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.

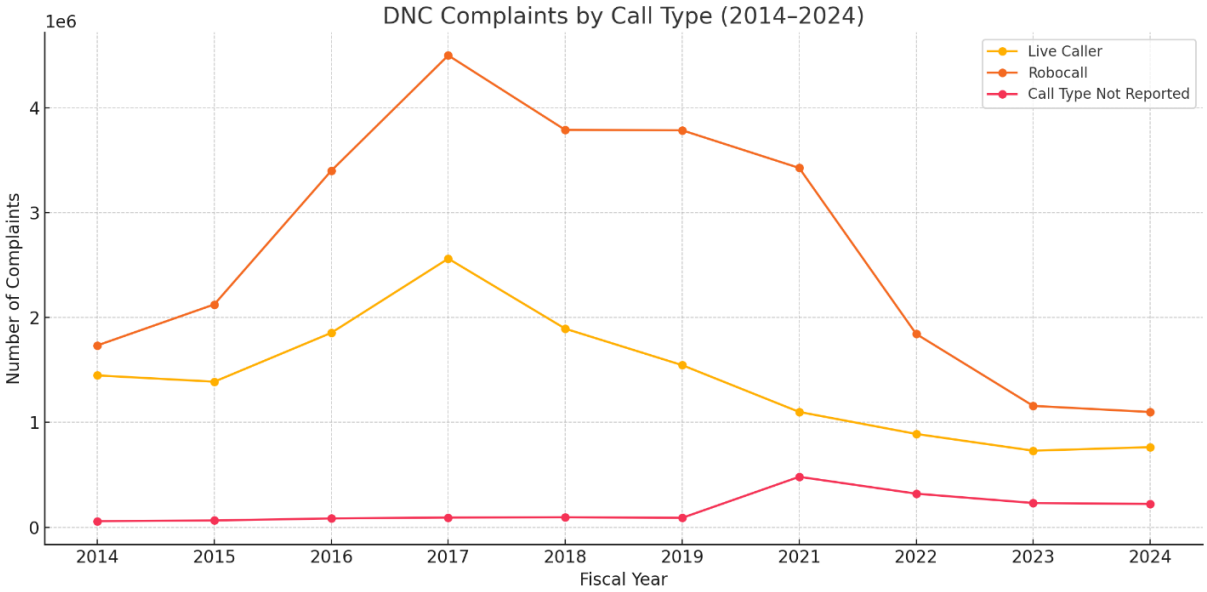
The good news is that the TRACED Act gave us a framework designed to evolve — if we keep investing in the tools that work.

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

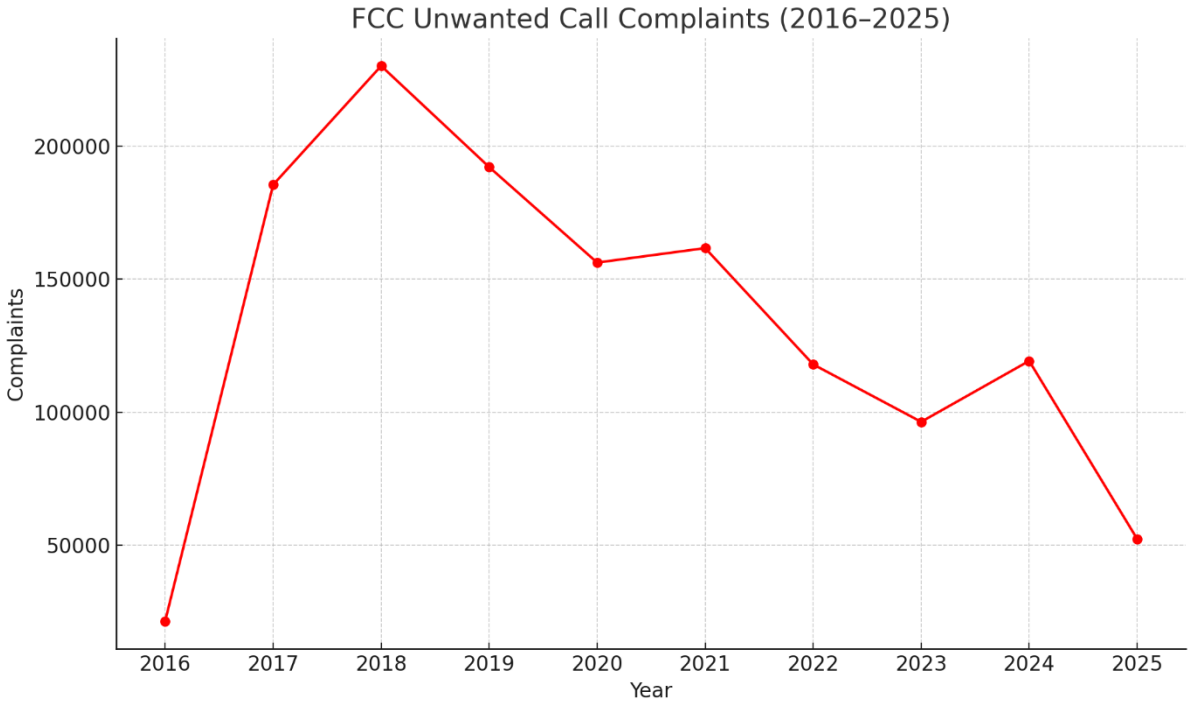
numbers, and automated and prerecorded voice messages at their core. Past illegal robocall campaigns were part of large-scale "fishing with dynamite" scams or illegal telemarketing schemes that exploited regulatory gaps and weaknesses in the phone network.

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.