILR-Expanding-Litigation-Pathways-April-2024.pdf ("*Expanding Pathways*"); 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/; 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

stifling 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 professional plaintiff's lawyers—and some professional *pro se* plaintiffs—are responsible for a massive volume of TCPA litigation.[50] For example in a petition to the FCC, filed in March of this year by the Ecommerce Innovation Alliance and others, the petitioners noted that:

> "a singular law firm based in south Florida, through aggressive social media campaigns, actively recruits plaintiffs to file TCPA lawsuits based on a misapplication of the law. They lure individuals with promises of money and false claims that all messages delivered during Quiet Hours are 'illegal texts' and boast about recovering 'millions of dollars' under the TCPA. Since November, two junior attorneys from this firm have inundated federal courts with 100 such cases."[51]

And as ILR research into TCPA litigation trends has shown, for each year from 2020-2023, just ten law firms have been responsible for more than half of that year's TCPA filings.[52]

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.

[50] *See Expanding Pathways* at 22.

[51] Petition for Declaratory Ruling and/or Waiver of the Ecommerce Innovation Alliance and Other Petitioners, CG Docket Nos. 02-278, 21-402, at i (filed Mar. 3, 2025).

[52] *See Expanding Pathways* at 22.

Professional TCPA plaintiffs also play a substantial role in TCPA litigation abuse by either pairing with a plaintiff's firm or filing TCPA claims *pro se*. For example, Terry Fabricant—the most frequently appearing plaintiff—regularly partners with the Law Offices of Todd M. Friedman, the law firm that filed the most federal TCPA cases in 2020 and 2021.[53] Together they filed 126 federal TCPA cases from 2020-2023.[54]

ILR's members know firsthand the difficulties with this kind of "gotcha" operating environment. The statute's private rights of action are expansive. Any person who receives an unlawful call or text may bring a lawsuit to recover $500–$1,500 per violation.[55] There is no cumulative limit to these damages, leading some plaintiff's lawyers to seek mind-boggling damages awards.[56] Further, massive classes—such as a recent class certification of over one million people in a TCPA case against a bank[57]—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.[58] Other examples include a class action settlement with a telecommunications company for $45 million[59] and another with a

---

[53] *Id.* at 23.

[54] *Id.*

[55] 47 U.S.C. § 227(b)(3).

[56] *See, e.g.*, Final Judgment, *McMillion et al. v. Rash Curtis & Associates*, No. 4:16-CV-03396, (N.D. Cal. Sept. 9, 2019), ECF No. 370 (The court order a $267M judgment against the defendant for violations of the TCPA.).

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

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

[59] Final Judgment ¶ 14, *Hageman v. AT&T Mobility LLC*, No. 1:13-CV-00050 (D. Mont. Feb. 11, 2013), ECF No. 68.

utility services company for $38.5 million.[60]

With enormous potential damages in play, plaintiffs have little incentive to go after criminal or overseas scammers, who offer a miniscule chance to easily generate such large payouts.[61] Instead, TCPA plaintiffs have opted to target legitimate businesses—many of them household names—and not the offshore robocallers and robotexters flooding Americans' phones with fraud and scam calls and texts. 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.[62]

- 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[63] for an automated phone call offering a Public Service Announcement for homeowners in default.[64]

- A ride-share company was sued for notifying a driver that he needed to update an expired

---

[60] *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).

[61] *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").

[62] *Silver v. City of Albuquerque*, No. 1:22-CV-00400, 2023 WL 2413780 (D.N.M. Mar. 8, 2023), *aff'd*, 134 F.4th 1130 (10th Cir. 2025).

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

[64] *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).

driver's license.[65]

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.[66] 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.[67]

And yet additional risks loom, with a predicted wave of TCPA suits that may seek to exploit the FCC's new consent revocation rule.[68] Certain of the requirements could be a boon for serial litigants, including a new provision that requires businesses making calls and sending text messages to honor opt-out requests made through "reasonable means" within 10 business days.[69] While the FCC has explained that certain words (*i.e.*, "stop," "quit," "end," "revoke," "opt out," "cancel," or "unsubscribe" via reply text message) sent as a response to a text constitute a *per se* reasonable means to revoke consent, the agency did not preclude the use of other words and

---

[65] *Eller v. Uber Techs., Inc.*, No. 4:23-CV-03526 (S.D. Tex. Sept. 19, 2023).

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

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

[68] *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order and Further Notice of Proposed Rulemaking, 39 FCC Rcd 1988 (2024).

[69] 47 C.F.R. § 64.1200(a)(10).

phrases to revoke consent, leaving it open to dispute, and hence litigation.[70]

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. [71]

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.[72] 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.[73]

Unfortunately, the *Duguid* decision has not stemmed the tide of frivolous TCPA litigation. An ILR study concluded that although there was a short-term reduction immediately following

---

[70] *Id.*

[71] *Cf. Sumco Panama Order* ¶ 1 (Aug. 3, 2023).

[72] *Facebook, Inc. v. Duguid*, 592 U.S. 395, 409 (2021).

[73] 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. 37 F.4th 867 (3d Cir. 2022).

Duguid in the volume of TCPA lawsuits filed, "plaintiffs have succeeded in prolonging litigation, taking cases to expensive discovery phases and even summary judgement, which creates risks for legitimate callers attempting to reach their customers with important information."[74] 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 have been increasing, with burgeoning class actions a major driver of TCPA filings. One observer notes that "TCPA class actions continue to pour in" and "class actions filings were up 100% (doubled!) in April [2025] compared to last year."[75]

Thus, *Duguid* has not led to long-term meaningful protections against opportunistic TCPA lawsuits.

D. The TCPA's Private Rights Of Action Harm 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 rights of action hurt businesses and consumers. Given that even innocent missteps can lead to business-ending liability, some companies may understandably choose to "cease communicating" altogether.[76] But, as explained above, many consumers *want* these

[74] *Expanding Pathways* at 6.

[75] Eric J. Troutman, *TCPA CLASS ACTIONS CONTINUE TO SKYROCKET!!: TCPA Class Action Filings DOUBLE in April, 2025 And That's Not All…*, TCPA World (May 30, 2025), https://tcpaworld.com/2025/05/30/tcpa-class-actions-continue-to-skyrocket-tcpa-class-action-filings-double-in-april-2025-and-thats-not-all/.

[76] *2015 TCPA Declaratory Ruling and Order* at 8093 (O'Rielly, Comm'r, dissenting in part and approving in part) (quoting Letter from Monica S. Desai, Counsel to Abercrombie & Fitch Co. and Hollister Co., to Marlene H. Dortch, FCC, CG Docket No. 02-278, at 3-4 (filed May 13, 2015)).

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.

E. TCPA Regulations Are Expansive, Complex, And In Need Of Reform.

The TCPA has spawned an expansive docket at the FCC intended to clarify the TCPA's statutory provisions and address novel issues presented by robocalls and robotexts. Over the years, the number of TCPA regulations has substantially increased with new obligations and exemptions, and understanding TCPA obligations is challenging given the number of cross-references and references to the underlying TCPA Reports and Orders. Thus, TCPA obligations are often ambiguous, have prompted numerous frivolous and costly lawsuits against legitimate businesses attempting compliance, and have led to varying inconsistent court interpretations. This threatens to create a patchwork of differing court interpretations compounding compliance and litigation costs.

Also, the TCPA and its associated regulations are frequently abused by elements of the plaintiffs' bar and serial plaintiffs to leverage excessive damage awards and settlements against the legitimate business community while leaving genuine bad actors largely untouched. Congress should encourage the FCC to review and clarify TCPA requirements and consider streamlining rules, reducing liability against the legitimate business community, and eliminating duplicative sections. This will provide more clarity for regulated parties, boost compliance, reduce the judiciary's workload in interpreting ambiguous requirements, and focus efforts on addressing bad actors.

IV. CONGRESS SHOULD CONSIDER MODEST CHANGES TO THE TCPA THAT LIMIT LITIGATION ABUSE BY CURTAILING DAMAGES AND FEES, PROTECTING GOOD-FAITH COMPLIANCE, AND REFORMING THIRD PARTY LITIGATION FUNDING TO HELP ADDRESS ABUSIVE TCPA LITIGATION.

Since the TCPA's 1991 enactment and in more recent legislation, 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. Congress also should consider the dangers of third party litigation funding ("TPLF") which has introduced distortions in our civil justice system more generally, and could promote additional abusive TCPA litigation.

To restore the balance intended in the TCPA, Congress should consider modest changes to reduce abusive litigation, 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.[77] Congress should

[77] *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).

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."[78] 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.[79] Additionally, Florida amended the Florida Telephone Solicitation Act to allow consumers to respond with "STOP" to cease further text message solicitations.[80] 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"

[78] 42 U.S.C. § 1320d-5(a)(3)(A).

[79] 16 CFR § 312.11(b).

[80] H.B. 761, 2023 Leg., Reg. Sess., § 1 (Fla. 2023) (amending Fla. Stat. § 501.059).

message was sent.[81]

- **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. As a commentator recently observed, "[e]very single one of these [TCPA] cases has the potential to completely ruin a business– the attorneys fees to defend the suits alone are enough to drive some companies out of business."[82] 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.

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.

In addition to these adjustments, Congress should be mindful of the impact of third party funding on incentives and outcomes in litigation, including class actions. TPLF allows hedge funds and other financiers to invest in lawsuits in exchange for a percentage of any settlement or judgment. As the Chamber ILR has shown through extensive research, third party funding of litigation is driving up massive verdicts that may have little relation to actual harm, and it offers the prospect

[81] Fla. Stat. § 501.059(10)(c).

[82] Eric J. Troutman, *TCPA CLASS ACTIONS CONTINUE TO SKYROCKET!!: TCPA Class Action Filings DOUBLE in April, 2025 And That's Not All…*, TCPA World (May 30, 2025), https://tcpaworld.com/2025/05/30/tcpa-class-actions-continue-to-skyrocket-tcpa-class-action-filings-double-in-april-2025-and-thats-not-all/.

of huge payouts to lawyers and funders, rather than helping consumers. ILR's research paper, *Nuclear Verdicts: An Update on Trends, Causes, and Solutions*, showed that "[p]laintiffs' lawyers are also increasingly bringing litigation funded by third parties seeking a return on their investment, which not only enables such advertising and speculative claims but also contributes to nuclear verdicts by driving up award demands and widening the gap for parties to negotiate a reasonable settlement."[83]

Congress can enact disclosure and other reforms to address the problems presented by the opaque and unrestricted TPLF industry, which can promote questionable TCPA lawsuits. The Chamber has developed and advocated several proposals that will protect our civil justice system from abuse. I will briefly note three of them. *First*, Congress and judges should require disclosure of TPLF agreements. Plaintiffs and their lawyers enter these agreements with funders in secret. *Second*, Congress should address ethics concerns raised when an outside party has a financial interest in litigation. It should, for example, prohibit funders from influencing a party's selection of an attorney, choices about litigation strategy, or settlement. *Third*, Congress can protect plaintiffs by making certain that they are aware that their attorney has committed to sharing their recovery with a third party and prohibiting funders from taking a larger share of the recovery than an injured plaintiff receives.

Some states have taken action to regulate the use of TPLF, and Congress can explore similar changes to the TCPA that preclude the expansion of opaque TPLF into TCPA litigation. Several members of Congress have expressed grave concerns about the role of litigation funding in our

[83] Nuclear Verdicts: An Update on Trends, Causes, and Solutions, U.S. Chamber Institute for Legal Reform (May 2024) https://instituteforlegalreform.com/research/nuclear-verdicts-an-update-on-trends-causes-and-solutions/.

civil justice system, and have called on the Department of Justice to examine the trend and take appropriate action.[84]

* * *

The business community wants to end illegal robocalls and robotexts in order to 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.

[84] *See* Grim Realities: Debunking Myths in Third-Party Litigation Funding, U.S. Chamber Litigation Center, at 27 (Aug. 29, 2024) https://instituteforlegalreform.com/research/grim-realities-debunking-myths-in-third-party-litigation-funding/ (noting calls by Rep. James Comer (R-KY), who "wrote to Chief Justice Roberts urging the Judicial Conference (the federal judiciary's rulemaking body) to review the role of litigation finance" and "called for concrete judicial reform, including a potential requirement that TPLF in federal lawsuits be disclosed as a matter of course").

Mr. PALMER. The Chair now recognizes Mr. Winters for 5 minutes for your testimony.

STATEMENT OF BEN WINTERS

Mr. WINTERS. Chair Guthrie, Ranking Member Pallone, Chair Palmer, Ranking Member Clarke, and members of the subcommittee, thank you for inviting me to testify before you on this important issue.

I am Ben Winters. I am the director of AI and privacy at the Consumer Federation of America, or CFA. CFA is an association of nonprofit consumer organizations established in 1968 to advance the consumer interest through research, advocacy, and education.

There is a staggering amount of monetary and emotional harm caused by scams perpetrated through robocalls and robotexts. Consumers lost over $12.5 billion to scams last year, which was a 20 percent increase from 2023. Even when no money is lost, there is a constant sense of annoyance and need for vigilance. Americans received an estimated 19.2 billion robotexts and 5 billion robocalls last month alone. And just this morning, the Washington Post featured the fact that there is a five times jump in scam losses from schemes that started in texts since 2020.

In this testimony, I will be highlighting how underregulated technologies like AI are making these problems worse, how Federal consumer protection agencies can be doing more, and how Congress can act to protect consumers from this annoying and dangerous problem.

Generative AI reduces the time and effort criminals have to expend in order to deceive their targets. Products like ChatGPT can create quick and unique human-sounding scripts that can be sent in text or read by humans or AI-generated voices, and it's easy to make variations that make them difficult to spot.

In CFA's recent "Scamplified" report, we illustrate how easy it is to use ChatGPT to generate text with an urgent ask to add $50 worth of bitcoin to a wallet. It spat out 30, 50, 100 texts with common women's names and real hospitals in common U.S. cities to create urgency. It even continued to spit out texts when we asked it to target it to someone that might have dementia.

And it is not just text generators. Voice-cloning tools can now replicate anyone's speech using just a few seconds from a phone call or a podcast interview. Scammers have exploited this to impersonate loved ones, such as in grandparent scams you have already heard about today.

Consumer Reports' investigation showed popular voice-cloning platforms do not require the user to verify their identity or gain consent before creating these voice clonings.

Beyond AI, there is a host of companies in what we call the scam stack, all of which are fueling an increase in scams. These include data brokers that sell data en masse based on people's behavior, purchases, relationships, location, and more, automated content delivery, things like we're talking about today, and methods of reporting which can be improved to bridge the gap between a victim and the authorities that could help.

Federal consumer protection agencies tasked with stopping scam robotexts and robocalls like the FCC and FTC are being stripped

down and distracted. The consequence is stark. In April, the Department of Justice eliminated their consumer protection branch entirely. This is the branch that brought a landmark criminal case against a data broker that sold over 30 million records of elderly Americans that was then used to perpetrate a scam. This type of enforcement of upstream actors is exactly what we need to see, and it is troubling to see that agency get axed.

Americans deserve an FCC that is focused on the complicated robocall ecosystem, and they have done a lot to try to address it. But the agency leadership right now seems focused on controlling the speech and hiring practices of entertainment companies that are perceived to be the enemies of the President instead of ramping up rulemaking and enforcement as an independent agency.

Chairman Carr's Delete, Delete, Delete Initiative, in which he is asking the American public what regulations the FCC should delete because they stand in the way of expansion and technological innovation, is illustrative of this disastrous deregulatory approach that does not even mention consumer protection.

At the FTC, the firing of key staff and, critically, two of the five Commissioners have left the agency ill equipped to protect American consumers. The agency must finalize the individual impersonation rule so they can deter and enforce violations of widespread things like voice cloning, like they have started to do with government and business impersonation, which they finalized last year.

Both agencies must prioritize enforcement against upstream actors, such as voice service providers and AI developers who knowingly facilitate these harmful practices. These intermediaries are critical to how illegal calls and texts scale and are essential to meaningful accountability.

Congress has to hold upstream actors accountable, just like I talked about, strengthen enforcement tools beyond just what's in the TRACED Act, increase transparency, and mandate consequences for known bad actors throughout the call path. We also urge Congress to increase funding for State enforcement, pass privacy laws restricting data brokers, and require responsible AI moderation and transparency.

One thing Congress absolutely should not do right now is pass a moratorium on regulating AI at the State level. The scale of these problems is one of many reasons it's not the time to do this. And if States can create transparency or establish appropriate liability, we should welcome it, embracing the critical roles of States not only to protect consumers but be the laboratory of democracy.

Right now, the FTC, FCC, and CFPB risk being cops off of their beat. And Congress must empower them, resource them, and restore them in order to aggressively protect consumers. The American people deserve nothing less.

Thanks again for the opportunity to testify, and I am happy to answer any questions you might have.

[The prepared statement of Mr. Winters follows:]

Consumer
Federation
of America

1620 I Street NW
Suite 200
Washington, DC
20006

202-387-6121
info@consumerfed.org
ConsumerFed.org

Consumer Federation of America

PREPARED TESTIMONY AND STATEMENT

FOR THE RECORD OF

Ben Winters
Director of AI and Privacy
Consumer Federation of America

"Stopping Illegal Robocalls and Robotexts:

Progress, Challenges, and Next Steps"

Before The
U.S. House Committee on Energy and Commerce
Subcommittee on Oversight and Investigations

Submitted June 2, 2025

I. Introduction

Chair Guthrie, Ranking Member Pallone, Chair Palmer, Ranking Member Clarke and Members of the Subcommittee, thank you for inviting me to testify before you on this important issue. I'm Ben Winters, Director of AI and Privacy at the Consumer Federation of America (CFA). CFA is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education. Our members include over 200 local, state, and national non-profit groups and consumer protection agencies.

There is a staggering amount of monetary and emotional harm caused by scams perpetrated through robocalls and robotexts. The FBI reports the amount of money lost from internet crime alone surpassed $16 billion last year, rising 33% between 2023 and 2024.[1] According to the Federal Trade Commission (FTC), consumers lost over $12.5 billion to scams last year, an approximately 20% increase from 2023, with sharp increases in lost money for job scams, fake employment agency scams, and investment scams.[2] Truecaller estimates that 60% of scam calls are robocalls.[3] With advanced technologies like AI both increasingly available and unregulated[4], more people are getting texts with personalized scripts written by text generation services and calls with voices that *sound* like their loved ones.[5]

Even when no money is lost, there is a constant sense of annoyance and need for vigilance when people are just trying to live their lives. One figure from the

---

[1] *FBI Releases Annual Internet Crime Report*, April 23, 2025, Federal Bureau of Investigation. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report

[2] *Top scams of 2024*, March 10, 2025, available at https://consumer.ftc.gov/consumer-alerts/2025/03/top-scams-2024

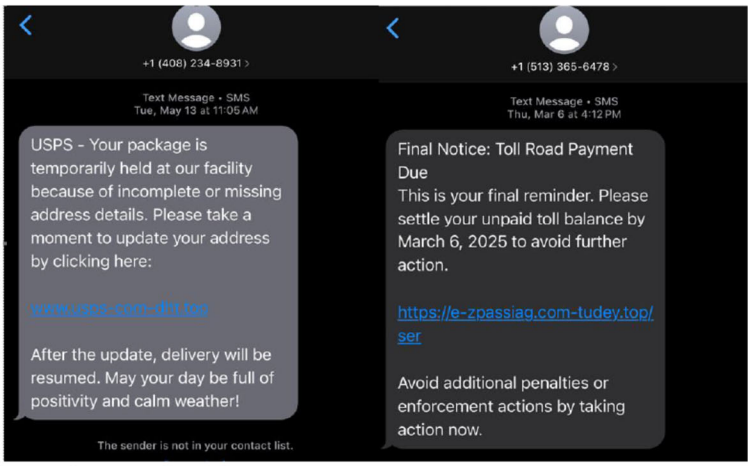
[3] *Id*

[4] Ben Winters, Scamplified · Consumer Federation of America, Consumer Federation of America (2025), https://consumerfed.org/reports/scamplified/ (last visited May 31, 2025).

[5] Charles Bethea, The Terrifying A.I. Scam That Uses Your Loved One's Voice, The New Yorker, Mar. 7, 2024, https://www.newyorker.com/science/annals-of-artificial-intelligence/the-terrifying-ai-scam-that-uses-your-loved-ones-voice (last visited May 31, 2025).

company Robokiller estimates that 19.2 billion spam robotexts were received by Americans in April 2025 alone.[6]

Americans from all over will recognize messages from scammers purporting to be EZ-Pass[7] or the United States Postal Service[8] and the annoyance, fear, or monetary loss they caused. These are real examples of those messages I've



personally received recently:

An October 2024 Federal Communications Commission (FCC) article shared that Americans are receiving 4 billion robocalls per month, and that "advancements in technology make it cheap and easy to make massive numbers of robocalls and to 'spoof' caller ID information to hide a caller's true identity."[9] This spoofing is what

[6] United States Spam Text Trends and Insights, Robokiller, https://www.robokiller.com/spam-text-insights#introduction (last visited May 31, 2025).
[7] Bill Chappell, (Don't) Click Here to Pay Your Tolls: How You Can Stop Spam Texts, NPR, Mar. 13, 2025, https://www.npr.org/2025/03/13/nx-s1-5326090/dont-click-here-to-pay-your-tolls-how-you-can-stop-spam-texts-smishing (last visited Jun 1, 2025).
[8] Smishing: Package Tracking Text Scams – United States Postal Inspection Service, https://www.uspis.gov/news/scam-article/smishing-package-tracking-text-scams (last visited Jun 1, 2025).
[9] Robocall Response Team: Combating Scam Robocalls & Robotexts, Federal Communications Commission, https://www.fcc.gov/spoofed-robocalls (last visited May 31, 2025).

leads to calls or texts that look like they're coming from *your* area or from the number of a more official source.[10]

Scammers thrive on chaos and fear like the risk of an unpaid bill or lost package to trick people into engaging with fraudulent offers or revealing sensitive information. They also capitalize on specific current events, such as when scams increase sharply following a natural disaster.[11] We fear that the current increase in regulatory, employment, and economic uncertainty present throughout the country will be a boon for scammers.[12]

These problems are getting worse,[13] and the American people deserve a full court press from Congress and federal consumer protection agencies. Entities responsible for much of the robocall and robotext problem have evaded responsibility for too long.

In this testimony, I will highlight (1) how underregulated technologies including AI are making robotexts and robocalls more effective and easier to make; (2) how federal consumer protection agencies can be doing much more to protect

---

[10] Margot Saunders and Chris Frascella, *Scam Robocalls: Telecom Providers Profit*, EPIC and NCLC (2022), https://www.nclc.org/resources/scam-robocalls-telecom-providers-profit/ (last visited May 31, 2025); *Robocall scammers using similar area code to spoof* you, 12WBOY (Apr. 20, 2018), https://www.wboy.com/news/national/robocall-scammers-using-similar-area-code-to-spoof-you/

[11] *See, e.g., Cora Lewis, After Disasters, People Are Especially Vulnerable to Scams. Here's How to Protect Yourself, Associated Press, Jan. 13, 2025, https://apnews.com/article/disaster-identity-theft-scams-a7c2ece38f6c22471f41e00a00d30f0f; After Storms, Watch Out for Scams, Federal Communications Commission, https://www.fcc.gov/consumers/guides/after-storms-watch-out-scams (last visited Jun 1, 2025).*

[12] Isabel Gottlieb, *Regulatory Uncertainty Tops List of Corporate Risks, Survey Says*, Bloomberg Law (Apr. 8, 2025), available at https://news.bloomberglaw.com/us-law-week/regulatory-uncertainty-tops-list-of-corporate-risks-survey-says; Annette Choi and Danya Gainor, *Analyzing the scale of Trump's federal layoffs in his first 100 days*, CNN (Apr. 29, 2025), available at https://www.cnn.com/2025/04/26/politics/federal-layoffs-trump-musk-dg; Talya Minsberg, *A Timeline of Trump's On Again, Off-Again Tariffs*, New York Times (May 26, 2025), available at https://www.nytimes.com/2025/03/13/business/economy/trump-tariff-timeline.html; Abha Bhattarai, *Consumer spending slows as Americans pull back amid tariff uncertainty*, The Washington Post (May 30, 2025). https://www.washingtonpost.com/business/2025/05/30/consumer-spending-tariffs-economy/

[13] YouMail Inc., U.S. Consumers Received Nearly 5 Billion Robocalls in April 2025, According to YouMail Robocall Index, Cision PR Newswire, May 6, 2025, https://www.prnewswire.com/news-releases/us-consumers-received-nearly-5-billion-robocalls-in-april-2025-according-to-youmail-robocall-index-302446599.html (last visited May 31, 2025); Getting more robocalls? Yeah, a lot of us are, U.S. PIRG Education Fund (2023), https://pirg.org/edfund/updates/getting-more-robocalls-yeah-a-lot-of-us-are/ (last visited May 31, 2025)

consumers from robotexts and robocalls; and (3) how Congress can act to protect consumers from this annoying and dangerous problem.

I. Underregulated technologies like AI, data brokers, and call spoofers are making scam problems worse.

A. *Generative AI is a fraudster's dream, and makes scam robotexts and robocalls easier to proliferate and more effective.*

Generative AI, the type of technology behind ChatGPT, ElevenLabs, Sora, and other content creation machines, is one of many types of technologies that facilitate the rise in the scale, accuracy, and plausibility of scams perpetrated through text, phone calls, and other formats.[14]

Generative AI reduces the time and effort criminals must expend to deceive their targets. Generative AI takes what it has learned from examples input by a user and outputs something new based on that information. These tools assist with content creation and can correct for human errors that might otherwise serve as warning signs of fraud.[15]

Investment scams, job opportunity scams, romance scams, impersonation scams, and phishing are the exact type that AI can "help" supercharge, and the kind that are rising *rapidly*.[16]

Text-generation tools like Chat GPT make it easier to write phishing attempts, those scams where the bad actor emails or texts something about an order or poses as a loved one or boss to get the recipient to click on something and divulge valuable and personal information by appearing as a trusted source. It also makes it easier to make variations of the same message, which can stymie filters and personalize messages to people easily. Products using text generation tools

[14] Ben Winters, Scamplified · Consumer Federation of America, Consumer Federation of America (2025), https://consumerfed.org/reports/scamplified/ (last visited May 31, 2025).
[15] Lana Swartz, Alice E. Marwick, and Kate Larson, ScamGPT: *GenAI and the Automation of Fraud*, Data & Society, https://datasociety.net/library/scam-gpt/ (last visited Jun 1, 2025).
[16] Ben Winters, *Scamplified* · Consumer Federation of America, Consumer Federation of America (2025), https://consumerfed.org/reports/scamplified/ (last visited May 31, 2025).

can also create quick and unique human-sounding "scripts" that can be either read by humans or by AI-generated voices.[17]

Filters and other "refusal mechanisms" limit some of the most harmful content, but moderation is inconsistent, inadequate, and unaccountable.[18] For example, Chat GPT refuses to output a phishing text when the prompt is "write a phishing text targeting grandmas," but will return "write an urgent text to my grandma to a grandmother asking her to send me money" to a given website.

These systems also create quicker or more aggressive or simply different variations that would reduce the texts likelihood of getting caught in filters.[19] In CFA's recent "Scamplified" report, we illustrate how easy it is to use ChatGPT to generate over 100 texts with an "urgent ask" to "add 50 dollars' worth of bitcoin to my wallet" (we included a link to a specific bitcoin wallet that ChatGPT's system included in the proposed texts). It was able to customize it with common women's names and include real hospitals in common U.S. cities to create urgency. The system continued to generate significant output texts when we asked it to "target it more to someone that might have dementia."[20]

Between the wide launch of ChatGPT in Winter 2022 and March 2025, there has been a 4151% increase in phishing attacks.[21] A 2021 study completed by Singapore's Government Technology Agency illustrated that phishing attempts made by GPT-3, the model behind ChatGPT, were more successful in tricking receivers into clicking on the email and divulging information than human-made phishing attempts.[22]

---

[17] Electronic Privacy Information Center, Generating Harms: Generative AI's Impact & Paths Forward, (2023), http://www.epic.org/gai (last visited May 31, 2025).
[18] Ben Winters, Scamplified · Consumer Federation of America, Consumer Federation of America (2025), https://consumerfed.org/reports/scamplified/ (last visited May 31, 2025).
[19] *Id.*
[20] *Id* at pp. 6-9.
[21] Adaptive Security, Adaptive Security (2024), https://www.adaptivesecurity.com/blog/ai-phishing-chatgpt-impact (last visited May 31, 2025).
[22] Lily Hay Newman, AI Wrote Better Phishing Emails Than Humans in a Recent Test, WIRED, Aug. 7, 2021, http://wired.com/story/ai-phishing-emails/ (last visited May 31, 2025).

Generative AI tools used to carry out robocalls and robotexts don't just stop with text generators, though. Voice cloning tools can now replicate anyone' speech using just a few seconds of audio, often harvested from podcasts, interviews, phone calls, or social media posts like YouTube videos.[23] Scammers have exploited this to impersonate loved ones—such as in "grandparent scams," where a cloned voice mimics a distressed family member to trick victims into sending money.[24] These tools are both accessible and affordable, with platforms like ElevenLabs offering subscriptions starting as low as $5 per month.[25]

According to a report by Consumer Reports earlier this year, major services including ElevenLabs lacked adequate safeguards to prevent misuse and often had weak or nonexistent authentication protocols in place.[26] This means that most platforms offering these services do not require the user to verify their identity or gain consent before creating or using another person's voice or likeness.[27] Single scam calls using these tools are robbing seniors of life savings within minutes.[28]

The FBI warned last year, "These tools assist with content creation and can correct for human errors that might otherwise serve as warning signs of fraud. The creation or distribution of synthetic content is not inherently illegal; however,

---

[23] Clare Duffy, AI Voice Scams Are on the Rise. Here's How You Stay Safe. - Terms of Service with Clare Duffy - Podcast on CNN Audio, CNN (2025), https://www.cnn.com/audio/podcasts/terms-of-service-with-clare-duffy/episodes/9fe98d50-96cf-11ef-aa1b-07ca04432229 (last visited May 31, 2025).

[24] Kyle Werner, New Wave of "grandparent" Scams Targeting Elderly Iowans with Fake Calls from Relatives, The Des Moines Register, Jan. 5, 2025, https://www.desmoinesregister.com/story/news/crime-and-courts/2025/01/05/grandparent-scam-iowa-attorney-general-brenna-bird/77454809007/ (last visited May 31, 2025).

[25] Grace Gedye, *AI Voice Cloning Report: Do These 6 Companies Do Enough to Prevent Misuse*, Consumer Reports (2025), https://innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf (last visited May 31, 2025).

[26] *Id.*

[27] *Id.*

[28] Alvaro Puig, Scammers Use AI to Enhance Their Family Emergency Schemes, Federal Trade Commission (2023), https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes (last visited May 31, 2025); Nation Fight Elder Fraud Center (NFEFC), https://www.fightelderfraud.org/ (last visited May 31, 2025).; Michelle Singletary, Scam Losses Hit Almost $17 Billion. The Fix Is Bigger than Self-Help., The Washington Post, May 16, 2025, https://css.washingtonpost.com/business/2025/05/16/166-billion-scam-losses-new-record/ (last visited May 31, 2025).

synthetic content can be used to facilitate crimes, such as fraud and extortion."[29] The Washington, DC Attorney General warned "We are witnessing a disturbing upward trend of scammers preying on District residents, particularly seniors, using artificial intelligence to steal their money, sensitive information and data," and the Maryland Attorney General shared last year that "Voices generated by AI are often used in scams. These are fake voices created by computers to sound like real people. Scammers use this technology, mimicking voices and even speech patterns, to trick people into believing they are talking to someone they know or trust. This makes it very difficult to differentiate between a legitimate call and a scam."[30]

The following real-life harms from voice cloning have already occurred, and underline the need for decisive action:

- **Kidnapping Hoax Calls with Cloned Voices:** Scammers use AI voice cloning to simulate a loved one in distress, demanding ransom. In one case, an Arizona mother received a call from what sounded exactly like her daughter crying that "bad men" had her – it was an AI-generated voice mimicry as part of a fake kidnapping scheme.[31] Law enforcement warns that fraudsters leverage *"fake audio or video recordings of people [victims] know, often asking for money to help them get out of an emergency."*[32] Such calls prey on panic, urging immediate payment before the ruse can be uncovered.
- **"Grandparent" or Family-Emergency Impersonation Scams:** Similar voice cloning tactics target relatives, especially seniors.[33] Scammers clone

[29] *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud*. (2024, December 3). Federal Bureau of Investigation. https://www.ic3.gov/PSA/2024/PSA241203
[30] *Consumer Alert: Spotting and Avoiding Imposter Scams*. (2024, May 31). Maryland Office of the Attorney General. https://www.marylandattorneygeneral.gov/press/2024/053124CA.pdf
[31] Erielle Reshef, Kidnapping Scam Uses Artificial Intelligence to Clone Teen Girl's Voice, Mother Issues Warning, ABC7 Los Angeles, Apr. 13, 2023, https://abc7.com/ai-voice-generator-artificial-intelligence-kidnapping-scam-detector/13122645/ (last visited May 31, 2025).
[32] *Attorney General Schwalb Issues Consumer Alert to Protect District Residents from Deepfake Telemarketing Scams*. (2025, April 18). Office of the Attorney General for the District of Columbia. https://oag.dc.gov/release/attorney-general-schwalb-issues-consumer-alert-3
[33] Charles Bethea, The Terrifying A.I. Scam That Uses Your Loved One's Voice, The New Yorker, Mar. 7, 2024, https://www.newyorker.com/science/annals-of-artificial-intelligence/the-terrifying-ai-scam-that-uses-your-loved-ones-voice (last visited May 31, 2025).

the voice of a grandchild or family member claiming to be in an accident, arrested, or otherwise in urgent trouble. The FTC has cautioned that a caller asking for money urgently, especially via wire or gift cards, is a red flag. In one incident, a victim *"got a call from her daughter's phone and she sent $1,500,"* believing her child needed bail money. Only later did she learn it was an AI-generated impostor. These AI-enhanced "family emergency" scams are on the rise, tricking Americans out of millions.

- **Executive/CEO Voice Impersonation Fraud:** Criminals have cloned company executives' voices to authorize fraudulent transfers. In 2019, scammers mimicked the voice of a German parent company CEO and convinced a U.K. subsidiary to wire them $243,000, believing the instruction was legitimate. More recently, British firm Arup lost approximately $25 million after criminals deep faked the voices (and on video, faces) of its CFO and other colleagues in a virtual meeting, tricking an employee into multiple bank transfers.[34] Such AI-aided "business email compromise" schemes by phone are an alarming evolution of corporate fraud, now reported internationally (e.g., in Europe, Asia) and targeting companies of all sizes.
- **Voice Cloning to Defeat Security Checks:** Beyond person-to-person deception, AI-generated audio impersonates individuals to bypass authentication. The FBI warns that criminals have "obtained access to bank accounts" by using cloned voice clips of the account holder.[35] For instance, if a bank's phone system uses voice-recognition passphrases, a scammer with an AI copy of the victim's voice could fool the system and gain account control. This threat extends to any identity verification that relies on voice, showing how generative AI can subvert security measures and facilitate fraud without needing to "engineer" a human victim socially.

[34] Grace Noto, Scammers Siphon $25M from Engineering Firm Arup via AI Deepfake 'CFO,' CFO Dive, May 17, 2024, https://www.cfodive.com/news/scammers-siphon-25m-engineering-firm-arup-deepfake-cfo-ai/716501/ (last visited May 31, 2025).
[35] *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud.* (2024, December 3). Federal Bureau of Investigation. https://www.ic3.gov/PSA/2024/PSA241203

B. *There is a whole host of technologies comprising the "scam stack," where the people building and using the technologies should be held responsible.*

Beyond just AI, in a recent publication, CFA highlighted the connection of several pieces of technology we're calling the "scam stack," all of which are fueling an increase in scams. These include:

- Data brokers who sell individuals' data, allowing scams to be hyper-targeted based on behavior, demographics, location, relationships, purchases, and more.
- AI companies that facilitate the faster and easier creation of the content of the messages – text, audio, images, and video.
- Robotexters, robocallers, caller-ID spoofers, underregulated and platforms, videoconferencing software, and mass email platforms that facilitate the delivery of the scam content.
- Payment platforms, banks, crypto wallet providers, and more that facilitate the transfer of funds.
- Methods of reporting – which can be improved on platforms like phone providers, email providers, social media companies, and more, where people often *receive* these.
- There is also the concern about the growing market and advertisement of "AI Agents" – tools that allow a user to have a program "take over" their device to complete a task like grocery shopping or creating documents. While they haven't come to fruition entirely yet, many would require a trustworthy user to screen share and allow remote control.

Adding to the longstanding scourge of scams, the availability of these technologies increases the urgency of swift action.

II. Federal Consumer Protection Agencies Need to Do More to Adequately Protect Consumers

Federal consumer protection agencies tasked with prosecuting and rooting out scam robotexts and robocalls are being stripped down, shut down, and

distracted. The consequence is stark: fewer agency staff hours dedicated to enforcement and rulemakings means more freedom for scammers to operate with impunity, unleashing a torrent of harassing calls and texts that fleece consumers of their hard-earned money and sensitive personal data.

In addition to the primary federal enforcers, the FCC and FTC, which are discussed at length below, attacks on agencies across the government are having ripple effects in preventing improvement in robotexts and robocalls.

In April, the Department of Justice eliminated their Consumer Protection branch entirely.[36] This is the branch that brought a landmark criminal case against a data broker for selling consumer lists of more than 30 million Americans that were used to carry out sweepstakes and other scams against elderly Americans.[37] Throughout 2025, the Consumer Financial Protection Bureau (CFPB) has been the explicit target of the administration. Whether it was multiple attempts at mass firings[38], preventing employees from doing any work[39], closing the physical offices[40], or giving companies that violated the law a corporate pardon[41], the CFPB has been a cop off its beat. When they were allowed to work, CFPB employees offered support to people who have been scammed[42] as a result of

[36] David Dayen, Justice Department Shutting Branch That Prosecutes Consumer Fraud Cases, The American Prospect (2025), https://prospect.org/justice/2025-04-24-justice-department-shuts-branch-that-prosecutes-consumer-fraud-cases/ (last visited May 31, 2025).
[37] Principal Deputy Assistant Attorney General Brian Boynton Delivers Remarks at White House Roundtable on Protecting Americans from Harmful Data Broker Practices, United States Department of Justice (2023), https://www.justice.gov/archives/opa/speech/principal-deputy-assistant-attorney-general-brian-boynton-delivers-remarks-white-house (last visited May 31, 2025).
[38] Stacy Cowley, Mass Layoffs Hit Consumer Financial Protection Bureau, The New York Times (2025), https://www.nytimes.com/2025/04/17/us/politics/consumer-financial-protection-bureau-layoffs.html.
[39] Laurel Wamsley, New CFPB Chief Closes Headquarters, Tells All Staff They Must Not Do "Any Work Tasks," NPR, Feb. 8, 2025, https://www.npr.org/2025/02/08/nx-s1-5290914/russell-vought-cfpb-doge-access-musk (last visited May 31, 2025).
[40] *Id.*
[41] Consumer Federation of America and Student Borrower Protection Center Issue Joint Memorandum on Trump-Led CFPB Pardons of Repeat Offender Corporations · Consumer Federation of America, Consumer Federation of America (2025), https://consumerfed.org/reports/consumer-federation-of-america-and-student-borrower-protection-center-issue-joint-memorandum-on-trump-led-cfpb-pardons-of-repeat-offender-corporations/ (last visited May 31, 2025).
[42] Melissa Chan, Democratic Lawmakers Warn Axing Consumer Financial Protection Bureau Will Leave Troops Vulnerable to Fraud and Scams, NBC News, Feb. 20, 2025,

schemes perpetrated over robotexts and robocalls, and continually provide essential support for other enforcement agencies around the country through the maintenance and sharing of the consumer complaint database.[43] The CFPB should also be able to proactively help consumers by intervening with monetary platforms when consumers lose money on platforms like Zelle, Venmo, cryptocurrency wallets, and more.

A. *The FCC's one-track focus on deregulation and censorship is harming consumers. They need both more authorities and a willingness to use them.*

The shadowy, fast-moving, and complicated nature of the robocommunication industry where new businesses pop up, bid on call delivery at scale, and are not adequately incentivized not to deliver illegal calls necessitates bold and robust policies and enforcement from the FCC.[44] As former Commissioner Geoffrey Starks put it in 2021, "As I have long said, illegal robocalls will continue so long as those initiating and facilitating them can get away with and profit from it. Last year's estimated 46 billion robocalls and last months estimated 4.1 billion calls are proof positive of that. We must therefore continue to be vigilant in our efforts to identify the sources of these calls and stop them in their tracks."[45]

With rising robotexts and robocalls, Americans need an FCC that prioritizes their lived experience of annoyance, frustration, and loss. The FCC was created by Congress to be an agency independent from the President.[46] However, the current

---

https://www.nbcnews.com/news/us-news/democratic-lawmakers-warn-axing-consumer-financial-protection-bureau-w-rcna192848 (last visited May 31, 2025).

[43] Ahead of CFPB Forum, Banking Committee Releases New Analysis Revealing Precipitous Drop in Consumer Complaints Processed After Trump-Musk Attack on American Consumers, United States Committee on Banking, Housing, and Urban Affairs, https://www.banking.senate.gov/newsroom/minority/ahead-of-cfpb-forum-banking-committee-releases-new-analysis-revealing-precipitous-drop-in-consumer-complaints-processed-after-trump-musk-attack-on-american-consumers (last visited May 31, 2025).

[44] *See e.g.,* Margot Saunders and Chris Frascella, *Scam Robocalls: Telecom Providers Profit* at pp. 25-30, EPIC and NCLC (2022), https://www.nclc.org/resources/scam-robocalls-telecom-providers-profit/ (last visited May 31, 2025);

[45] 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)

[46] The Federal Communications Commission (FCC), National Telecommunications and Information Administration, https://www.ntia.gov/book-page/federal-communications-commission-fcc (last visited May 31, 2025).

FCC Chairman Brendan Carr seems focused on controlling the speech and corporate hiring practices of CBS, NBC, Disney, ABC and more because they are perceived political enemies of the President.[47] FCC Commissioner Anna Gomez described the current actions of the agency as "weaponized to chill speech and to punish the press."[48] Civil society representing viewpoints from all over the political spectrum have expressed concern that this focus is on "grabbing headlines" and takes away from "more important, basic work."[49]

At the same time, Chairman Carr released the "*Delete, Delete, Delete*" initiative, in which Carr asked the American public what regulations from the FCC should be "deleted" because they "stand in the way of deployment, expansion, competition, and technological innovation." The announcement has no mention of consumer protection and runs counter to the dire need for *more* regulation in this space.[50]

In their 2022 report, NCLC and EPIC recommended that the FCC (1) require that all providers in the call path engage in effective mitigation against robocalls, (2) place clear financial consequences on providers who transmit illegal robocalls when they knew or should have known that the calls were illegal, (3) use suspension from the Robocall Mitigation Database as a mechanism to protect telephone subscribers from receiving illegal calls, (4) mandate that tracebacks conducted by the Industry Trace Group are made public, and (5) impose strict

[47] Karl Bode, Brendan Carr's FCC Is an Anti-Consumer, Rights-Trampling Harassment Machine, The Verge, Apr. 28, 2025, https://www.theverge.com/tech/656653/brendan-carr-fcc-anti-consumer-harassment-dei-trump (last visited May 31, 2025).
[48] Liam Reilly, FCC Commissioner Rips a "Weaponized" Agency Punishing News Outlets Trump Dislikes, CNN, May 15, 2025, https://www.cnn.com/2025/05/15/media/fcc-anna-gomez-rips-weaponized-agency-brendan-carr-trump (last visited May 31, 2025).
[49] Liam Reilly, FCC Commissioner Rips a "Weaponized" Agency Punishing News Outlets Trump Dislikes, CNN, May 15, 2025, https://www.cnn.com/2025/05/15/media/fcc-anna-gomez-rips-weaponized-agency-brendan-carr-trump (last visited May 31, 2025).; Brendan Carr's Bizarro World FCC, The Foundation for Individual Rights and Expression, https://www.thefire.org/news/brendan-carrs-bizarro-world-fcc (last visited May 31, 2025); Jessica J. González, How FCC Chairman Carr Has Fueled Trump's Authoritarian Takeover, Free Press (2025), https://www.freepress.net/blog/how-fcc-chairman-carr-has-fueled-trumps-authoritarian-takeover (last visited May 31, 2025).
[50] FCC Opens "In Re: Delete, Delete, Delete" Docket, Federal Communications Commission (2025), https://www.fcc.gov/document/fcc-opens-re-delete-delete-delete-docket (last visited May 31, 2025).

licensing and high bonding requirements for VoIP providers in order to address.[51] These recommendations are still sound and should be adopted by the agency.

Voice and internet service providers should be required to permanently block the worst offenders perpetrating scam calls and online fraud, including upstream providers who facilitate these calls; these bad actors often operate several steps removed from the companies that directly provide services to consumers.[52] The FCC has made progress, but its ability to issue orders against every offender is limited. A better solution would be to require providers to automatically block upstream sources of scam.[53]

The Telephone Consumer Protection Act (TCPA), enacted in 1991, restricts certain types of automated telephone dialing systems as well as the dissemination of artificial or prerecorded voice messages.[54] It's the reason consumers can ask to opt-out of many robocalls, the reason the Do Not Call registry exists, and is *supposed* to require any telemarketer to get "prior express written consent" before making a call. The FCC has strengthened the protections for and tried to limit the amount of robocalls and robo-texts using AI in recent years. However, the current FCC has delayed enforcement for these rules, and they may be the target of the "Delete, Delete, Delete" initiative or other aggressive corporate-friendly deregulation efforts.[55]

---

[51] Margot Saunders and Chris Frascella, *Scam Robocalls: Telecom Providers Profit* at pp. 25-30, EPIC and NCLC (2022), https://www.nclc.org/resources/scam-robocalls-telecom-providers-profit/ (last visited May 31, 2025);
[52] Margot Saunders and Chris Frascella, *Scam Robocalls: Telecom Providers Profit* at pp. 4-5, 12, EPIC and NCLC (2022), https://www.nclc.org/resources/scam-robocalls-telecom-providers-profit/ (last visited May 31, 2025);
[53] Kayla Ferdinand, Client Advisory on the FCC's Enforcement of the Know Your Customer Rule Against Telnyx, HWG LLP (2025), https://hwglaw.com/2025/02/07/client-advisory-on-the-fccs-enforcement-of-the-know-your-customer-rule-against-telnyx/ (last visited May 31, 2025).
[54] *Robocalls*. EPIC - Electronic Privacy Information Center. https://epic.org/issues/consumer-privacy/robocalls/
[55] FCC Opens "In Re: Delete, Delete, Delete" Docket, Federal Communications Commission (2025), https://www.fcc.gov/document/fcc-opens-re-delete-delete-delete-docket (last visited May 31, 2025); FTC Launches Public Inquiry into Anti-Competitive Regulations, Federal Trade Commission (2025), https://www.ftc.gov/news-events/news/press-releases/2025/04/ftc-launches-public-inquiry-anti-competitive-regulations (last visited May 31, 2025).

Last December, the FCC announced that 2,411 voice service providers are at risk of being removed from the Robocall Mitigation Database (RMD) and consequently blocked from the U.S. phone network.[56] Participation in the RMD requires each voice service provider to certify that they are taking certain minimum actions to detect and reduce (or mitigate) the volume of illegal robocall traffic that they transmit through the U.S. phone system; providers are not permitted to accept calls from companies that are not listed in the RMD, so removal from the RMD is tantamount to removal from the U.S. phone network.[57] There need to be better mechanisms to make the RMD useful in protecting consumers, though. There is no requirement, much less an automated mechanism, that non-compliant providers be suspended from the RMD, and the FCC does not have the scale to monitor compliance by each of the 9,856 providers that have registered.[58] The RMD should not simply require a provider to have tools to block bad actors, but a provider at any stage of a call's path should have an affirmative responsibility to block bad actors.[59]

B. *The FTC Must Finalize the Individual Impersonation Rule and Prioritize Vigorous Enforcement Against Upstream Actors Facilitating and Supercharging Robotexts and Robocalls*

Recent leadership changes at the FTC—most notably the firing of key staff and critically two Democratic commissioners[60]—have left the agency ill-equipped to

---

[56] FCC Opens "In Re: Delete, Delete, Delete" Docket, Federal Communications Commission (2025), https://www.fcc.gov/document/fcc-opens-re-delete-delete-delete-docket (last visited May 31, 2025).
[57] *Id.*
[58] Robocall Mitigation Database Listings, Federal Communications Commission (FCC), https://fccprod.servicenowservices.com/rmd?id=rmd_listings (last visited Jun 1, 2025).; Electronic Privacy Information Center, Public Knowledge, National Consumers League, In Re: Improving the Effectiveness of the Robocall Mitigation Database, EPIC - Electronic Privacy Information Center, https://epic.org/documents/in-re-improving-the-effectiveness-of-the-robocall-mitigation-database/#_ftn20 (last visited Jun 1, 2025).; Margot Saunders and Chris Frascella, *Scam Robocalls: Telecom Providers Profit*, EPIC and NCLC (2022), https://www.nclc.org/resources/scam-robocalls-telecom-providers-profit/ (last visited May 31, 2025).
[59] Margot Saunders and Chris Frascella, *Scam Robocalls: Telecom Providers Profit*, EPIC and NCLC (2022), https://www.nclc.org/resources/scam-robocalls-telecom-providers-profit/ (last visited May 31, 2025).
[60] Ashley Gold, Trump Fires Democratic FTC Commissioners, Axios, Mar. 18, 2025, https://www.axios.com/2025/03/18/trump-fires-democratic-ftc-commissioners (last visited May

protect American consumers. It reflects a focus on politics at the expense of consumers. These shifts have drained institutional knowledge, reduced productive internal discussions, and weakened the Commission's ability to respond proactively to emerging threats like robocalls, robotexts, and AI-enabled deception. At a time when bold, strategic enforcement is needed, the FTC risks being less able to act quickly and effectively to protect consumers.

The FTC's 2024 impersonation rules[61] are an important step forward, and CFA is encouraged to see the agency enforcing the government impersonation rule in 2025.[62] While the rule addressing business or government impersonation has been finalized and enforced, the rule addressing impersonation of individuals has not.[63] With the increase availability in voice cloning, it's critical that the FTC finalizes this rule. These technologies make it easier than ever to deceive consumers, often without traditional fraud indicators, and make proactive enforcement more urgent. Since those cloning tools don't have adequate controls against cloning individuals, the FTC must finalize and enforce these rules.[64]

Both rules can give the FTC powerful tools to hold platforms accountable when they allow deceptive impersonation to thrive—especially in cases where developers fail to implement basic safeguards like authentication or content moderation.

31, 2025); Lauren Feiner, FTC Workers Are Getting Terminated, Including Consumer Protection and Antitrust Staff, The Verge, Mar. 3, 2025, https://www.theverge.com/news/623242/federal-trade-commission-terminations (last visited May 31, 2025).

[61] FTC Announces Impersonation Rule Goes into Effect Today, Federal Trade Commission (2024), https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-announces-impersonation-rule-goes-effect-today (last visited May 31, 2025);

[62] FTC Highlights Actions to Protect Consumers from Impersonation Scams, Federal Trade Commission (2025), https://www.ftc.gov/news-events/news/press-releases/2025/04/ftc-highlights-actions-protect-consumers-impersonation-scams (last visited May 31, 2025).

[63] FTC to Hold Informal Hearing on Proposed Rule Amendment Banning Impersonation of Individuals, Federal Trade Commission (2024), https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-hold-informal-hearing-proposed-rule-amendment-banning-impersonation-individuals (last visited May 31, 2025).

[64] Grace Gedye, *AI Voice Cloning Report: Do These 6 Companies Do Enough to Prevent Misuse*, Consumer Reports (2025), https://innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf (last visited May 31, 2025).

The FTC must also avoid a reactive, case-by-case "whack-a-mole" approach as much as possible. It should strategically target the infrastructure enabling these scams. One important enforcement priority is to target the "means and instrumentalities" of crimes like scam texts, such as the agency's *Rytr* case last year.[65] Although that case focused on the use of Generative AI to create endless fake reviews, the same is being done for scam texts.[66] CFA, EPIC, and the National Consumers League offered support for the use of means and instrumentalities to stem harm rather than playing whack-a-mole, and also pushed for stronger remedies "would require companies outputting content to restrict outputs when prompts are clearly intended to violate the law."[67]

Similarly to the FCC, the agency must prioritize enforcement against upstream actors—such as voice service providers and AI developers—who knowingly facilitate these harmful practices.[68] These intermediaries are critical to how illegal calls and texts scale and are essential to accountability. For example, VoIP providers that knowingly transmit robocalls have been successfully prosecuted, resulting in major reductions in complaint volume. These wins resulted in an over 50% decrease in complaints about that problem between 2021 and 2024.[69] Targeting upstream facilitators works—and should be expanded.

---

[65] *Rytr LLC,* 168 F.T.C. 123 (2024) (Docket No. 232-3052), https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-approves-final-order-against-rytr-seller-ai-testimonial-review-service-providing-subscribers

[66] Lana Swartz, Alice E. Marwick, and Kate Larson, ScamGPT: *GenAI and the Automation of Fraud*, Data & Society, https://datasociety.net/library/scam-gpt/ (last visited Jun 1, 2025); Ben Winters, *Scamplified* · Consumer Federation of America, Consumer Federation of America (2025), https://consumerfed.org/reports/scamplified/ (last visited May 31, 2025).

[67] Consumer Federation of America, Electronic Privacy Information Center (EPIC), and National Consumers League, Comments *In Re Ryr LLC settlement* (FTC-2024-0041) (Nov. 4, 2024), https://consumerfed.org/wp-content/uploads/2024/11/CFA-EPIC-NCL-Rytr-Comment.pdf

[68] Grace Gedye, *AI Voice Cloning Report: Do These 6 Companies Do Enough to Prevent Misuse*, Consumer Reports (2025), https://innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf (last visited May 31, 2025).

[69] Reports of Unwanted Telemarketing Calls Down More Than 50 Percent Since 2021, Federal Trade Commission (2024), https://www.ftc.gov/news-events/news/press-releases/2024/11/reports-unwanted-telemarketing-calls-down-more-50-percent-2021 (last visited May 31, 2025).; https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-sues-stop-voip-service-provider-assisted-facilitated-telemarketers-sending-hundreds-millions; https://www.ftc.gov/news-events/news/press-releases/2022/04/ftc-takes-action-stop-voice-over-internet-provider-facilitating-illegal-telemarketing-robocalls; https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-law-enforcers-nationwide-announce-enforcement-sweep-stem-tide-illegal-telemarketing-calls-us

The FTC needs to use the full range of authorities, including the impersonation rules and unfairness doctrine, to disrupt these harmful ecosystems.

III. Congress can and should be doing more to address robocalls and robotexts.

Meaningful consequences and incentives for actors throughout the call path to block illegal calls before they're sent to consumers and root out the entities delivering them should be Congress' priority when addressing robocall and robotexts. Providers transmitting the calls must be held responsible, full stop.

While Congress gave the FCC some tools in the TRACED Act to protect consumers against robocalls, it doesn't go far enough. Enforcement needs to be rigorous, and massive unaddressed gaps remain.[70] Congress should provide a private right of action for key violations of the TRACED Act. For example, the TRACED Act already prohibits VoIP service providers from charging consumers for call blocking technologies, but there are insufficient tools to enforce it. [71] A private right of action would allow consumers to address the scourge of calls that impact them directly. In addition to there being no private right of action for that provision, onerous arbitration clauses that would prevent meaningful action from aggrieved individuals shouldn't be allowed.

We would be honored to work with your staffs to ensure that all legislation, including the Do Not Disturb Act package,[72] reflects this needed focus on enforcement to make a meaningful dent in robocalls and robotexts if reintroduced. Key updates to provisions in the bill would be essential in meaningfully addressing the problem.

---

[70] TRACED Act Implementation, Federal Communications Commission, https://www.fcc.gov/TRACEDAct (last visited May 31, 2025).
[71] *Id* at Section 10.B.
[72] Congressman Frank Pallone, Jr, *Pallone Introduces Comprehensive Legislation to Curb Onslaught of Annoying and Abusive Robocalls* (Jan. 29, 2024), https://pallone.house.gov/media/press-releases/pallone-introduces-comprehensive-legislation-curb-onslaught-annoying-and

Congress can also work to codify principles put forward in a voluntary agreement between all 51 U.S. Attorneys General and major Voice Service Providers in 2019. It included statements for those Voice Service Providers to analyze and monitor network traffic, investigate suspicious calls and calling patterns, and actually shut down that party's ability to originate, route, and terminate calls on its network when found to be violating the law.[73] While that document does explain that "failure to adhere to these principles is not in itself a basis for liability," it doesn't preclude Congress or the FCC from codifying the principles.[74] As is often the case with voluntary agreements between companies and governments, they mean nothing without enforcement. Clearly, this agreement hasn't been implemented vigorously enough.

While not solely focusing on stopping robocalls, CFA also urges the following digital policy pursuits that would address harms caused by robocalls and robotexts and improve the consumer experience in the digital age:

- ***Increase Funding and Resources for State Enforcement Entities***: Policymakers should allocate more funding and dedicated resources to state Attorneys General offices to enhance their ability to investigate, prosecute, and enforce against robocalls, robotexts, and AI-enabled scams. Many scams target vulnerable populations at the state and local level, and state AGs are often best positioned to assist victims and hold perpetrators accountable. With the resources they have, all 51 attorneys general have made significant efforts through their Anti-Robocall Litigation Task Force.[75] Additional staff, specialized training, and advanced investigative tools can empower state enforcers to more proactively monitor for AI-powered fraud, take swift action, and deliver meaningful penalties. This two-pronged approach - benefiting victims through restitution and

[73] 51 Attorneys General and Telecom Companies, State AGs Providers AntiRobocall Principles-With Signatories, (Aug. 28, 2019), https://oag.ca.gov/system/files/attachments/press-docs/State%20AGs%20Providers%20AntiRobocall%20Principles-With%20Signatories.pdf (last visited Jun 1, 2025).
[74] *Id.*
[75] North Carolina Department of Justice, *Anti-Robocall Litigation Task Force | Warning Notices* (last visited June 1, 2025), available at https://ncdoj.gov/protecting-consumers/telephones-telemarketing/fighting-robocalls/warning-notices/

compensation, while also serving as a strong deterrent against future scams - can be a powerful complement to the other policy recommendations. Equipping state-level consumer protection agencies with the necessary resources is crucial to combating the growing threat of AI-enabled scams in communities across the country.

- ***Pass a law explicitly exempting Generative AI companies from Section 230, or otherwise place legal responsibility for reasonable content moderation.*** Recent discussions around Section 230 of the Communications Decency Act have included attempts to explicitly bar artificial intelligence (AI) companies from its protections, particularly through the bipartisan No Section 230 Immunity for AI Act introduced by Senators Josh Hawley (R-Mo.) and Richard Blumenthal (D-CT). This legislation seeks to amend Section 230 to hold AI companies accountable for the content generated by their algorithms. Advocates for this change argue that AI-generated content can pose unique risks, including the spread of misinformation, harmful deepfakes, and other deceptive practices that may not be adequately addressed under the current framework. The Hawley-Blumenthal bill aims to clarify that AI companies should be liable for the outputs of their systems, especially when those outputs can lead to real-world harm. This legislative effort reflects growing concerns about the ethical implications of AI technologies and the responsibility of developers to ensure that their systems do not contribute to societal issues.
- ***Establish Transparency and Explainability Requirements for All AI Systems:*** Policymakers should mandate that AI companies provide clear and accessible explanations of how their systems work, including the data inputs, algorithms, and potential biases. This should also include moderation details for companies of a certain size. This transparency can help identify vulnerabilities that scammers may exploit and identify the appropriate actors for responsibility.
- ***Establish Mandatory Reporting and Information Sharing Practices:*** Congress should encourage or require all platforms used for creation and distribution of these scams to offer easy, one-click reporting to the appropriate authorities from the platform that they experienced the scam

on. This reduces a barrier to reporting and puts that additional work on the entity better positioned to do so.

- ***Pass Comprehensive Privacy Law; Mandate real data minimization in privacy laws.*** Data minimization is the concept that data can only be collected and used for a specific purpose requested or expected by a consumer. This is often referred to as a ban on secondary data uses, including sales. The development of new technologies like Generative AI systems shouldn't be able to be built on people's work, output, and life without actual informed consent.
- ***Empower people to sue for harms they face in a privacy or AI law.*** A private right of action empowers individuals harmed by violations of privacy or AI laws to sue violators. While enforcement agencies are often well poised to address these harms, the incentives are off when harms are not widely knowable.

CFA vehemently opposes the state AI regulation moratorium[76] provision in the reconciliation bill that passed the house.[77] The scale of these problems is one of many reasons it's not the time to restrict states from regulating the ways AI is causing harm. If states can create transparency or establish appropriate liability regimes for some of the tools in the scam stack, we should welcome it, embracing the critical roles of states not only to protect consumers but be the laboratory of democracy.[78]

IV. Conclusion

Robocalls and robotexts are not just an inconvenience—they are a growing vector for financial fraud, emotional distress, and personal data theft. These harms are

[76] Julia Edinger, State AI Regulation Ban Clears U.S. House of Representatives, GovTech, May 23, 2025, https://www.govtech.com/artificial-intelligence/state-ai-regulation-ban-clears-u-s-house-of-representatives (last visited May 31, 2025).
[77] CFA Statement on dangerous Attempt by the House to Quash All State AI Regulation, Consumer Federation of America (May 12, 2025), available at https://consumerfed.org/press_release/cfa-statement-on-dangerous-attempt-by-the-house-to-quash-all-state-ai-regulation/
[78] Kara Williams & Ben Winters, Debunking Myths About AI Laws and the Proposed Moratorium on State AI Regulation, Tech Policy Press, May 28, 2025, https://www.techpolicy.press/debunking-myths-about-ai-laws-and-the-proposed-moratorium-on-state-ai-regulation/ (last visited May 31, 2025).

increasingly supercharged by generative AI and a loosely regulated "scam stack" of technologies and platforms that enable bad actors to target consumers at scale, with disturbing precision and plausibility. As this threat escalates, our current regulatory framework is not only insufficient—it is actively being dismantled.

Congress must act. Federal consumer protection agencies need not only stronger tools and authorities but also the political and institutional will to use them. Agencies like the FTC, FCC, and CFPB must be empowered, resourced, and restored to aggressively protect consumers—especially the most vulnerable. We must also confront the technologies enabling these scams at every level, from voice-cloning tools and data brokers to voice service providers and payment platforms.

Inadequate action from the FTC and FCC as well as Congress gives a green light to scammers. Congress has the power to lead a coordinated, comprehensive response—one that prioritizes prevention, accountability, and consumer safety. The American people deserve nothing less.

Thank you again for the opportunity to testify. CFA is eager to answer any questions and help you help consumers.

/s/ Ben Winters
Director of AI and Privacy
Consumer Federation of America
bwinters@consumerfed.org

Mr. PALMER. I thank you all for your testimony. We will now move on to questioning. I will begin and recognize myself for 5 minutes.

Mr. Bercu, the Broadband Association's Industry Traceback Group conducted more than 3,600 tracebacks of suspected unlawful robocalls in 2024. Generally speaking, what percentage of unlawful robocalls are foreign originated?

Mr. BERCU. Thank you for the question. So I do not have an exact number on how many came from foreign countries or foreign entities. But we do know that a lot of the fraud comes from abroad. Illegal telemarketing, we see that sometimes originate at home, sometimes abroad. But a lot of the fraud does originate overseas.

And one of the things we have been seeing a lot lately is—because so much of enforcement and regulation was focused on who brought the illegal call into the country, what we're now seeing is some of the bad actors spinning out U.S.-based LLCs so that we are tracing it to a U.S. entity that probably has no people in the United States at all.

Mr. PALMER. Dealing with the foreign actors, though, creates some tremendous challenges because we cannot charge them with a crime right now, unless they are operating in country. Is there any recourse through civil action? I mean, what recourse do you have to deal with foreign actors? And be as brief as you can.

Mr. BERCU. Yes, I think we can do criminal action, and I think that needs to be a priority. The same people attacking us here are attacking other countries as well. I think there's a lot of opportunities for collaboration. And just to give you one anecdote, when the FBI did work several years ago with the Central Bureau of Intelligence in India to raid some of the call centers there, we saw IRS robocalls drop 80 percent overnight.

Mr. PALMER. Ms. Leggin, can you tell us how CTIA's Secure Messaging Initiative works to trace back robotexts? And how effective has this been to stop illegal and unwanted robotexts?

Ms. LEGGIN. Thank you for the question. CTIA's Secure Messaging Initiative was launched to convene the messaging ecosystem and the various players that have a role there in protecting consumers so that we can facilitate information sharing among the industry stakeholders to complement their existing industry tools to better fight the bad actors, and then to share that information with law enforcement partners at the FCC, FTC, DOJ, and the 50-State attorney general enforcement task force. To date, we have done over 172,000 robotexts as part of those information packages that we share with law enforcement. And we've done over a dozen of those packages that focus on scams that you all have seen, including government or bank impersonation, package delivery, and AI-enhanced scams as well.

We continue to focus on the areas where we're hearing that scams are happening for consumers so that we give that information to law enforcement so they can prioritize their efforts to go after the bad actors and stop the traffic at the source.

Mr. PALMER. Mr. Bercu, I want to go back to you. How widely has the STIR/SHAKEN caller ID authentication framework been implemented? And what percentage of the providers still need to implement the framework?

Mr. BERCU. So under FCC rules, it is implemented on the IP portions of providers' networks. And we have seen a shift in practice because of it, especially the high-volume illegal telemarketers. One of the things, I think, because of STIR/SHAKEN, they've moved away from spoofing to actually getting real numbers, which STIR/SHAKEN does not directly address.

Mr. PALMER. Mr. Waguespack, in your testimony you were talking about how the private right of action has been abused. Instead of protecting people who have been harmed by scam robocalls, it has led to basically a cottage industry that is attacking legitimate companies. Can you talk a little bit about that?

Mr. WAGUESPACK. Thank you, Mr. Chairman. Well, in the statements from—the opening statements from the panel and obviously from the witnesses here, there seems to be a unified focus that these bad actors a lot of times which are very hard to find which are located overseas, those are the true ones driving a lot of this issue. The private right of action provisions within TCPA are not utilized to go after those bad actors. Instead, a cottage industry has developed to go after simply where there are opportunities to make money.

And also the provisions of the PRA within TCPA are extremely broad compared to other Federal statutes. There's no caps on recovery, as you see in HIPAA, no safe harbor provision you see in COPPA, no cap on attorney fees that you see in other statutes. And so it has created a class action factory that is being exploited by just a handful of firms—

Mr. PALMER. So it has become a predatory use of the private right of action. I saw where one of the judgments was for $260-something million. So how do we respond to that?

Mr. WAGUESPACK. I think we borrow from other statutes already in place at the Federal level. You look to HIPAA to put a cap on the total recovery. They set that at 25,000. There is no cap here. It is up to 15,000 per occurrence under this statute, which absolutely drives those numbers up.

And most of these suits, they are not trying to win in court, they are just trying to drive discovery to make it very expensive and drive settlement. And you are seeing it play out time and time again. In fact, there is one law firm that has done over 155 cases over a 3-year period on this front. They have developed a niche market. There is even one plaintiff who has done almost 125 himself on this issue.

So you have a handful of folks exploiting this system. That is not helping the consumers that desperately need some of the help from these scam robocalls.

Mr. PALMER. Thank you.

The Chair now recognizes the ranking member of the subcommittee, Ms. Clarke, for 5 minutes for her questions.

Ms. CLARKE. Thank you, Mr. Chairman.

Unwanted calls continue to be the top consumer complaint received by the FCC, the Federal Communications Commission. In 2024, Americans received over 52 billion robocalls, and 49 percent of those robocalls were scams or from telemarketers.

Mr. Bercu, how has the robocall and robotext threat landscape changed since the implementation of the TRACED Act and STIR and SHAKEN?

Mr. BERCU. So I think we have made a lot of progress. But as you are recognizing, there is work left to do. We have seen complaints. They are still too high, but they have dropped pretty dramatically from the highs from several years ago.

We have seen some of the bad actors, instead of—for scam robocalls, they are about 50 percent of what they once were for scam robocalls. But we have seen the scammers move from mass robocalls to more targeted, more sophisticated attacks where they know exactly who they are calling. So that is a little bit of how this has changed over time.

Ms. CLARKE. Thank you. So we still have more to do.

With the work left undone in the fight against phone scams, it baffles me that the Trump administration is undermining the government institutions that combat them. In March, President Trump attempted to illegally removed Senate-confirmed Commissioners from the Federal Trade Commission, an independent agency with the explicit mission to protect the public from unfair and deceptive business practices like unlawful telemarketing and robocalls. And in April, in accordance with a Trump administration instruction, the Department of Justice announced plans to dissolve its consumer protection branch, which tries cases targeting large-scale scams against seniors, AI, and cybercrimes against consumers, and illegal telemarketing. This just makes no sense.

The Consumer Financial Protection Bureau, FCC, FTC, and the Department of Justice have all been hit by early retirements, terminations, and deferred resignations. And they are all agencies that combat the robocall problem we are gathered to discuss today.

Mr. Winters, how does an unstable and depleted FCC and FTC workforce impact the role both agencies play in addressing the robocall scams?

Mr. WINTERS. Thanks for the question. I mean, these underresourced consumer protection agencies is just a big win for scammers, right? Less cops on the beat mean less consequences, and they can sort of act with impunity. And so what we need to be doing—and I think was reflected in all of our testimony today, is that we need more enforcement, more resources, and more proactive behavior. And everything from firing Commissioners to budget cuts goes exactly against that.

Ms. CLARKE. Thank you. Last week, President Trump released a detailed Fiscal Year 2026 funding proposal. If enacted, this proposal would make permanent and add to the number of fired Federal employees, including 74 at the FCC, 83 at the FTC, and 32 of which are identified as consumer protection roles. The proposal also cuts 42 million from the FTC and more than 18 million of which would go directly toward protecting consumers.

Mr. Winters, what would happen to the robocall-fighting infrastructure if the Federal Government pulled back from its role, whether it be from a lack of manpower, funds, or general disinterest in holding scammers accountable?

Mr. WINTERS. In the interest of time, I'll be simple, in that it will get worse.

Ms. CLARKE. And what do the government actions we have discussed today tell the scammers and fraudsters who conduct robocalls and texts about the priorities of the U.S. Government? Do you think actions like these make robocalls more likely to occur in the future?

Mr. WINTERS. Yes. I mean, I think it incentivizes bad behavior. It makes people feel like we are absolutely not going to be able to—we're not going to get enforcement action against us, it is going to be hard to track. It is hard to track when you have a full-court press against it, and we have seen that for years. But if we are pulling back, then that is even, you know, an unimaginable harm for American consumers.

Ms. CLARKE. Very well. Well, Mr. Chairman, in their written testimony, several of today's witnesses said Congress must increase support for and prioritize enforcement actions if we truly want to stop bad actors. The experts are calling for more funding and enforcement, not less. And I ask my colleagues across the aisle to listen to them.

With that, I yield back.

Mr. BALDERSON [presiding]. Thank you, Ms. Clarke.

Next is the chairman of the full committee, Mr. Guthrie.

Mr. GUTHRIE. Thank you. I thank all the witnesses for being here. I appreciate you all being here this morning.

So, Mr. Bercu, in July of 2020 the FCC first selected USTelecom, the Broadband Association's Industry Traceback Group, as the single registered consortium to conduct private-led traceback efforts, and has redesigned USTelecom's ITG each year since.

So could you kind of explain—I know I am going between two hearings, so if you are repetitive, it helps me to repeat anyway, so how does traceback work and how has the USTelecom ITG helped the FCC with its efforts to fight illegal robocalls?

Mr. BERCU. Yes, absolutely. So traceback helps solve for one of the problems, which was when a call is spoofed and we do not know where it is coming from, the carrier does not know exactly where it came from—STIR/SHAKEN helps with that, but traceback goes even farther. And we go hop by hop in a semiautomated system through a portal, and we find out exactly where it is coming from. And in fact, in our tracebacks we have identified over 2,000 providers from 75 different countries. So we will trace it all over the world until we can find out who is making the calls and actually disrupt it there.

Our data has been used for virtually every robocall enforcement by the FCC, by the FTC, by the State AGs, so it has been a very successful partnership with the industry and government.

Mr. GUTHRIE. Well, should the technology not be in place to say if I am sitting in Bowling Green, Kentucky, and a phone call is coming in from Nigeria that is not in my data in my cell phone or anything like that, should that be—there is technology that can block that from coming. I mean, you have to sign up for it, I gather, but there is technology that keeps that from coming to your phone, does it not?

Mr. BERCU. So the challenge is that there is not perfect information at the carrier side about where that call is coming from. STIR/SHAKEN helps with that. I am optimistic that a recent rule clari-

fication the FCC did last year, that will continue to advance STIR/SHAKEN and the impact there. But that is the challenge. And so there's definitely tools to achieve that, but the carriers do not have perfect information to know that call is coming from Nigeria.

Mr. GUTHRIE. My understanding is that when a lot of these robocalls happen, they are not like I am calling Neal Dunn in Florida and faking him out on something, like I am a criminal in Bowling Green calling Neal Dunn in Florida. It is usually, spam is just thousands of calls instantaneously going out. Can carriers not determine that and block those calls?

Mr. BERCU. So that type, it still happens, but that is at a fraction of what it once was, thanks to enforcement, thanks to the TRACED Act, thanks to STIR/SHAKEN. Those types of calls are down, depending on the data you look, about 50 percent.

Where we see fraud calls, a lot of the robocalls that people still hate, a lot of those are illegal telemarketing. That is the majority of the robocalls people get, where it is telemarketing that no one consented to and they are violating the TCPA.

But what we are seeing with the scams are the scams are getting more sophisticated, more targeted, where they are targeting individuals.

Mr. GUTHRIE. OK, so Ms. Leggin, could you talk about how the CTA is trying to help fight these spam calls and robocalls?

Ms. LEGGIN. Sure thing. Thank you for the question.

As Josh said, the——

Mr. GUTHRIE. I think you probably need your mic. There you go.

Ms. LEGGIN. Try that again?

Mr. GUTHRIE. Perfect. It was on?

Ms. LEGGIN. Is it on now?

Mr. GUTHRIE. Maybe just closer to it. Yes, closer to it.

Ms. LEGGIN. Sorry. Cannot see if it is on or not.

Thank you for the question.

Like Josh's members, the wireless industry are dedicated to protecting consumers from illegal and unwanted robocalls. We helped lead the way in developing the STIR/SHAKEN framework, and we supported this committee's efforts through the TRACED Act to promote the deployment of that. And it is now working well as a call authentication tool to help protect consumers from spoofed calls. It is just one tool in the toolbox, though, so especially over the last few years we have been developing lots of different call blocking, labeling, filtering tools to complement STIR/SHAKEN as part of a multipronged approach to protect consumers from robocalls.

At CTIA, we are developing the next generation of call authentication, which is branded calling or RCTA's BCID, or branded calling ID, which gives consumers even more information about who is calling and why, to help empower consumers about whether to answer the phone again, as well as protecting them by providing consumer resources to educate them about which calls to ignore, so that we are kind of coming at it from all fronts.

Mr. GUTHRIE. I assume that could be a competitive thing between providers to say, "Hey, if you use our service, we can help you block your robocalls." I assume that would be.

So Mr. Waguespack, how about increasing fines for illegal robocalls? What would that—would such a change affect legitimate

businesses? And how could we improve collection of existing fines or overall enforcement?

Mr. WAGUESPACK. You know, obviously, FCC and FTC, I think, have done a really great job working with industry partners to develop through traceback and other initiatives to identify those, so we definitely encourage strong enforcement. And add that DOJ should also go after these bad actors any way we can. We think going through those channels as compared to unleashing a small niche cadre of plaintiff firms to go after quite frankly credible businesses just because they cannot find the bad actors has been the wrong minor approach within TCPA.

So it is that private right of action that truly we think is a disincentive to businesses to reach out to develop those partnerships with their consumers that, quite frankly, most of their consumers want.

Mr. GUTHRIE. OK, thank you. Well, my time has expired, and I yield back. Appreciate you all being here. Thanks.

Mr. BALDERSON. Thank you, Mr. Chairman.

Next up is the ranking member of the full committee, Mr. Pallone.

Mr. PALLONE. Thank you so much. And, look, I think we all know we have to do more to stop these dangerous and unwanted calls and texts that continue to bombard Americans. I mean, I get so many myself every day. And they are not just harassment, they are causing real harm. The phone scams alone defrauded Americans of $25 billion in 2023.

Now, the TRACED Act, which I authored in 2019, required the implementation of the STIR/SHAKEN call authentication technology to help verify the legitimacy of calls. So I wanted to ask Mr. Bercu, you run the Industry Traceback Group, which traces calls to their origin as required by the TRACED Act on behalf of the communications industry. In your testimony, you discuss how industry is utilizing this framework to fight the problem of robocalls and to protect consumers from scam artists.

What more can industry do to protect consumers from unwanted and dangerous robocalls and robotexts? I am going to ask you a question and then Mr. Winters, so a couple minutes.

Mr. BERCU. Sure. So thank you for the question, Ranking Member Pallone.

I think the industry, we do have blocking and labeling deployed. We do—STIR/SHAKEN is deployed. I think there is a lot at work there. But I think what our experience shows is that when we are dealing with whether it is the illegal telemarketers, whether it is the criminal fraudsters abroad, they do not stop because it gets a little bit harder. This is their business, so they keep trying to find new paths.

So I think what we see with Traceback, we are tracing them back, we have adapted to tracing back the targeted scam calls, working closely with the financial sector, other sectors as well. And I think that is more of the work to be done, complemented by very aggressive enforcement against the actual bad actors.

Mr. PALLONE. Thank you. So in March, President Trump illegally, in my opinion, fired the two Democratic FTC Commissioners, meaning that their crucial voices are missing from any discussion

at FTC of how to better protect consumers from robocalls and robotexts. And they have my full support in their ongoing lawsuit to be rightfully restored at the FTC, and I think that is the very first step that needs to be taken.

But just last year, I introduced, and I mentioned also, the Do Not Disturb Act, a comprehensive piece of legislation that aims to build on the success of the TRACED Act. And it would ensure that scam artists using illegal robocalls or robotexts cannot exploit new loopholes as new technology makes it even easier for fraudsters to steal from Americans.

So, Mr. Winters, I have 2 questions. You have 2 minutes.

Do you agree there is a need for legislation to provide updates to current laws like last year's Do Not Disturb Act, and do the FTC and FCC need more authority from Congress to fight text message scams? Is it just money and enforcement, or do they actually need more authority, if you will?

Mr. WINTERS. Thank you. Yes, so on that first question, I think there is a lot more that Congress can do, and there is more that they need to do. And so whether that is some of the provisions in the Do Not Disturb Act, like codifying the rule about AI disclosures and increasing penalties for AI-generated scam calls, there is a lot more that can be done by Congress, including giving more resources to not just FCC but to State attorneys general, who are leading the forefront of a lot of this work, and increasing collaboration.

Mr. PALLONE. But do they need more authority, though?

Mr. WINTERS. They do need more authority. One thing in particular is that they are not able to directly collect fines. They have to refer fine collection to the Department of Justice. And so they have to rely on another overworked agency to collect fines. And we see a lot of times, although there are big headlines and numbers of fines, the FCC might not actually be able to resolve and get a lot of that money back. So that is one thing that needs to be done in terms of authority.

And they also need the authority to put more automatic suspension and provisions in the robocall mitigation database, so that when there are repeat bad actors, they are automatically taken out. They cannot just stay in the robocall mitigation database. There is not enough sort of continued standards and continued enforcement using that.

Mr. PALLONE. Well, thank you. And, Mr. Chairman, as you can see, I think there is no question more authority is needed for the agencies. But I will repeat what I said earlier, which is they also need more resources and staff, and cutting back on staff and firing, you know, some of the Commissioners is certainly not the way to go if you really want to try to improve the situation with robocalls. And so I would not only ask that we try to move toward more authority to fight these scams, but also provide the resources, not cut the resources, not cut the staff.

And with that, I will yield back.

Mr. BALDERSON. Thank you, Mr. Pallone.

I am up next. So welcome everybody. I am glad you are able to join us.

Ms. Leggin, I will direct my questions to you this morning.

According to the FCC, text message scams have increased 500-fold in recent years. How have scams become more sophisticated over the years?

Ms. LEGGIN. Thanks for the question. CTIA and our members are dedicated to protecting consumers from scam and spam text messages while also making sure that legitimate ones go through, because we know that consumers open and read and trust their text messages as one of the most preferred platforms for communications today.

Over the years, we have seen bad actors increasingly target text messaging because they know that consumers open and read those texts. So as bad actors have evolved and enhanced their tactics, we've evolved and enhanced our defenses as well. So over the years, we've enhanced our blocking/filtering tools by enhancing them with machine learning and AI. We have launched the Secure Messaging Initiative, which is our work to partner with law enforcement to give them actionable information about bad actors so that they can go and take traffic off at the source, and those are working to help the FCC, the FTC, DOJ, and the attorney general enforcement task force in giving them information they can go after bad actors with.

Mr. BALDERSON. OK, thank you very much. You also answered my follow up.

Are mobile carriers and other industry players doing enough to address the growth in scam and illegal robotexts?

Ms. LEGGIN. Our industry is really dedicated to this issue. As just one metric, we blocked over 55 billion texts last year while also making sure that the legitimate ones go through and supporting over 2 trillion legitimate texts. So it really is always a balance. But we've dedicated a lot of different resources to enhancing our protections against bad actors.

In terms of more things we can do, again, we can welcome help from Congress in prioritizing resources towards enforcement so that the agencies we work with can take on more of those cases, do more investigations, and go after the bad actors to stop that traffic at the source.

Mr. BALDERSON. All right, thank you.

How well are mobile carriers engaging with States and other entities for information sharing and enforcement? For example, with the scam toll text, did mobile carriers pause delivery and contact State toll authorities to verify the legitimacy of the numbers?

Ms. LEGGIN. Our members were focused on the toll road scams as well as the other versions of that as part of our work to protect consumers from all those types of scams that impersonate legitimate businesses.

The wireless carriers as well as other partners in the messaging ecosystem, including providers of other types of messaging apps that were targeted by that type of scam, including over-the-top online-based and at-base messaging, all were working together to share information with law enforcement to help them find the bad actors responsible and take them off the field.

Mr. BALDERSON. OK, thank you. How can we get mobile carriers to better engage and pull their weight to stop the flood of robotexts

at the same level as robocalls? At the same level they did for robocalls, I'm sorry.

Ms. LEGGIN. The wireless industry and our messaging ecosystem partners are really focused on this issue. For years, we have been seeing bad actors really target the voice network because there were not blocking and other protections in place until the last few years.

In text messaging, we have actually had the ability to block and to filter and to employ up-front vetting and verification for decades. And so for a long time the messaging platform was really protected from bad actors. Of course, bad actors are getting more sophisticated and over the last few years targeting text messaging more. But this has been an area of focus and a priority for our members for years. And we continue to dedicate significant resources toward protecting consumers while maintaining trust in text messaging.

Mr. BALDERSON. OK, thank you very much. I yield back my remaining time.

Next up is the gentlelady from Colorado, Ms. DeGette.

Ms. DEGETTE. Thank you so much.

So I just got back along with many of our colleagues on this committee from a conference on artificial intelligence. And so I would like to talk with you about that today, because I think it is really being implemented in a disturbing way by scammers to find new ways to deal with Americans. A lot of us have been hearing these chilling stories about how somebody gets called by somebody who they think is their child or their parent and asked for money, and the voice sounds eerily like their loved one.

So, Mr. Winters, I want to ask you, how has AI technology been used to create more sophisticated robocall and robotext scams that target consumers?

Mr. WINTERS. Thanks for the question. It has been in a lot of different ways, and so I will categorize the two different types of AI systems in it. So one in text generation services, like sort of as I mentioned in my opening statement, whether it is something like ChatGPT or cloud that you might have played around with, or one of the ones that even has less moderation, you can create a bunch of texts really quickly that have good grammar and, you know, seems like—you do not have the bells going off in your head from them. So you can do that.

You can have a list of people's names, target-based off their location, other information you have, have it connect to a link of, you know, a wallet or a Zelle or something like that. So it is just a sort of scale and accuracy and plausibility thing.

The other big category is the sort of impersonation of people, whether that be through voice or video. And that is where you see the really harrowing stories of sort of like real-time fraud and deepfake stuff that, you know, have not only caused a lot of emotional harm but have sort of ruined people's lives. Yes.

Ms. DEGETTE. So this kind of goes without saying, but because of this degree of sophistication, even when you have an educated consumer, it becomes much more difficult to identify these scams?

Mr. WINTERS. Absolutely. I mean, I think that one thing is it is really difficult and kind of an impossible proposition to have all American people be able to spot when something is AI in the mo-

ment and then not respond to the emotional sort of "I'm your son and I'm in jail" thing, even if you are able to flag that. And then not all AI-generated anything will be a scam or a fraud, so it is complicated there. Because you do not necessarily want to teach that, or it will just get people paranoid. So it is really—it should be on the companies and on the enforcement——

Ms. DEGETTE. Right, so if we are not going to rely on the consumers by education, Ms. Leggin, what more can industry do to filter these messages and prevent them from ever getting to the victims?

Ms. LEGGIN. So as Mr. Winters said, it is a balanced approach to make sure that we are blocking the messages that we do not want consumers to receive and they do not want to receive, while also making sure that legitimate ones go through.

Ms. DEGETTE. That is right.

Ms. LEGGIN. So with AI-enhanced scams, for example, there are aspects of that that we can also detect using AI by analyzing vaster quantities of data, by enhancing our existing tools and algorithms and frameworks, and then by complementing those with large fraud teams to help protect consumers from scams.

Ms. DEGETTE. And do you think that the Federal agencies have the necessary authorities to fight against these scams? Or can companies do it themselves? Do they have the authority to do it?

Ms. LEGGIN. We value our partnerships with all the law enforcement entities, including the FCC, FTC——

Ms. DEGETTE. Right. Do you think they have enough authority to do it?

Ms. LEGGIN. We think——

Ms. DEGETTE. Yes or no will work.

Ms. LEGGIN. We think that the best authority, the best way for them to continue to help us, is by prioritizing resources towards enforcement.

Ms. DEGETTE. Resources. So that means Congress and the administration have to adequately fund them, right?

Ms. LEGGIN. We continue to work——

Ms. DEGETTE. No, a yes or no will work.

Ms. LEGGIN. Yes.

Ms. DEGETTE. OK. Mr. Winters, do you think they have enough authorities?

Mr. WINTERS. No.

Ms. DEGETTE. And why is that?

Mr. WINTERS. I mean, if they did and they had the resources as well, I think we probably would not be here today. You know, they need an ability to, as I mentioned, follow up on the fines that they levy and actually collect those. They need sort of required transparency and basic moderation obligations for AI companies. There are lots of things that just using something like unfair deceptive practices authority are—

Ms. DEGETTE. OK, thanks. We look forward to working with you to see what new authorities we want.

Mr. WINTERS. Definitely.

Ms. DEGETTE. I just have a little time left, so I want to ask you one more question. In the bill, the great big bill, a couple weeks ago that we are now learning all of the things that were included,

one of the things that was included in the reconciliation package was a 10-year moratorium on State and local enforcement of their own AI bills.

Does a 10-year moratorium on State AI bills prevent States from using evolving technologies to help fight this program? And do you think that's something Congress should look at, Mr. Winters?

Mr. WINTERS. So we vehemently oppose the moratorium provision. I do not think the moratorium as written would stop State agencies from using AI, but it would harm consumers without a doubt.

Ms. DEGETTE. Thank you. I yield back.

Mr. BALDERSON. Thank you.

Next up is my good friend Mr. Griffith from Virginia.

Mr. GRIFFITH. Let me start in a little bit different direction than I planned on going, Ms. Leggin. You were asked about adequate funding a minute ago, and I got the sense that while you were told to give a yes or no answer, you wanted to see the Federal Trade Commission and others to receive adequate funding. But it seemed to me that you were not trying to get into the debate as to what the definition of adequate funding is. Am I correct that I read your body language correctly? That you did not want to get into that debate, but you do want them to be adequately funded?

Ms. LEGGIN. That is right. It is up to each agency to allocate resources to their enforcement teams. But what we have said and what we are seeing with our work with our enforcement partners, is that sometimes the consumer fraud protection folks lack the personnel or resources they need to go after cases. So we welcome, you know, information collection or just a way to try to allocate the existing resources——

Mr. GRIFFITH. But it is also true that AI may make this much more efficient, and so we are looking forward to that too. Is that not correct?

Ms. LEGGIN. That is right, AI——

Mr. GRIFFITH. I have to move on to what I was really going to go after. But for you and Mr. Bercu, the good news is that the fraud, while terrible, is on the downward slope. And I hear from my constituents all the time about receiving robocalls. And a couple of years ago, it was all about the fraudulent stuff, and they were concerned about that. But I will tell you, in the last year, particularly in the last few months, the real concern has become Medicare and particularly Medicare Advantage solicitors calling up the folks in my district. And I have an older population, generally speaking, than most districts. And they are just driving them crazy with all these calls.

And a 2023 survey estimated that 30 percent of Medicare Advantage-eligible beneficiaries received seven or more calls a week.

I have to tell you, Mr. Chairman and witnesses, I have had constituents who have told me if they only got seven a day, they would be thrilled. That would be a down number.

So what can we do? Because this is a huge issue in my district. What can we do to make that situation better?

Mr. BERCU. Yes, I think that those calls, if they are robocalls, if they are telemarketing calls, they may be in violation of the TCPA, they may be in violation of the telemarketing sales rules.

Mr. GRIFFITH. So how do we get them to use—because I have asked. I have said to folks as I have been talking with them, "Have you put yourself on the Do Not Call list?" And they said, "Yes, but it does not seem to change anything." So how do we make that better?

Mr. BERCU. I mean, so one of the things is—and we would be happy to work with you—we have got to trace back those calls. We have to see who is ignoring the law, get that information, get that to the right enforcement authorities to go after them. And we have seen success with that. Like, the auto warranty campaign was the same. We worked very closely with the States and the FCC, and that went from the most prolific robocall campaign in America to basically zero right now. So that is the answer there.

Mr. GRIFFITH. All right, well, I will be glad to work with you in any way, because when I start going to events and I start hearing this at, you know, at a majority of the events I go to, whether it be a street festival or a meeting of folks, that tells me we have a problem.

Ms. Leggin, I got the toll texts. Of course, I called my staff assistant and said, "How come you have not kept my account up to date?"

[Laughter.]

Mr. GRIFFITH. Not realizing—I was on the road. And she said, "It is a scam, do not worry about it."

But I have gotten a number of those things since then and some others, and apparently somebody out there thinks I need a new job. And I click delete. I report as junk and delete. Does that do any good?

Ms. LEGGIN. It certainly does. That is one of the key tools that the wireless industry and our partners on the device side have made available for consumers, to delete, report junk. You can also forward your scam texts to 7726, which spells "spam" and both of those are key inputs for wireless providers and our messaging partners in making our algorithms and filtering and blocking more sophisticated and responsive to what we are hearing from consumers out there, like you and others in this room that have gotten those types of texts.

In addition, we look at those types of scams and we develop evidence on them and refer them to our law enforcement partners through our Secure Messaging Initiative as well, so that we are working to target the bad actors responsible.

Mr. GRIFFITH. All right, I appreciate that.

Mr. Waguespack—and I hope I get your name right.

Mr. WAGUESPACK. That is pretty good.

Mr. GRIFFITH. All right, not too bad.

I do not know that I really have a question for you, but I will just make a comment. As a recovering attorney, I hate the whole strike suit industry where they get an itch and they just go after things. I want people to be able to sue when they are legitimately harmed. And I just make the offer that if I can work with you in any way to try to make the law so that it lets the legitimate complaint go forward but stops the strike suits where they are just trying to make it expensive and get a settlement—you talked about

that earlier—just let me know what I can do to be of assistance. I will try.

Mr. WAGUESPACK. I appreciate that. That is the balance we are looking for, and the balance is found in other Federal statutes all across the Code.

Mr. GRIFFITH. All right, I appreciate it, and yield back.

Mr. BALDERSON. Thank you, Mr. Griffith.

Next up is Mrs. Trahan.

Mrs. TRAHAN. Thank you, Mr. Chairman.

Well, I am glad to know that the frustration of unwanted robocalls is as universal in Congress as it is with our constituents. According to one estimate, Massachusetts residents received over 43 million robocalls in the month of May alone. Each of these unwanted calls wastes the precious time of the people we represent, and there are real risks that the caller on the other end is a scammer looking to swindle them out of hundreds or even thousands of dollars.

The scourge of robocalls and robotexts must end. And yet the Trump administration does seem determined to cut enforcement agencies like the FCC and the FTC who fight for Americans every single day.

Mr. Winters, can you just explain in brief the role that the FCC plays in combating robocalls and texts and how this agency works with private-sector partners to do that?

Mr. WINTERS. Sure, thanks for the question.

The FCC has a lot of responsibility and a big thing, you know, to cover. But one of the things they do is maintain and establish the robocall mitigation database. They have enforcement and investigation teams for, you know, reading consumer complaints, taking them in, analyzing it, and trying to do enforcement when possible. And I think they also, you know, work with industry colleagues—and maybe I will speak more to that—to try to ensure that they are doing as much as they can.

But I think already, even when there were no cuts to staffing, it is really hard for them to actually make meaningful consequences for the repeat bad actors, whether it is certain ability to get the fines themselves, or the fact that there is a relatively low standard for the robocall mitigation database. There are all sorts of reasons why, even if fully staffed, they do not have quite the right authorities or the right approach. And so, you know, to cut their staffing would make it even harder.

Mrs. TRAHAN. Thank you. In February, President Trump signed the Executive Order 14215, incorrectly named Ensuring Accountability for All Agencies. This EO strips the independence from many of our regulatory agencies, including the FCC. And the FCC is essential in the fight against illegal robocalls, making the actions of the Trump administration all the more concerning.

Mr. Winters again, what effects will there be in the fight against illegal robocalls and texts if the Trump administration undermines the independence of Federal agencies like the FCC?

Mr. WINTERS. Thanks. Yes, the independent nature of the FCC and the FTC both is essential for them to be able to focus on consumer protection and not go down political pursuits. I highlighted a little bit in my oral and wrote more about it in my written testi-

mony. But particularly at the FCC, this relationship with the White House has taken priority and makes it so Chairman Carr is most of the time talking about DEI hiring practices at companies and threatening to pull licenses for airing interviews with Democratic candidates, for example, as well as, you know, just focusing on, you know, providing contracts for people like Elon Musk in getting Spectrum lines.

All of that focus is not on consumer protection, right? And one of the reasons why is because of that lack of independence where they cannot focus on that because they are sort of, you know, focusing on the priorities of the President.

Mrs. TRAHAN. Thank you. The FCC's budget justification lists cracking down on illegal robocalls as a performance indicator for the agency, which is a necessary priority. Unfortunately, the Trump administration has doubled down on its mission to hamstring the Federal Government's ability to hold robocall scammers accountable by proposing to eliminate 74 positions at the FCC in the Fiscal Year 2026 budget.

The FCC, however, is not alone in fighting robocalls. Industry has, in many instances, implemented solutions and voluntarily adopted best practices. Yes, they can always do more. But as lawmakers, we should look to build upon their good work while identifying gaps where the Federal Government can add value.

Ms. Leggin, can you discuss the importance of public-private partnerships in combating robocalls and robotexts and suggest specific ways in which Congress can accelerate the efforts that industry has already taken?

Ms. LEGGIN. Thank you. Public-private partnerships are a key tool in helping us go after bad actors so that we are stopping robocalls and robotexts at the source. CTIA's members participate in the USTelecom Industry Traceback Group to help identify the bad actors behind illegal robocalls, and our members on the wireless side, and then also throughout the messaging ecosystem, participate in CTIA's Secure Messaging Initiative, which convenes the messaging ecosystem to share information among each other and with our law enforcement partners across the Federal agencies and with the State attorney general enforcement task force so that they can take that information and go after the bad actors as well.

Mrs. TRAHAN. Thank you. Thank you to all the witnesses. I appreciate it.

Mr. BALDERSON. Thank you.

Next up is the gentleman from Pennsylvania, Dr. Joyce.

Mr. JOYCE. Thank you, Chairman and Ranking Member, for holding today's hearing. And thank you for all of the witnesses who have agreed to testify today.

When I return to my district, Pennsylvania's 13th Congressional District, I hear about the pervasive and unrelenting illegal robocalls and texts that my constituents are faced with, often on a daily basis. So many of my constituents are senior citizens. I sat down and did a senior citizen seminar twice in the district in the last month, and you hear recurrent themes. You hear the "Grandma, grandma, it's Mike, I'm in Mexico and I'm in jail. I need your help. I need it." It sounded just like Mike. I hear that repeatedly when I have these roundtable discussions with seniors.

And it seems like the scammers are getting creative and finding actually new ways to trick us with incredible-looking text messages and very convincing grandma and grandpa calls. Scammers have even learned how to incorporate AI into intimidating loved ones to convince them to turn over personal information. Credit card numbers, bank numbers. Too many of my constituents are risking their retirement savings, and subsequently they lose faith in the system that we have set in place to protect them.

We need to do better. We need to both educate consumers and anticipate the next angle of attack that these scammers will take, particularly with the assistance of our partners in law enforcement and the DOJ.

Mr. Bercu, your testimony mentioned a project piloted by the Industry Traceback Group, ITG, in partnership with banks and carriers aimed at tackling fraud and consumer financial losses. Can you elaborate on the pilot goals and successes thus far, and is there collaboration with law enforcement?

Mr. BERCU. Yes, absolutely. I think some of the most promising work our industry is doing is partnering across sectors, because the fraudsters are hurting our collective customers, whether that is banks or the carriers and your constituents.

So what we have been doing is working with banks to help them identify where their number has been spoofed, and a few carriers. So working with the carriers, getting examples of calls that the carriers see from the bank's number, getting that back to the bank, and the bank can tell us, "Oh, those were not us."

And what we are doing with that is two things. We are able to trace that back, find out who made the calls, find out who was spoofing the number, get that information in the hands of law enforcement to take action with it, but also help the bank identify and look at those customers and say, "Oh, did any of these customers that got the fake call pretending to be us have a suspicious transaction?" and helping to find that. And I think criminal enforcement has to be key here, because that—we know the scammers will use any tool available to them, and they will not stop just because it gets a little harder. They keep evolving. And so the key is going after them, and we stand ready to continue to support that.

Mr. JOYCE. And I agree, the scammers certainly have the ability to be incredibly crafty, devious, and downright evil in this regard.

Talk to me about how you interface with financial institutions to make them aware of these situations.

Mr. BERCU. So I think that is actually one of the promising things going on across the industry, is that we work directly with a lot of the financial institutions, we work with tech companies, others. Marriott was mentioned before. We worked very closely with Marriott to trace the calls pretending to be Marriott. So that is what we are doing. But there are broader conversations now about how the industries can even keep growing and continue to integrate.

In my opening testimony, one thing I mentioned that I think Congress can do to help here is a safe harbor for that fraud information sharing, because I think there are questions about rules

and risks when you do share information. So I think that is one way we can continue to lock those good partnerships.

Mr. JOYCE. And thank you. Thank you for being proactive in this.

Mr. Waguespack, many of my constituents are in rural central Pennsylvania, where internet connectivity is difficult and educational digital resources on illegal robocalls are inaccessible. How can Federal agencies and industry partner, coordinate efforts to better educate consumers specifically in rural areas with limited internet access in those digital resources?

Mr. WAGUESPACK. Well, I think on leaning into what has been done since TCPA was first initiated, where you have private-sector solutions going in and working with—we have talked a lot about FCC and FTC, but also the local law enforcement and local financial institutions on the ground there, putting that initiative out there.

Mr. Bercu talked about some of the information sharing that is done with the banks to prevent the fraud. There is also a second level down that is a good example of the education program. Through the bankers association, they have armed about 2,000 banks out there to talk to their consumers, "Here is a hit list of the things we will never ask you for, so if you get an email that has this, this, this, or this, ignore it, it is spam, here is how you call us back." And so we can use the private sector, I think, to develop some of that messaging and make sure consumers can be informed with the decisions they need to be able to fight back on their own.

Mr. JOYCE. I thank all of the witnesses for presenting here today. Mr. Chairman, my time has expired, and I yield back.

Mr. BALDERSON. Thank you.

Next up is the gentlelady from Texas, Mrs. Fletcher.

Mrs. FLETCHER. Thank you. And thanks to our Chairman Palmer and Ranking Member Clarke for convening this hearing today. Thank you to our witnesses for all of your testimony. I think it has been really helpful for all of us. And as we have heard throughout the morning, abusive robocalls and robotexts are not just nuisance, right? They are a danger. And we need to do something about that.

I appreciate the work that you are doing, and also the issues that you have brought to our attention this morning and the conversation around what we can do about it.

You know, I am concerned, as several of my colleagues have mentioned, that we are hearing consistently from you we need more enforcement, we need more coordination, we need adequate resourcing, and we need adequate staffing to be able to do some of the things we are doing in a complex and challenging environment where the technology is moving faster than Congress, faster than our agencies. And what we are seeing at the same time is that those resources both in terms of money and staff are being cut from the administration. As we speak, they are asking Congress to rescind additional funding. They are stopping funding.

And so, you know, as several of my colleagues have noted, agencies like the FCC, the FTC, and the DOJ have actually utilized the law that we passed together, the work that we have done collaboratively, to und the problems and really conduct meaningful enforcement that has stopped scammers. And now, it seems like the

administration is taking the cops off the beat in this area and in many others.

Mr. Winters, you noted in your testimony and you mentioned just earlier this morning that the Trump administration has taken steps to dissolve the DOJ's consumer protection bureau. And I believe you just said the Consumer Protection Branch of the DOJ, you just told us this morning that they had successfully prosecuted a case and stopped scammers who had—I guess it was against the data brokers who had sold the data of 30 million Americans. And that data winds up in the hands of criminals who use it in these scams and others. So I think it's really important that we understand that these agencies need to be fully funded and that shuttering something like the DOJ's Consumer Protection Branch, this expert-led enforcement agency, really puts our communities at more risk. It is not something we should be doing.

You also mentioned in your testimony that the CFPB, the Consumer Financial Protection Bureau, and the work that it has done in this area, and the administration is also shuttering or attempting to shutter that agency that Congress created and that has been really critical to protecting consumers. And that's what we're talking about in this hearing: protecting consumers, protecting American citizens from these scams.

I think that what we are hearing this morning also calls on all of us on this committee to redouble our efforts to do our work around creating comprehensive privacy laws that protect American consumers. Because what I am hearing from you and what we are seeing is that our data is being stolen, is being sold, is being used. And it is being used by these scammers.

So can you take, with the time that we have, just can you talk a little bit more about cutting the DOJ's Consumer Protection Branch as well as the CFPB, and what that would mean, Mr. Winters, in terms of protecting American consumers? In this larger context, if you want to talk too about the effort to take away the staff and the funding for these agencies that are protecting consumers from robocalls and robotexts that we are all clearly worried about and clearly concerned. We want to address how is this going to help or hurt us in that effort.

Mr. WINTERS. Yes, absolutely, and thank you for the question. I mean, very simply, taking resources away from these agencies, and in the case of the CFPB and this part of the DOJ, completely trying to stop all of their work is absolutely not going to help in the fight against these harms.

On the DOJ consumer protection case that I mentioned, yes, that is a data broker that sold a list of over 30 million elderly Americans directly to a scammer. It is not just that it ended up in the scammer's hands. Data brokers will sell to anyone at any time. And so what Congress needs to do for both scam reasons and lots of other reasons is pass comprehensive data privacy law with data minimization and a private right of action and a few other key things. Or at least, if you want to be more focused, it should be focused on restricting the sale of consumer data.

CFPB specifically, shuttering that really cuts off a central resource for people that are victims of scams, especially. They have had, you know, counselors, people that answer the phone and take

complaints and try to get things resolved for you. There are a bunch of great stories of people that literally had their scams resolved. You know, they got money back from their bank with the help of CFPB professionals. So they can do things on enforcement and work with financial actors where people are losing their money. But they also are just critical support. And they provide also tracking of those complaints and, you know, gets it to State AGs and those who can help.

Mrs. FLETCHER. Thank you, Mr. Winters. I have gone over my time. I do have more questions for the panel, so I will submit them for the record, and I will yield back. Thank you.

Mr. BALDERSON. Thank you.

Next up is Mr. Tonko.

Mr. TONKO. Thank you, Mr. Chair.

Americans received over 52 billion robocalls in 2024, which is nearly 200 calls for every American adult. Americans also have lost 25 billion annually to scams that begin as spam calls. Unfortunately, we know the scammers often target older Americans who are especially vulnerable victims to these scams. Older adults in particular lost 4.9 billion through all types of fraud last year alone.

I know I listened to the exchange that you had with my colleague, Representative DeGette. But I want to delve into this with the senior perspective.

Certain scams put even the most technically savvy at risk, scams that in some cases mimic law enforcement, hospitals, or Medicare, or the voices of family members seeming to be in danger or in need of money.

So, Mr. Winters, what specific tactics do scammers use to target seniors and other vulnerable groups?

Mr. WINTERS. Yes, I mean—and thank you for the question—scammers in general capitalize on uncertainty and fear. And especially for seniors, especially those who are on a fixed income, all sorts of concerns about an unpaid bill, a toll account that you do not quite have set up yet, Medicare, you know, potential fraud and targeting, like, they are going to be thinking that the senior citizens are good targets for it. This is exactly why we had the case where a data broker bought a large list of senior citizens and targeted them with scams. And that is, you know, a terrible thing.

And so, again, yes, they try to capitalize on uncertainty and fear. And that is why you see lost bills, job opportunities, especially in this current climate where a lot of people are getting fired and the economic uncertainty is everywhere, the job opportunity scams are going to be—more people are going to fall for them because, you know, you want a job, you need a job, you need to pay your bills.

So, you know, I think that those are some of the ways in which they are targeting everyone but, you know, are hitting seniors most.

Mr. TONKO. And what prevention strategies have been the most successful in that fight against illegal robocalls and texts?

Mr. WINTERS. Yes, so, you know, there have been really strong enforcement actions by the Federal Trade Commission of voice-over-internet providers. So, you know, I think the most appropriate and effective enforcement is going sort of upstream, especially when you are trying to get accountability for some of the actors

that are providing the content or the delivery or the targets of some of these scams.

One other really good case was the Rytr case by the FTC last year, where they targeted using the means and instrumentalities concept. In this case, it was a tool that generated lots of fake reviews, and the FTC was cracking down on fake reviews. But you can use that same tool to generate sort of an endless list of scam texts. And that sort of, you know, is a force multiplier for scammers.

And again, you know, the use of these AI tools makes it harder because, you know, there are no typos, it comes in, you know, perfect English, and there's no, you know, these weird links that we have all sort of become accustomed to, so that makes it even tougher.

Mr. TONKO. Thank you. And, Ms. Leggin, how is the wireless industry working to protect that older community and otherwise more vulnerable customers?

Ms. LEGGIN. That is a priority for the wireless industry. And to do that, we work with AARP and we support their National Elder Fraud Coordination Center, which works to take reports of victim losses in and then bring cases against bad actors.

We also were happy to participate in the FTC's Stop Senior Scams Working Group, and we led the working group focused on text messaging issues, which was a cross-sector effort to explore ways that we could do more to protect older Americans from scams.

We also participate in other working groups with consumers directly to try to push out our educational materials so that they know which text not to click on, which calls not to answer. And we have those resources on our website and our members' websites as well.

Mr. TONKO. Thank you. And the AARP that you mentioned has said that, and I quote, "The alarmingly high levels of fraud against older adults underscores that stronger protections are urgently needed."

So as technology evolves, so must our ability to combat these illegal and harmful calls and texts. Mr. Bercu, what additional tools does the Industry Traceback Group need to protect Americans from fraudulent calls or fraudulent texts?

Mr. BERCU. Thank you for the question. So I mentioned in my opening testimony I think there are ways to build on what is working and reinvest in our work. We are always adapting to the threat. A few years ago, we were only really tracing illegal robocalls. Now we are tracing threatening calls, we are tracing targeted scams. And I think that doubled last year, how many we traced. So we are always adapting and I think Congress's support through targeted immunity, through extending the cycle, will allow us to continue to invest and to innovate.

Mr. TONKO. Well, I thank you very much.

And with that, I yield back.

Mr. BALDERSON. Thank you.

Next up is the gentlelady from New York, Ocasio-Cortez, please.

Ms. OCASIO-CORTEZ. Thank you, Mr. Chair.

Mr. Winters, I want folks back home to kind of understand why this problem is happening. You know, the average American re-

ceives about 15 robocalls each month, but obviously, depending on who you are, you could be experiencing that in a day. And we know that it was not always like this. So I want folks to understand what the root of this problem is, so that they also understand what some of our solutions can be.

Is it fair to say that essentially back in the day, calls used to be routed through phone wires, through your telecom company, and so your telecom provider, whether it was Verizon or AT&T or T-Mobile, they were responsible for routing the calls and therefore they were kind of able to trace who was making them, is that right?

Mr. WINTERS. Yes.

Ms. OCASIO-CORTEZ. And then, as internet applications started to grow, then voice service providers and calls over digital services started to really expand in their infrastructure. And so it was not just your cell phone provider or even your landline provider that was in charge of your phone calls, it then became kind of these other kind of internet companies, right?

Mr. WINTERS. Yes, there are a lot of intermediary service providers. Sometimes a call will go through like eight or 10 of them before reaching you through AT&T or whatever.

Ms. OCASIO-CORTEZ. Yes, so it was really in that switch from call and telecom providers to the expanding growth of internet providers that really kind of allowed the volume of these calls to blossom, because we were not just talking about telecom regulation but internet regulation, right?

Mr. WINTERS. I think that's definitely a lot of the reason to blame for those additional intermediary providers that are harder to track through.

Ms. OCASIO-CORTEZ. And so it is no longer about who your personal provider is. As you said, you could have eight, you could have 10 of these companies routing this call. So you have the person who wants to make this robocall, and then it just leapfrogs between all these intermediary companies.

Mr. Winters, how many of these intermediary companies currently exist? And does the Government have any way to keep track of who these actors are?

Mr. WINTERS. Thanks for the question. Yes. It is kind of an unanswerable question. I think since we have been there, there are probably additional companies that have popped up and registered on the robocall mitigation database. I think last time I checked a few days ago, it was over 9,500 of these intermediary service providers. And so, you know, there is a list online. It is not a high barrier to entry. You have to, you know, register that you are a company, you have to put a robocall mitigation plan in the form. But there is not a lot of vetting there, right?

Ms. OCASIO-CORTEZ. And if these kind of abusive companies—sure, they have to register. But if we find that they are not complying, the consequence just seems to be that they get delisted from the database, correct?

Mr. WINTERS. Only sometimes. Not even that sometimes.

Ms. OCASIO-CORTEZ. OK. But without any additional penalties, is there anything to stop these companies from just immediately getting relisted?

Mr. WINTERS. No. You can, you know, if you are delisted, you can get another corporation and set it up and sign up again.

Ms. OCASIO-CORTEZ. So if you are a bad actor in this space, someone that is, you know, really perpetuating spam calls, in some cases fraudulent calls, you can be found to be breaking these rules, you can get delisted from the FCC, and then you can just turn around and it is, what a hundred bucks to——

Mr. WINTERS. I think that is not even necessarily in force yet, but yes, it will be a hundred bucks.

Ms. OCASIO-CORTEZ. Yes, it's a hundred bucks, and maybe you will have to pay it, maybe not.

Mr. WINTERS. Mm-hmm.

Ms. OCASIO-CORTEZ. So clearly, there is an enforcement problem here in keeping these bad actors out of the space.

In your opinion as a consumer protection advocate, how can we as Congress work to strengthen some of these protections? And what do you think some of the best solutions here are?

Mr. WINTERS. Yes, I think particularly to the lack of accountability in the robocall mitigation database, you know, there are a few really easy things that either the FCC can do or Congress can instruct the FCC to do to speed that up, I guess. There is a really low barrier. Right now, you have to have reasonable precautions of taking—you know, to mitigate robocalls. And that standard should be increased to effective, actual implementation. There should be requirements for the downstream providers, the bigger companies, to have responsibility for the calls that they are taking in from those eight to 10, whatever, plus intermediary service providers. And, you know, there is just insufficient tracking, insufficient consequences for repeat offenders, even—even under the company they are doing.

And one thing we advocate for to try to increase that accountability, because it is genuinely a difficult problem to try to track all these service providers, even if there is a full-court press. But one proposal we have put out there is to implement bonding for robocall mitigation database members, so that a third party is incentivized to make sure that they are actually doing what they say they are going to do and help protect consumers. So very happy to work with your office to try to make that happen. Thanks.

Ms. OCASIO-CORTEZ. Thank you very much. I yield back.

Mr. BALDERSON. Thank you.

Next up is Mr. Mullin for 5 minutes.

Mr. MULLIN. Thank you, Mr. Chair. Thank you all for being here today.

Americans lose billions of dollars every year to phone-based scams. We must crack down on illegal robocalls and robotexts.

With the recent enactment of laws that further empower enforcement agencies, there has been progress toward protecting people from these predatory practices, but not enough.

I want to recognize former Congresswoman Anna Eshoo, who represents a district neighboring mine. She has represented that for over 30 years before her recent retirement. I want to thank her for her leadership on this issue.

She introduced key legislation like the Hangup Act and the Robocalls and Texts Act, and I am proud to help uplift some of that

work that she led on in this committee and hopefully carry it forward in the future.

As we have heard today, more must be done to keep up with the rapidly advancing technology and the increasingly sophisticated tactics that scammers are using. Enforcement agencies need the tools and resources to stay ahead. The more sophisticated the methods, the more likely people fall victim to them. As more companies integrate AI into their products, it is becoming even harder for consumers to distinguish legitimate communication from fraud.

Mr. Bercu, you mentioned AI-generated messages are harder to detect and can present challenges for enforcement. How can the Government and industry better coordinate to establish safeguards to limit harm to people from illegal calls using AI?

Mr. BERCU. Thank you for the question. I think it—the fact that the criminal actors behind these calls use AI just underscores they will use every tool, every channel available to them to defraud Americans. And I think that is one of the challenges we have, is they are not going—they are already violating the law with impunity. They are committing fraud, that is violation of the criminal code. So that is one of the things I think we think, is we do need a national strategy. We do need to prioritize criminal enforcement, because they are going to continue to use the tools.

And from the carrier perspective, there is not going to be a good way to know which tools they are using because, as Mr. Winters pointed out, they are so far upstream from where our members sit.

Mr. MULLIN. Thank you for that. We know that certain people in our communities are particularly vulnerable, like seniors and individuals with limited English proficiency. Mr. Winters, what can the FTC in coordination with other agencies do to be proactive in protecting vulnerable populations from these kinds of scams?

Mr. WINTERS. Thank you for the question. You know, I think it is a lot of the same, of working to cut off the problem at the source, right? So whether we are talking about an AI tool that makes it super easy to generate a million texts that threaten to be immigration enforcement or something, for example. The enforcement action should target those developers that are putting those products out there.

Same thing goes for, you know, putting liability and responsibility for people throughout the call stream, to make sure that the calls they are taking content from are, you know, actually doing what they're saying they're going to do. But I think that the FTC and all these, you know, State attorneys general as well can be doing more to do better investigation of the members of the robocall mitigation database, making sure that the STIR/SHAKEN protocols are implemented, you know, thoroughly and it actually does what it is supposed to do. I think a lot of times, we see scam calls that have the high level of attestation, despite that being the whole point. So I think that there is just a lot more that they can do together.

Mr. MULLIN. And you also strongly assert, Mr. Winters, in your testimony that the FTC's overall enforcement capacity has been diminished by the recent unlawful firings of two Democratic Commissioners and deep staff and budget cuts at the agency. So how are

those agency cuts going to hinder FTC's ability to advance its efforts to combat illegal robocalls and robotexts?

Mr. WINTERS. It will hurt their ability to do so. As we have talked about, it is already a really difficult issue, even if you are trying your best and have all the resources you can. If you are taking people away, especially at an agency like the FTC that has a really broad jurisdiction, of course you are going to have less resources, less creative cases, just because, you know, more things are being put on less people, and the priorities are not there either. And so especially without the Commissioners, two of the five Commissioners, you do not get dissent, you don't get the conversations that might generate more creative ideas or different ideas. And so between that and the staffing, it will just make it a lot harder.

Mr. MULLIN. Thank you for that. I yield back.

Mr. BALDERSON. Thank you. Next up is the gentleman from Texas, Mr. Pfluger.

Mr. PFLUGER. Thank you, Mr. Chairman. Thanks for the witnesses being here.

I want to take a little bit different approach on this and just talk about a little bit of the impact that I am not sure has been fully discussed today, and that is to physicians. And in the process of getting screenshots of the physicians in my district, and one in particular who is showing me kind of the impact of about 20 a day that they are getting, that is really preventing—these calls, these robocalls are preventing that physician from being able to take calls from the ER or from labor and delivery. And it is pretty concerning.

So apparently, the apps that they are using to either diagnose or have conversations with their patients—the Abridge app is one of them, and then there is another app, and I am not familiar with these, so I am not the expert on this—but you cannot use those apps when calls are coming in.

And so I just wrote down from the screenshot the calls that recently came in. This was from last week on Friday: 2:31, 2:53, 2:57, 3:48, 3:53, 3:58, 3:59, 4:38, and 4:48. And in that period of time, starting at 2:30, ending at almost 5:00 p.m., you know, there were a number of patients that were disrupted.

So I know we are beating a dead horse with just how painful these things are. But that actually is pretty serious, you know, when they cannot take a call from the labor and delivery section saying, "Hey, we have an incident here that you need to get up pretty quick and, you know, deliver."

So I will start with Ms. Leggin. And, by the way, thank you all. I know we are all working together to try to solve these. But, you know, to what extent do you see TCPA and TRACED being effective? And then I will go a step further. I mean, we have had these discussions already in this hearing but, you know, the sense of urgency and what else needs to be done to prevent that physician and all the other physicians from having to deal with that in the middle of what could be an emergency situatio.

Ms. LEGGIN. Thank you for the question. And that seems like a serious issue.

TRACED and the TCPA are great tools that are helpful and helping bring enforcement actions against bad actors under the

TCPA if you are violating those consent, autodialer, prerecorded voice provisions. But unfortunately, bad actors do not care about the TCPA or other laws, so they are going to spam you no matter what. And that is where our work with law enforcement partnerships on the calling side through the ITG or on the texting side through the Secure Messaging Initiative—to bring investigations against those bad actors so that we are stopping those at the source are really helpful.

Mr. PFLUGER. Yes, go ahead.

Ms. LEGGIN. And I was just going to say you have heard me say throughout this hearing, we would welcome help from Congress in prioritizing resources towards enforcement to bring more cases against those bad actors.

Mr. PFLUGER. What do you think we can do—and anybody is open to answer this. What do you think we can do for hospitals in general? You know, for those that are providing emergency services. Because nobody is using a pager anymore. It is all cell phone. Maybe they need to go back to that.

But what can we do to think creatively to really stop that for those—I mean, every constituent of mine wants it stopped. But are there specific ideas?

Ms. LEGGIN. That is a good question. You know, it is a really challenging issue, especially when we want to make sure that critical public safety, public health services need to get their calls through. You know, the same tools that we apply to protect consumers can protect, you know, the personal lines of physicians and other things. Call blocking, call labeling, call filtering services, and then combining that with enforcement so that we are stopping those at the source.

Mr. PFLUGER. This particular physician goes through, deletes and, you know, reports junk and does—reports it and does all that. So it sounds like it has been a continued issue.

I will go to Mr. Bercu. When we look at the gaps, and just kind of building on this same theme, you know, are there specific things that you would have us do to address those gaps and, if so, maybe describe how they affect, let's just go with the physician sector, healthcare.

Mr. BERCU. Yes, absolutely. And I think, by the way, I think we have the right framework. Mr. Winters was talking about the robocall mitigation database, and I could not agree more, we need to find ways to quickly find the bad actors in that database, get them out. The FCC does require that providers have to do due diligence about who they take traffic from. So we are developing the data to see who keeps taking traffic from these shell companies. So I am optimistic we will continue to make progress.

There are—as Ms. Leggin mentioned, there are blocking, labeling, and specific-use cases. I know we work sometimes with some companies that sit on the inbound call side for a hospital. And we have had successful—and they have really sophisticated tools to see which is the consumer and which is not. So those are some of the things I would recommend that the doctor looks into.

Mr. PFLUGER. Thank you. My time has expired. I yield back.

Mr. BALDERSON. Thank you.

Next up is Mr. Allen for 5 minutes, please.

Mr. ALLEN. I want to thank Chairman Palmer for convening this hearing. And you probably heard this today from every district in the country, but my constituents frequently express their frustration with the persistent barrage of illegal robocalls, robotexts. They are a nuisance, and they are a significant distress, anxiety, particularly for our elderly population, because some of these folks are up to no good and are taking advantage of our constituents.

These communications often exploit our most vulnerable individuals. And it is really eroding our trust in the telecommunications systems. I look forward to receiving updates on the progress made under existing laws and exploring actionable next steps to protect consumers and strengthen enforcement. And I want to thank our witnesses for being here with us.

Mr. Bercu and Ms. Leggin, there has been a lot of public and private action in the fight against illegal robocalls, both under the Telephone Consumer Protection Act and under the TRACED Act. Generally, robocall numbers have been on a downward trend over the years.

If illegal robocalls trends have dropped, why am I still getting so many complaints from my constituents?

Mr. BERCU. Yes, I think some of the members sort of expressed that. There are really positive numbers, the 50 percent reduction in scam robocalls. But not everyone is having the same experience. Some people do get more than others. So that is an ongoing challenge.

But there again, I think we have the right framework. We are tracing back those illegal calls. Some of those are illegal telemarketing. We are tracing them back. That information is making its way to enforcement.

And in terms of the scam calls in particular, we know that they are going to keep going. Just because it gets a little harder does not mean they say, "OK, we are going to go do another line of business." They are just going to keep coming through a new channel, through a new method, through a new shell company. And so that is really where we think the answer has to be actually going after them with criminal enforcement. And we think that should be a priority.

Mr. ALLEN. Ms. Leggin, would you care to add to that?

Ms. LEGGIN. I agree with what Mr. Bercu said. You know, the framework that we have in place continues to show progress, and we continue to build upon that with new tools and enhance those tools with machine learning and AI and the latest technologies to make them even better. And I agree that more focus on enforcement by taking those bad actors off the field is where we need help.

We saw a group of State attorneys general, for example, recently get a judgment against prolific robocaller Jonathan Spiller, so that that prevents him from starting new businesses or otherwise kind of popping up again after getting an enforcement action against him.

So things like that will continue to help make a big difference and continue to drive those robocall numbers down.

Mr. ALLEN. So we are identifying these bad actors. It is just a matter of prosecuting them?

Mr. BERCU. In many cases we are, where we are getting good data that can further the investigation. It is one of the reasons that I am actually optimistic about continuing to work across sectors, because we can now combine some of our data with some data that the banks can get that through, as Ms. Leggin mentioned, the AARP's National Elder Coordination Council. Really aggregate data. Because that is one of the challenges. If it is one scam, it is hard to get a prosecutor involved. But if you can show it is a multi-million-dollar scam, you can. So that is still where some of the work needs to go.

Mr. ALLEN. Well, thank you.

Mr. Waguespack, in April 2025, FCC issued a notice of proposed rulemaking. They proposed a 2-year time line for providers to maintain non-IP infrastructure to either complete their IP transitions or fully implement one or more of the available non-IP caller ID authentication frameworks in their non-IP network.

In your opinion, is the FCC's 2-year time line reasonable?

Mr. WAGUESPACK. I would yield to my colleagues to the right on more of the technical time line there, because they are the ones that are going to be implementing some of that.

I would say from our perspective, if I could just—since I have the mic for a second—bring in another universe of recipient of a lot of these robocalls that we have not really addressed yet, is what lies in between business and consumers a lot of times is small business. Because a lot of those recipients, they are kind of part consumer, part business owner. Their cell phone becomes their business phone and their residential phone, et cetera. They cannot qualify for Do Not Call if it is considered business or not.

That is a vulnerability that we hear a lot from our members on small business. And it is also a vulnerability that is being exploited from some of these predatory lawsuits I mentioned earlier in my opening statement.

Mr. ALLEN. All right, you have answered my second question there about the impact, particularly in rural areas, and other non-IP networks.

Ms. Leggin, in your testimony you discuss how CTIA and its wireless partners embark on the next generation of call identification solutions, namely branded calling. What is branded calling, and how will it help reduce scams and scam calls?

Ms. LEGGIN. Thank you for the question. CTIA is building the next generation of branded calling by bring together the wireless ecosystem players to give the consumer more information about who is calling and why. And branded calling, as the name suggests, means that the logo of the caller comes through.

This framework provides verified identity of the caller and builds upon the STIR/SHAKEN framework to make that information that comes through to the caller even clearer and better. So by doing so, we help empower the consumer to make better choices about do you want to answer the call or not. And we think that will be a really helpful tool in continuing to protect consumers from scam calls.

Mr. ALLEN. Good. I thank all of you. And, Mr. Chairman, I yield back.

Mr. BALDERSON. Thank you. I now recognize the Ranking Member Clarke.

Ms. CLARKE. Thank you, Mr. Chairman. Mr. Chairman, I have a request for unanimous consent. Representative Sorensen sent a letter to the chair and myself about the importance of taking action and his bipartisan QUIET Act, which addresses some of the issues raised here today.

I ask for unanimous consent for his letter to be entered into the record.

Mr. BALDERSON. We received the letter. And seeing no objection, accept it.

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

Mr. BALDERSON. Thank you.

Ms. CLARKE. Thank you.

Mr. BALDERSON. Next up, the gentleman from the great State of Ohio, Mr. Rulli, for 5 minutes.

Mr. RULLI. Thank you, Chairman.

The question will be directed at Ms. Leggin. This is a bipartisan issue and I think the most engaging, sensitive constituency that we have, I would say, over 60. When I was young, I used to listen to a lot of talk radio in the 1980s and the 1990s. And it was a subject then and it is just a subject as much right now today. They want to enjoy their peace and their tranquility. And these robocalls just keep ruining it.

So what percentage of illegal robocalls and spam text messages originate abroad? And where do they primarily originate from? What part of the world?

Ms. LEGGIN. Thank you for the question. It is a mix of robocalls and robotexts that come from both the U.S.——

Mr. BALDERSON. Ms. Leggin, your mic, please. Sorry.

Ms. LEGGIN. Sorry. Microphone.

It is a mix. It comes from bad actors that are both located in the U.S. and outside the U.S. And we take seriously our work to protect consumers from illegal robocalls and robotexts that originate abroad. It continues to evolve. But southeast Asia is one area, including India, and the call centers there that Mr. Bercu mentioned earlier continues to be a source of illegal and unwanted robocalls and robotexts.

So we support efforts like those at the FCC, where they have memorandums of understanding with international partners, with States to collaborate on enforcement against the bad actors located outside of the U.S.

Mr. RULLI. Out of curiosity, do you think that America has migrated into an evolution where we have gotten better than we have in the early 1990s? Or not really?

Ms. LEGGIN. We have definitely gotten a lot better than the early 1990s. And especially over the last 10 years on the robocall front, we have had a lot of attention to this issue from this committee, through the TRACED Act, from the FCC and other agencies giving us more tools, more authority to go after bad actors in this space. And there has been a lot of innovation in the texting space as well over the years to make our onboarding, our filtering, our blocking and consumer reporting tools even better. And we continue to enhance those very day.

Mr. RULLI. Thank you so much. And then I have a question for Mr. Bercu. To fight against robocalls and spam texts, the FCC has formed international alliances and partnerships with countries like Australia, Brazil, Canada, the EU, Romania, Singapore, just to name a few. How should we move forward with helping the FCC handle enforcement with countries that are bad players, like in Laos and in Cambodia, who seem not wanting to get involved in the Government? How can we get more involved with these countries that are allowing these illegal procedures to happen?

Mr. BERCU. That is a great question.

Mr. BALDERSON. Is your mic on?

Mr. BERCU. Sorry. That's a great question.

So I think one of the things we would love to see is that is why we do need a national strategy, because the same people attacking us here are also attacking consumers in Canada and the U.K. and Thailand.

I think as we go around the world, there is more of a coalition of the willing to go after the criminal actors here. And so, you know, the FCC has those MOUs with other countries. But we also need it coming from the criminal law enforcement authorities at that level, and working together to take down some of these entities. And organized crime, really, is what we are going after with those.

Mr. RULLI. Do you think it is obtainable?

Mr. BERCU. I think it is obtainable. I think we have seen some other countries take very aggressive actions. For example, Myanmar is now building out their reporting about these fraud centers in Myanmar. The Thai Government shut off the power, so they are going to generators. But I think there is room to continue to build on those and build those collaborations. Because again, those same entities are attacking us all over the world.

Mr. RULLI. Outstanding. Thank you so much.

And with that, I yield my time back to the chair.

Mr. BALDERSON. Thank you. Next up is the gentleman from Texas for 5 minutes, Mr. Weber.

Mr. WEBER. Thank you, Mr. Chairman.

Ms. Leggin, I am coming to you. I had to be at another hearing for a long time. I apologize if this is redundant.

In many cases, robocalls are so believable that millions of Americans fall prey to the various scams every year. However, the recent rise in robotexts, as we call them, adds a new layer of complexity. What makes combating spam and scam texts—why is that more difficult than robocalls?

Ms. LEGGIN. Thank you for the question. CTIA and our members throughout the messaging ecosystem take seriously our goal to protect consumers from illegal and unwanted robotexts. Voice and text are different technologies, and they present different ways that bad actors target consumers. So we've got different problems with different solutions.

So it is just a different ecosystem where we still bring blocking tools to bear in the texting space. For example, we blocked over 55 billion scam texts just last year. But that is just one piece of the——

Mr. WEBER. Can I give you my cell phone and have you block some more?

[Laughter.]

Ms. LEGGIN. Happy to help, yes.

We continue to up those efforts and bring new tools to bear.

In messaging, we've got tools throughout the message flow, including up-front vetting and verification services that help identify whether legitimate businesses are who they say they are. And it helps deter bad actors from getting on the platform in the first place. We've got sophisticated algorithms, machine learning, AI, and fraud teams that look at ways to protect consumers from unwanted and illegal text messages in the middle, and then we've got consumer reporting on the back end so that you can delete and report junk, or you can forward your spam text to 7726. And the wireless industry takes those in to use to enhance our protection tools so that we are taking in that consumer feedback to make those tools even stronger.

Mr. WEBER. Do you know, this question may be a little bit to the left, do you know or are you all able to determine how many texts a company sends out at any given time? They send out a million, 10 million? Can you identify that, know that?

Ms. LEGGIN. So companies use a variety of different platforms to send out their communications. So to us, that is not something that we look at. What we look at is trying to make sure that we are looking for suspicious patterns, indicators of spam or other illegal things to target those, to protect consumers from those. Otherwise, it's really a balance to protect consumers while also making sure that legitimate business communications go through.

So like I said, we blocked 55 billion last year. But we also let—you know, supported 2 trillion texts to go through. So it is always a balance.

Mr. WEBER. Well, I think a trillion of those came to my cell phone.

Mr. Bercu, I am going to come to you. As you are probably aware, there are varying levels of jurisdiction and oversight when dealing with either foreign or domestic entities.

Now, I missed the first half of his question. So if this is redundant—did he ask you about this?

Mr. BERCU. He may have but I am happy to——

Mr. WEBER. Well, what are some of the unique challenges regulators and law enforcement face when dealing with foreign-originating robocalls? Is that what you all just went through?

Mr. BERCU. We went through an aspect of that. But I am happy to talk about it. We have traced—in our tracebacks, we have traced calls——

Mr. WEBER. And how do they vary from domestic ones?

Mr. BERCU. Yes. So I think in our experience, both on what we have seen through our tracebacks but also some public reporting, I think what we see is that illegal telemarketing, often that is homegrown and there are entities—John Spiller, Ms. Leggin mentioned earlier—that might be more local. But we do see a lot of the fraud comes from abroad, especially the scaled fraud.

So in terms of other countries, I think those same actors are attacking everyone around the world. I think there is a lot of work

to be done collaboratively with other countries. We have traced those, we do trace those, we find those entities. We sometimes see entities log into our portal saying they are a U.S. company but log in from abroad. So I think we are building that dataset and it can arm criminal law enforcement to go after it.

Mr. WEBER. OK, very quickly. Our first responders, medical professionals, and others often deal with individuals who are at their most vulnerable, making them a prime target for potential scams and attacks. So the question is going to be—but I have one to ask real quick—how do we address spoofing related to hospitals, police, government agencies, and other public service entities? And I want to hone in on this as a question for the two of you all. And we will go back to you, Ms. Leggin. How about have you all ever encountered what is known as swatting?

Ms. LEGGIN. Yes.

Mr. WEBER. And how often? Or would you put a percentage on that? And what do you do about it?

Ms. LEGGIN. So we take swatting very seriously. You know, that is where someone calls in a fake emergency and has, you know, a police team go to your house. That is something where we are not really seeing that as much on wireless 911 calls as much as it is on other networks. But regardless, the same tools that protect consumers from illegal and unwanted robocalls—like call authentication, like STIR/SHAKEN, call filtering, call blocking, and then tracing back calls after they have gone through to find the bad actor responsible—are all things that we encourage to address swatting, as well as partnerships with law enforcement to go after that criminal activity as well.

Mr. WEBER. OK. I thank you, Mr. Chairman. I yield back.

Mr. BALDERSON. Thank you. Seeing no other Members here wishing to ask questions, I would like to thank our witnesses again for being here today. Without objection, that will be the order.

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

Without objection, the subcommittee is adjourned.

[Whereupon, at 12:25 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

Documents for the Record

Committee on Energy and Commerce, Subcommittee on Oversight and Investigations

Hearing Titled "Stopping Illegal Robocalls and Robotexts: Progress, Challenges, and Next Steps"

June 4, 2024

1. Letter to Chairman Palmer and Ranking Member Clarke from Representative Sorensen, submitted by the Minority.

ERIC SORENSEN
17TH DISTRICT, ILLINOIS

COMMITTEE ON AGRICULTURE

SUBCOMMITTEE ON CONSERVATION, RESEARCH, AND BIOTECHNOLOGY

SUBCOMMITTEE ON GENERAL FARM COMMODITIES, RISK MANAGEMENT, AND CREDIT

COMMITTEE ON ARMED SERVICES

SUBCOMMITTEE ON TACTICAL AIR AND LAND FORCES
SUBCOMMITTEE ON READINESS

Congress of the United States
House of Representatives
Washington, DC 20515-1317

1314 LONGWORTH HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-1317
(202) 225-5905

423 17TH STREET, SUITE 201
ROCK ISLAND, IL 61201
(309) 786-3406

403-1/2 NE JEFFERSON STREET
PEORIA, IL 61603
(309) 621-7070

401 E. STATE STREET, GROUND FLOOR
ROCKFORD, IL 61104
(779) 513-4960

June 4, 2025

Honorable Gary Palmer
Chairman
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Honorable Yvette Clarke
Ranking Member
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
2322A Rayburn House Office Building
Washington, D.C. 20515

Chairman Palmer and Ranking Member Clarke,

Endless robocalls and robotexts are more than just annoying and frustrating – they can cause seniors to lose entire life savings when malicious scammers take advantage of new technology to impersonate their loved ones, their bank, or the government. We must take action to address this issue and hold bad actors accountable. With AI's growing ability to convincingly imitate voices and create deceptive and convincing fraudulent messages, the stakes have never been higher.

My bipartisan Quashing Unwanted and Interruptive Electronic Telecommunications (QUIET) Act address this issue at its core. It would hold bad actors accountable with higher penalties than are currently on the books and ensure that if criminals use Artificial Intelligence to impersonate an individual to defraud someone that they'll be held accountable. Too often, we see stories of family members, particularly older family members, who have been duped by criminals who pretend to be a loved one in a compromised position and in need of assistance, having their hard-earned savings stolen as a result.

Americans are fed up with the endless stream of messages pretending to be either the United States Postal Service with updates on packages that weren't ordered or fake messages from someone's bank about purchases they did not make. The illegal spam robocalls and robotexts also make it harder for regular Americans to tell when something really has gone wrong and they need to act.

We need to do more to build trust in our systems, and addressing robocalls and robotexts is a step in the right direction. I am thankful for the Committee's continued attention to this issue. I stand ready and willing to work with my colleagues on both sides of the aisle and with the Committee to bring an end to illegal and predatory robocalls and robotexts.

Sincerely,

Eric Sorensen
Member of Congress

Joshua M. Bercu Executive Director, Industry Traceback Group

Senior Vice President, Policy, USTelecom — The Broadband Association

Questions for the Record Responses

Stopping Illegal Robocalls and Robotexts: Progress, Challenges, and Next Steps.

July 7, 2025

The Honorable Russ Fulcher

1. **As of April 2025, more than 221 million phone numbers are currently registered on FTC's Do Not Call registry.**
    a. **What types of calls does the Registry block? What calls are allowed? Why does the Registry not block spam calls?**

The Do Not Call Registry was established two decades ago to allow Americans to opt out of unsolicited telemarketing calls. Telemarketers must check the Registry before making unsolicited telemarketing calls, but unscrupulous illegal telemarketers and criminal scammers ignore the Registry entirely to blast their unsolicited and illegal calls to consumers.

In terms of blocking, voice service providers have implemented various types of blocking, including network-based blocking of invalid, unallocated, and unassigned numbers, analytics-based blocking based on traffic patterns, and blocking based on Do Not Originate (DNO) Lists, including the DNO Registry maintained by the Industry Traceback Group (ITG). The DNO Registry includes numbers intended only for inbound calls to the Social Security Administration, Internal Revenue Service, courts and public safety offices, banks, retailers, and other trusted entities. DNO is a blunt, but very effective tool. Calls made from numbers on a DNO list will be blocked, as those numbers should never make outbound calls.

    b. **Is extending the Do Not Call registry to block spam calls feasible?**

The Do Not Call Registry has been highly effective in stopping unsolicited spam calls from actors that follow the law, such as legitimate telemarketers. However, criminals engaged in fraud and unscrupulous telemarketers that ignore the laws are not, and will not be, deterred by the Do Not Call registry or implementing rules.

2. **How effective has the Registry been in reducing illegal robocalls?**
    a. **What issues or challenges are we seeing with the use of the Do Not Call registry?**

The Do Not Call Registry has been highly effective in reducing unsolicited telemarketing calls. But it is not the right tool in addressing illegal robocalls from actors that ignore the law. For those actors, traceback, analytics-based and DNO blocking, and call authentication can help. While there is more work to do, these efforts have led to substantial declines in scam robocalls as well as unwanted call complaints to the FCC and FTC. Criminal enforcement also is critical to deter the actors that violate our laws with impunity to defraud Americans.

3. **How do we address flagrant violators of the Do Not Call registry, particularly those who are based overseas, and outside the jurisdiction of U.S. laws and enforcement authorities?**

Criminal enforcement and coordination with partners abroad is critical to deter the actors that ignore the Do Not Call Registry and other applicable laws in their efforts to defraud Americans.

The Honorable Lizzie Fletcher

1. **Mr. Bercu, there are more than 140 languages spoken throughout Harris and Fort Bend counties. In the Gulfton neighborhood in my district, people speak more than 50 languages.**

   When we discuss the potential victims of abusive and dangerous robocalls and robotexts, those in our communities who speak English as their second or third language or are learning English now, are particularly vulnerable to these scams. Whether these individuals who are being scammed out of their money or their sensitive personal data, they are at a disadvantage when trying to discern what is real and what is a scam.

   What steps can enforcement agencies and Congress take to protect these communities from fraudulent robocalls and robotexts, particularly those that seek to exploit these language barriers to target vulnerable populations?

Criminals that exploit language barriers to target vulnerable populations are an ongoing challenge. The tools deployed by voice service providers, including analytics-based blocking and call authentication, can help reduce but not eliminate these scams. Traceback also can help. The ITG, working closely with law enforcement and other industry partners, has successfully traced calls targeting non-English speakers and we stand ready to continue to do so. Ultimately, to best fully stop these criminals, the government must prioritize criminal enforcement, including against transnational actors.

CTIA Responses to Questions for the Record
Ms. Sarah Leggin
Subcommittee on Oversight and Investigations Hearing
June 4, 2025
"Stopping Illegal Robocalls and Robotexts: Progress, Challenges, and Next Steps."

The Honorable Russ Fulcher

1. **As of April 2025, more than 221 million phone numbers are currently registered on FTC's Do Not Call registry.**

    a. **What types of calls does the Registry block? What calls are allowed? Why does the Registry not block spam calls?**

    b. **Is extending the Do Not Call registry to block spam calls feasible?**

The Do Not Call ("DNC") Registry is a list of telephone numbers that telemarketers are prohibited from placing unsolicited calls to. American consumers can register their telephone number on the DNC Registry to indicate that they do not wish to receive unsolicited telemarketing calls. Consumers may consider unsolicited telemarketing calls to be a type of spam call, which would be covered by the DNC Registry's rules. Both the Federal Trade Commission ("FTC") and the Federal Communications Commission ("FCC") have rules that prohibit telemarketers from placing unsolicited calls to telephone numbers on the DNC Registry. In 2023, the FCC clarified that the DNC Registry's protections include text messages, meaning telemarketers are prohibited from sending unsolicited marketing texts to telephone numbers on the DNC Registry, in addition to unsolicited telemarketing calls.

To help balance the need for legitimate callers to reach consumers with the need to protect consumers from unsolicited telemarketing calls, the DNC Registry rules do not apply to non-marketing calls, such as prescription updates, delivery notifications, and other "transactional" calls that businesses frequently make to consumers. The DNC Registry rules also have certain exceptions, including an exception for consumer consent: If a consumer lists their telephone number on the DNC Registry and subsequently gives consent to a caller to receive telemarketing calls, the caller is allowed to contact the consumer. Of course, a consumer may later revoke their consent, at which point the caller may not contact the consumer.

Because the DNC Registry is a list of telephone numbers, the DNC Registry cannot block calls. Instead, it is an informational resource that telemarketers consult when working to comply with U.S. telemarketing laws. The DNC Registry rules protect consumers by giving consumers a private right of action to sue unsolicited telemarketing callers, and they also give the FTC or FCC authority to take enforcement action against those callers that violate the rules. Unfortunately, bad actors seeking to send spam ignore the DNC list and other rules that protect consumers, so the best way the FTC can protect consumers is to support industry efforts to target bad actors and prioritize resources for enforcement against those scammers.

To complement the protections of the DNC Registry, the wireless industry and its partners have developed a multi-pronged approach to protect consumers from illegal and unwanted robocalls and spam and scam texts, including tools that block unsolicited telemarketing calls. For example:

- *Blocking Tools.* Wireless service providers have developed and implemented tools to give consumers more control over the calls that they receive. For example, AT&T's ActiveArmor features automatic fraud and spam call blocking; it is included free with AT&T's plans. T-Mobile offers a variety of tools – including Scam ID, Scam Block, and Scam Shield – to help consumers identify and stop unwanted calls. Verizon offers Call Filter, an enhanced call-labeling and blocking service.
- *Network Analytics.* Wireless service providers use network analytics, including those that implement machine learning or artificial intelligence, to analyze network traffic, identify calls that are highly likely to be illegal, and block such calls before they reach consumers.
- *STIR/SHAKEN.* Consistent with the directives of the bipartisan TRACED Act, wireless service providers developed and implemented STIR/SHAKEN, which is a caller ID authentication framework used to verify voice calls and inform tools that block calls.
- *Branded Calling ID™.* CTIA and its wireless partners are developing the next generation of call authentication, called "Branded Calling ID™." Branded Calling ID™ leverages STIR/SHAKEN to deliver trusted visual information to consumers' smartphones, including a caller display name (*e.g.*, "Home Depot"), call logo, and call reason (*e.g.*, "Order Ready for Pickup"), all of which helps assure the recipient that the call is coming from a verified source.
- *Industry Guidelines.* Industry stakeholders have implemented "rules of the road" to guide how businesses and other organizations interact with consumers via text. For example, CTIA's *Messaging Principles and Best Practices* focus on the need for message senders to obtain consent before texting consumers. Messaging ecosystem participants enforce the *Best Practices* to help ensure that consumers receive wanted texts.
- *Consumer Reporting Tools.* Industry stakeholders have also developed consumer reporting tools to help identify spam and scam texts more quickly. For example, wireless service providers have established a common number for reporting spam messages (*i.e.*, 7726 (SPAM)). Wireless service providers also have partnered with Apple and Google so that consumers can "Report Junk" directly through the messaging applications installed on their wireless phones. Wireless service providers use the data gathered from these tools to update their network analytics and spam mitigation tools, helping keep pace with bad actors' constantly changing tactics.
- *Secure Messaging Initiative.* CTIA launched the Secure Messaging Initiative to convene the messaging ecosystem, facilitate information sharing on suspected bad actors, and enhance law enforcement efforts to identify and go after bad actors. To date, the SMI has already traced over 172,000 robotexts and made over a dozen enforcement referrals to the FCC, FTC, Department of Justice, and 50-state attorneys general enforcement task force.

To best help protect consumers, Congress can prioritize resources for enforcement against the bad actors that are violating the DNC Registry and other rules and policies that are helping to stop scam and spam calls and texts.

U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

July 15, 2025

The Honorable Gary Palmer
Chairman
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515
c/o Noah Jackson, Legislative Clerk

RE: Responding to Question from "Stopping Illegal Robocalls and Robotexts: Progress, Challenges, and Next Steps" Hearing

Dear Chairman Palmer:

Thank you for the opportunity to respond to the additional question for the record following my appearance before the Subcommittee on Oversight and Investigations hearing on June 4, 2025, entitled, "Stopping Illegal Robocalls and Robotexts: Progress, Challenges, and Next Steps".

Response to Question from the Honorable Russ Fulcher: "How effective have the Do Not Call registry's safe harbor provisions been at protecting businesses from inadvertent errors and resulting lawsuits?"

The Do Not Call Registry's safe harbor provisions, while providing important protection for diligent businesses in the context of calls inadvertently made to numbers in the Registry, do not shield businesses from the broader risks imposed by the TCPA's complex and expansive regulatory framework. Even when companies maintain robust compliance measures, inadvertent violations may occur through channels outside the Registry's scope, leaving these enterprises vulnerable to costly litigation and class action lawsuits for technical missteps rather than truly intentional misconduct. The TCPA's private rights of action fuel this type of "gotcha" litigation.

This litigation environment has effectively transformed the TCPA into a tool for extracting excessive settlements, often implemented by a narrow group of plaintiffs' law firms searching for deep pocket paydays, instead of targeting the true perpetrators of illegal robocalls and scams. In light of these challenges and as I outlined in my testimony before the Subcommittee, Congress should consider modest, measured reforms—such as establishing a cumulative damages cap, instituting a broad safe harbor for inadvertent errors, and limiting attorney's fees—to recalibrate the balance between necessary consumer protections and the regulatory certainty required for lawful business communications.

Thank you for considering our perspective on this critical issue. We look forward to working with the Committee to advance policies that support reform of the Telephone Consumer Protection Act.

Sincerely,

Stephen Waguespack
President
U.S. Chamber Institute for Legal Reform

○