Prepared Testimony of Joshua M. Bercu
Executive Director, Industry Traceback Group
Senior Vice President, Policy, USTelecom — The Broadband Association
Before the Senate Judiciary Committee
Hearing on "Scammers Exposed: Protecting Older Americans from Transnational Crime Networks"

I. Introduction

Chairman Grassley, Ranking Member Durbin, and Members of the Committee:

Thank you for the opportunity to testify today and for your leadership on this critical issue. Your continued partnership is vital to sustaining the vigilance, innovation, and coordination we need to fight the scammers and fraudsters exploiting the American people we all serve.

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 ten years, USTelecom has led the ITG, which serves as the entity designated by the Federal Communications Commission to trace back suspected unlawful robocalls. I also have served in leadership roles on the Aspen Institute FSP's National Task Force for Fraud & Scam Prevention and the Federal Trade Commission's Scams Against Older Adults Advisory Committee.

Our industry has been making real and meaningful progress confronting illegal robocalls, including both scam robocalls and illegal telemarketing campaigns. The communications industry has developed and deployed powerful tools and mechanisms like call blocking and labeling, the STIR-SHAKEN call authentication regime, and industry-led traceback – all of which are complemented by a strengthened accountability regime at the FCC and aggressive enforcement by government partners at the federal and state level.

We are leveraging these tools in the fight against ever more persistent and personalized fraud schemes. While not every one of the tools translates directly to stopping all forms of fraud, many have proven highly effective in disrupting the infrastructure that enables transnational scam operations.

From this work, we've seen both what's possible and what's still urgently needed. Because even with these tools, 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.

II. Disrupting Scam Infrastructure Through Traceback and Enforcement

Traceback is one of the tools we have adapted to disrupt call-based scam operations. By rapidly tracing the path of illegal calls back through the network, we help identify the upstream providers and actors enabling or originating fraud. Over the past several years, traceback has

contributed to dozens of enforcement actions – civil and criminal – by federal agencies and state attorneys general. We also have begun to work with international law enforcement partners.

We know the combination of identifying the bad actors responsible, including through traceback, and then holding them accountable works:

- Raids of illegal call centers in India led to an 85% drop in robocalls unlawfully impersonating the IRS in 2016.
- Enforcement targeting those responsible for unsolicited vacation and timeshare robocalls led to those calls dropping by half in 2017.
- A joint effort between Canadian and Indian authorities targeting illegal call centers in India led to a 77% decline in calls impersonating the Canadian Revenue Agency in 2018.
- FTC enforcement led to a 60% decline in unlawful health insurance robocalls in 2019 and FCC and state attorneys general action led to the virtual elimination of the illegal auto warranty robocall campaign between 2021 and 2022.

Today, thanks to coordinated action by industry and government, many of the most disruptive, high-volume scam calls – like those impersonating the IRS or Social Security Administration – no longer reach vulnerable Americans at the same scale. And while scam robocalls remain a concern, data from YouMail shows their volume is about 50% lower than at their March 2021 peak.

But the success in reducing illegal robocalls has overlapped with a deeper shift in the fraud landscape. Even as scam call volumes fall, losses to scams have continued to climb, reaching record highs. These scams, including those that begin outside the voice network, are driving the 25-30% increase in fraud losses over the past year.

Criminals evolve. They've shifted from mass robocalling to more targeted, sophisticated attacks. That evolution makes disruption harder, in turn making traceback and enforcement more essential than ever.

III. Meeting the Fraud Threat: Building Partnerships and Collaboration

Today's fraudsters aren't blasting millions of robocalls impersonating the Social Security Administration. They're shifting from high volume to high impact, targeting individuals 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, and public safety agencies. And they don't need volume to succeed — they just need to know their target's vulnerabilities. They prey on trust and use it to steal from their victims.

In the case of older adults, they can rip away what their victims spent a whole life building.

The good news: we are not powerless against these deeply personal and devastating scams. Traceback is an essential tool. It used to take law enforcement agencies months to determine who made an illegal call — we now often find those criminals within hours. That speed and scalability allow us to keep pace with today's fast-moving fraud.

In recent years, the ITG expanded its collaborative footprint beyond the telecom industry to voluntarily include banks, major tech companies, the hospitality industry, and more. These partnerships have helped broaden the reach and relevance of traceback as a cross-sector tool for fraud disruption. They also could be a differentiator in building actionable cases for criminal law enforcement against the call source. While we can't undo what's been done, we can go after the bad guys and prevent them from defrauding someone else.

For instance, the ITG is proactively 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. Early results have been promising, and we believe it can serve as a model for enhanced cross-sector collaboration. Beyond this pilot, individual voice service providers are also forming partnerships across industry sectors to explore ways to strengthen real-time fraud detection, alerting, and response.

International coordination continues to be another essential frontier. The threat of foreign actors exploiting U.S. networks is not new, but their tactics are evolving. Increasingly, we trace calls back to entities posing as U.S.-based providers: forming shell LLCs, using disposable domains, and in some cases impersonating real telecom companies. These tactics are designed to evade other providers' know-your-customer programs and regulatory scrutiny. They reinforce why criminal enforcement remains essential. Civil enforcement alone cannot deter the groups of individuals orchestrating these schemes.

SIMBoxes add another layer of complexity. These locally deployed devices allow scammers to simulate thousands of unique mobile identities. To a carrier, they usually look like thousands of individual callers rather than one high-volume source, making them harder to prevent. But they require someone physically present in the U.S. to operate, which creates a rare opportunity for enforcement. These actors are within reach of domestic law enforcement and turning that vulnerability into a point of disruption and deterrence should be a clear priority.

Meanwhile, AI is further blurring the line between robocalls and live scams. Criminals can now use AI-generated voices that pause, laugh, and respond in real time. These tools are cheap, scalable, and increasingly convincing. While analytics-based call blocking and labeling and call authentication 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.

The industry is moving aggressively to respond in the face of these evolving threats. We are evolving our tactics, our tools, and our partnerships. But we cannot make arrests or prosecute the criminals — even when we identify them. The most effective way government can support this

work is to strengthen public-private partnerships, unlock additional cross-sector collaboration, and ensure that criminal actors face real consequences for exploiting Americans.

IV. 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 causing harm, results-focused, and supportive of the tools and partnerships that work.

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

- **Establish a national anti-scam strategy with a central coordinator and prioritize criminal enforcement.** The United States need a unified, whole-of-government approach that elevates scams as a national policy and enforcement priority. A designated White House federal lead or task force would improve coordination, eliminate silos, and give industry a clear point of contact – accelerating action against rapidly evolving threats.

  Critically, the strategy must prioritize cross-border criminal enforcement. The actors we identify in tracebacks of scam calls are not confused marketers. They're criminals, often operating transnationally, who are undeterred by regulatory fines. Strengthening support for prosecution, training, investigations, and cross-border coordination will help ensure these actors face real consequences.

- **Provide a safe harbor for improved fraud prevention and detection.** Emerging partnerships between telecom providers, financial institutions, tech platforms, and other stakeholders are showing real promise in identifying and disrupting scams. A well-scoped safe harbor could unlock even deeper collaboration across the internet ecosystem to accelerate threat detection and to better prevent consumer harm. Right now, however, privacy regulation and other legal concerns can inhibit companies from using and, where appropriate, sharing data that could help identify and stop fraud.

- **Support and scale what works – including proven tools like traceback.** As scams evolve, we need to double down on tools and partnerships that have shown real results. Traceback is one such tool: it can help drive criminal prosecutions, civil enforcement actions, and real-world disruption of scam networks, and increasingly serves as a model of effective cross-sector collaboration. But like many effective solutions, it requires sustained support and legal clarity to remain viable. Congress should reinforce frameworks that work like traceback, ensuring stability for the program and protecting it from litigation designed to undermine the process and the program's mission.

V. Conclusion

While we've made progress – together – fraud continues to take a toll. Scam robocalls are down, enforcement actions are up, and industry tools like traceback are evolving with the threat.

But the progress in reducing illegal call volume doesn't mean the threat is gone. Criminal fraudsters are adapting quickly, targeting individuals, impersonating trusted institutions, and operating from beyond the perceived reach of U.S. enforcement.

Our next phase of work must expand our focus on converting intelligence into impact, using traceback and cross-sector collaboration not just to detect fraud, but to help deter, disrupt, and penalize it, and prevent perpetrators from targeting another victim.

Strengthening the public-private partnership, especially around coordinated criminal enforcement, is one of the most important ways the federal government can help turn progress into real accountability and deliver meaningful protection for the American public.

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