Prepared Testimony of Joshua M. Bercu
Executive Director, Industry Traceback Group
Vice President, Policy & Advocacy, USTelecom – The Broadband Association
Hearing on Protecting Americans from Robocalls

Before the Senate Committee on Commerce, Science, & Transportation
Subcommittee on Communications, Media and Broadband

October 24, 2023

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

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

I am pleased to be here today to share my insights on why this country has an illegal robocall problem and what industry together with federal and state government partners is doing to address it. Illegal and unwanted robocalls started to grow and get out of control in the early 2010's. The problem grew in large part because of the rise of the internet-based calling technology known as voice over internet protocol, or "VoIP." VoIP technology made it easier and more affordable for consumers to call their friends and family anywhere in the world, but it also made it cheap and easy for bad actors to call American consumers from anywhere in the world. These bad actors care little about the legal restrictions that apply to such calls.

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

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

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

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

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

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

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

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

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

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

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

- ***Government and Brand Imposter Calls.*** Fraudulent high-volume robocalls that impersonate the Social Security Administration, sheriff offices, utilities, financial institutions, technology companies, and the like. In our experience, these calls predominantly originate abroad.

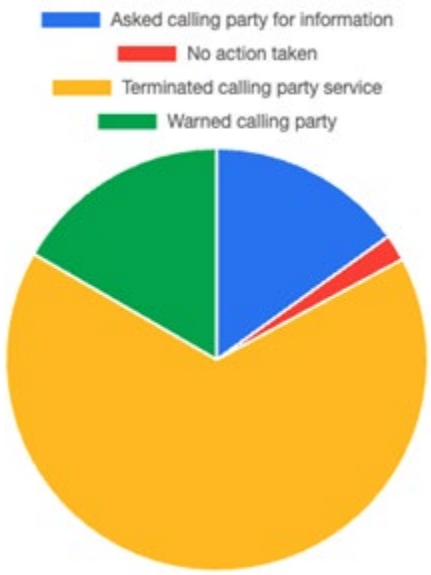
- ***Unsolicited Lead Generation Telemarketing Calls.*** Unsolicited high-volume lead generation telemarketing calls. These calls seek to sell a service or product, *e.g.*, warranty, insurance, or debt reduction products, but in violation of consent requirements, and sometimes trademark law as well. These are the robocalls that your constituents are most likely to receive today.

- ***Malicious Live Calls.*** Targeted attacks, often with a live caller. These include voice phishing (or "vishing") attempts, "Grandma scams," swatting calls, and more. For instance, earlier this year, the ITG worked with a local police department in Indiana to trace back a series of spoofed calls, including bomb and mass shooting threats to a high

school and a swatting call targeting a student in the school, helping the police apprehend the suspect before any harm was done.

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

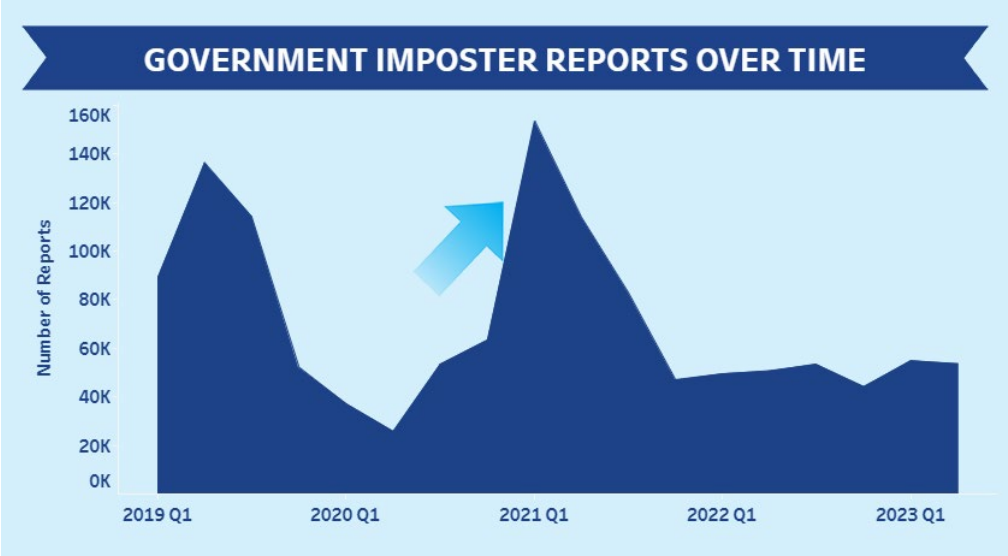
Actions Taken by Originating Providers in Response to ITG Tracebacks



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

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

increasingly rare, a trend that correlates to an overall decline in government impersonation scams.

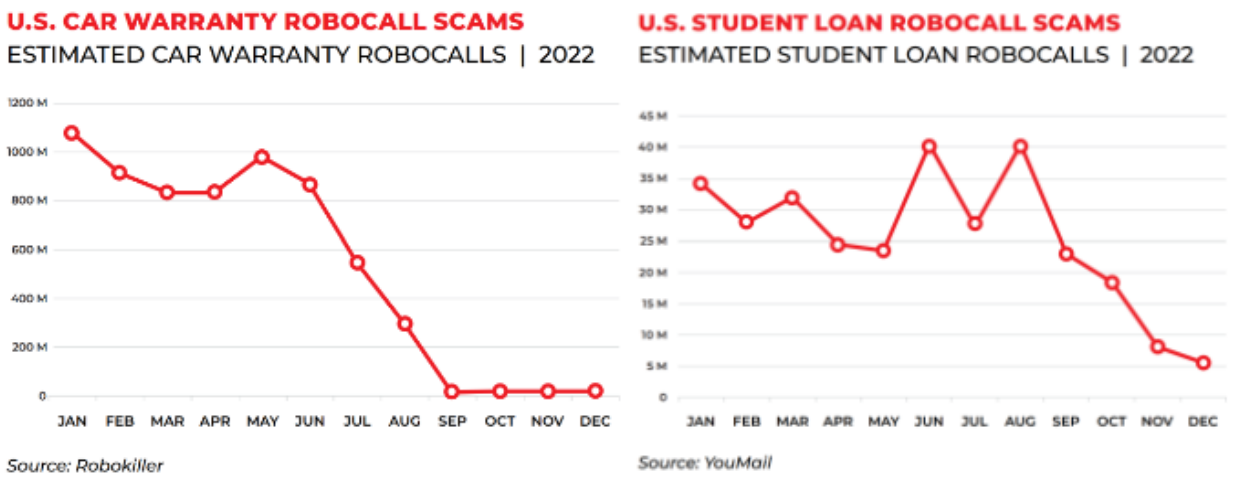


Source: FTC Consumer Sentinel

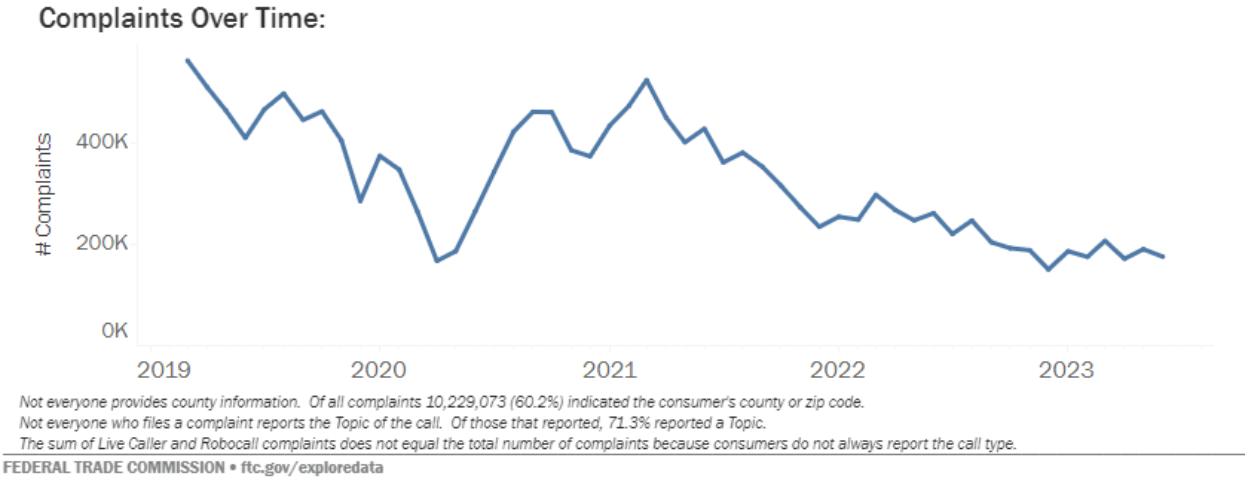
The drop in scam robocalls has unfortunately been supplanted by a substantial rise in unsolicited telemarketing calls. The lead generators responsible for these billions of unwanted robocalls do not sell any product or service; rather, as the government has alleged in one case, they act as "a massive 'consent farm' enterprise, using deceptive ads and websites to induce nearly one million consumers a day to provide their personal information and purported consent to receive telemarketing calls."[1] These lead generators then sell these questionably obtained consents to various third parties. For example, a consumer may sign up for a job listing website or to participate in a raffle, but that person almost certainly missed the fine print that links to a second page of "Marketing Partners" and purportedly gave consent to receive robocalls from hundreds, or even thousands, of entirely unrelated entities. Worse, the ITG has seen some evidence that suggests these already flimsy claims of consents could actually be entirely falsified, where a bot used public data to consent on behalf of consumers for calls they never asked for and do not want.

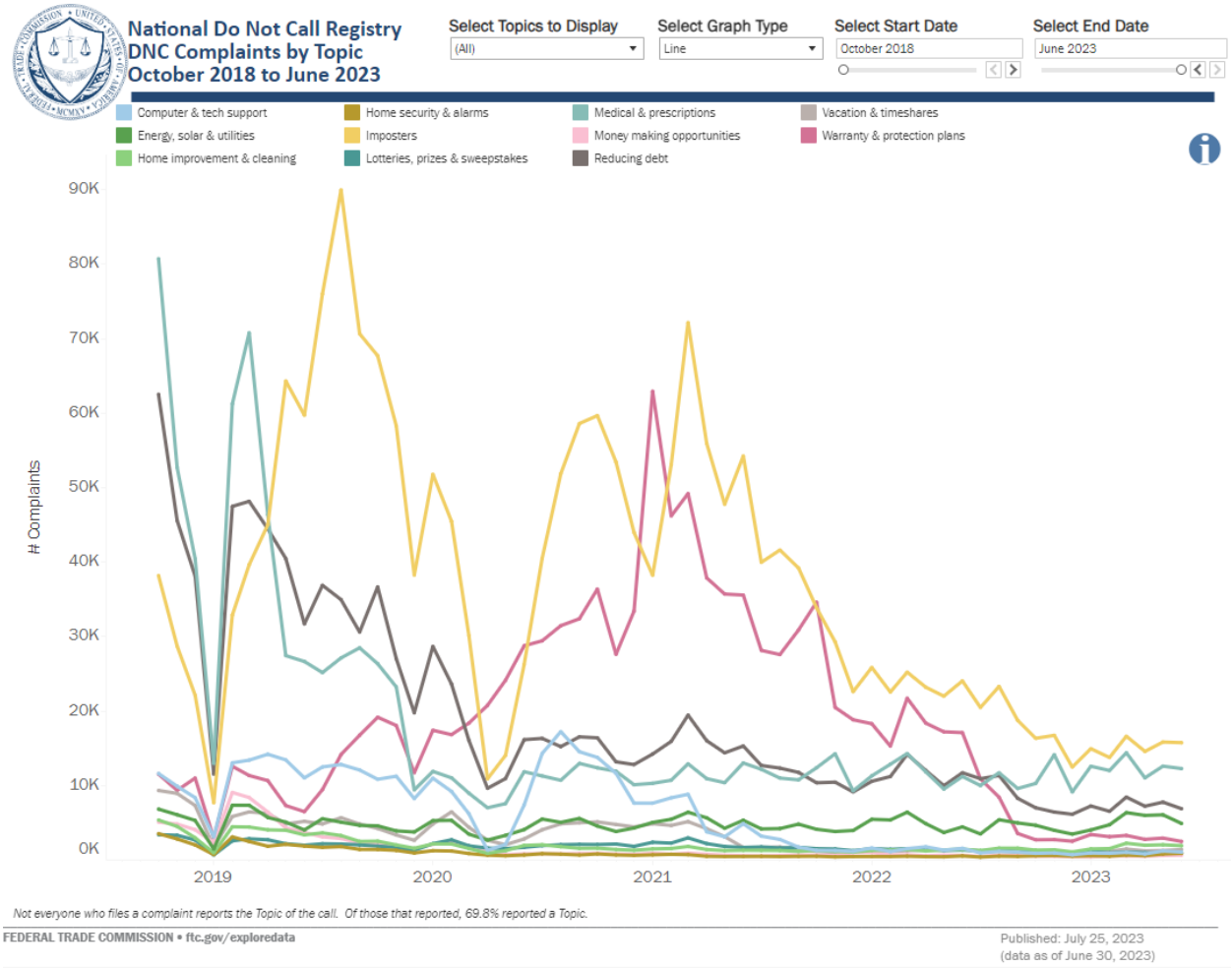
But even with these illegal robocalls, consumers are in fact seeing the positive impact of the ITG's efforts and federal and state enforcement actions. The billions of unsolicited robocalls offering auto warranties which you and your constituents almost certainly received have dropped almost to zero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

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

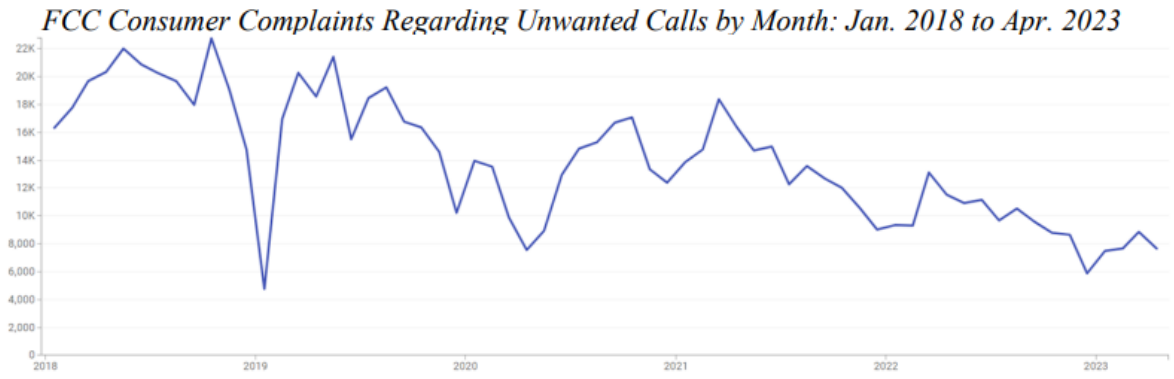


Americans are starting to notice these differences. There were over 560,000 Do Not Call complaints to the FTC in March 2019. Complaints declined after passage of the TRACED Act before peaking again in March 2021. Since then, however, there has been a steady and persistent decline – one that aligns with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





FCC complaint data shows an equivalent trend.



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

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

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

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

- *Criminal Enforcement.* Congress should ensure that the U.S. Department of Justice (DOJ) has the resources, authorities, and prioritization it needs to prosecute the criminals behind unlawful robocalls, including fraudsters overseas as well as recidivist robocallers that stand up new entities under pseudonyms as soon as their prior ones are shut down. The criminal fraudsters overseas make their livelihood by defrauding Americans in some form, and will continue even if they cannot do so through robocalls. Likewise, recidivist robocallers are not deterred by financial penalties because these bad actors will never pay their fines. The threat of criminal enforcement for the fraud they have committed will make them think twice, however.

- *Support FTC and FCC Clarifications of Consent for Lead Generation Telemarketing.* The FTC recently released updated guidance under the Telemarketing Sales Rule regarding a consumer's consent to receive lead generation calls. The FCC has an open proceeding to clarify its view of consent for lead generation calls under the Telephone Consumer Protection Act. These efforts are important to ensure that bad actors cannot continue delivering millions of robocalls each day that no one asked for or wanted under flimsy-at-best claims of consent. Congress should support efforts to ensure that any telemarketing robocalls consumers receive are ones that they in fact consented to and are expecting to receive.

- *Number Trace.* To address problematic number rotation, Congress should formally expand the role of the traceback consortium to investigate how bad actors get access to the thousands and thousands of numbers they rotate through. Just as tracebacks have infused accountability about how unlawful calls get onto the phone network, number traces will infuse more accountability into how unlawful callers get numbers through the number wholesale market.

- *Re-Introduce and Pass the Robocall Trace Back Enhancement Act or Similar Protection.* The registered traceback consortium should have protection from frivolous and nuisance lawsuits intended to undermine the traceback process and detract resources of the consortium. Those resources are better dedicated to continuing to enhance the traceback process and its disruption of illegal robocalls and support of federal and state enforcement.

- *Extend Consortium Designation Process to Every Three Years.* Under the TRACED Act, the registered traceback consortium must be designated by the FCC annually. The FCC's review and oversight are integral to confirming that the consortium operates in a neutral and non-discriminatory manner. Conducting the designation process on an annual basis, however, ties up the Commission's resources as well as those of the consortium. Those resources could be better dedicated to investments in continuing the fight against illegal robocalls.

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