Prepared Testimony of Joshua M. Bercu
Executive Director, Industry Traceback Group
Senior Vice President, Policy, USTelecom — The Broadband Association
Before the House Committee on Homeland Security
Subcommittees on Border Security and Enforcement and Cybersecurity and Infrastructure Protection
Joint Hearing: "Online Scams, Crypto Fraud, and Digital Extortion:
An Examination of How Transnational Criminal Networks Target Americans"
April 21, 2026

I. Introduction

Chairman Garbarino, Ranking Member Thompson, Chairman Guest, Ranking Member Correa, Chairman Ogles, and Members of the Subcommittees:

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 transnational criminal networks 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 over ten years, USTelecom has led the Traceback Group, 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 Federal Trade Commission's Scams Against Older Adults Advisory Group and the Aspen Institute Financial Services Program's National Task Force for Fraud & Scam Prevention.

The telecom industry has been making real and meaningful progress to protect American consumers by confronting illegal calls, including both illegal robocalls and scams. Communications providers have developed and deployed powerful tools and mechanisms like call blocking and labeling, call authentication, and industry-led traceback — all complemented by a strengthened accountability regime at the FCC and aggressive enforcement by government partners at the federal and state level.

My testimony focuses on the telecom infrastructure that transnational criminal organizations, or TCOs, abuse and misuse to reach American victims and on the industry tools, enforcement partnerships, and policy frameworks we need to disrupt them. The Traceback Group's work sits at an important intersection: we trace the illegal calls that the same criminal networks you are examining today often are behind. And the intelligence we develop supports a myriad of government enforcement actions against these groups and the in-on-the-scheme entities they rely on.

From this work, we've seen both what's possible and what's still urgently needed to protect consumers. The bottom line: we have built and deployed the right tools and anti-scam infrastructure. The foundation is strong. Now we need to keep building on it, deepening collaboration across industry sectors and with government to ensure those tools deliver real accountability for the criminals behind these scams.

II. Disrupting Scam Infrastructure Through Traceback and Enforcement

Traceback is one of the tools we have adapted to disrupt call-based scam operations. 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.

By rapidly tracing the path of illegal calls back through the network, the Traceback Group helps identify the multiple providers that carry the call and actors enabling or originating fraud. We work closely with federal and state law enforcement, routinely tracing calls referred to us – including scams impersonating the Department of Homeland Security, IRS, Social Security Administration and other federal agencies – and providing actionable information to support enforcement. Over the past several years, traceback has contributed to dozens of civil and criminal actions. 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 calling operations in India led to an 85% drop in robocalls impersonating the IRS in 2016, and a similar joint effort by Canadian and Indian authorities in 2018 drove a 77% decline in calls impersonating the Canadian Revenue Agency.

- Enforcement targeting those responsible for unsolicited vacation and timeshare robocalls led to those calls dropping by half in 2017.

- 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. Data from YouMail shows scam robocall volume is about 50% lower than at the March 2021 peak.

In recent years, industry collaboration has expanded beyond the communications sector and the public sector. The Traceback Group, for example, now works with banks, major tech companies, the hospitality industry, and others to identify the criminals behind illegal calls and feed that information to law enforcement. In one recent instance, some of our data was shared through the National Cyber-Forensics Training Alliance to support takedowns by the Department of Homeland Security's Homeland Security Investigations. These burgeoning partnerships are one of the most promising developments to protect consumers.

III. How Criminal Networks Abuse U.S. Telecom Infrastructure

The progress is real, but so is the evolution of the threat. Today's fraudsters aren't blasting millions of robocalls impersonating the Social Security Administration. They're shifting from high volume to high impact, and the criminal networks behind these schemes are sophisticated, organized, and global. From a telecom perspective, this evolution is defined by how these

organized crime groups abuse and misuse U.S. communications infrastructure to reach consumers.

A decade ago, the dominant illegal calling threat to U.S. consumers was concentrated in South Asia, principally India and to a lesser degree Pakistan and Bangladesh. Operators ran tech-support, IRS-impersonation, and bank-fraud scripts out of illegal calling operations. That threat persists, but the center of gravity has shifted. As has been well-documented, the most consequential development is the rise of industrial-scale "scam compounds" in Southeast Asia, principally in Myanmar, Cambodia, and Laos. In parallel, Mexican drug cartels have built their own illegal calling operation networks targeting American consumers.

One important point for Congress' consideration, however, is structural. What was once a regionally bounded set of criminal enterprises has become a globalized, industrialized fraud-as-a-service marketplace. Criminal fraudsters' toolsets are bought, sold, and shared across these ecosystems. Playbooks, scripts, and even trafficked labor move through Telegram channels, dark-web forums, and overlapping financial infrastructure. The practical consequence is that successful techniques are copied, traded, and operationalized across regions on a timeline measured in weeks, not years.

While the threat of foreign actors abusing U.S. networks is not new, 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 — tactics designed to evade know-your-customer requirements and regulatory scrutiny. Beyond this, we see growing instances where legitimate callers and calling platforms — a hospital, a school broadcast service, tools used for get-out-the-vote calls, and more — are compromised and used to deliver scam impersonation calls, leveraging stolen credentials and deployed at scale using AI and automation. At the same time, SIMBoxes add another layer of complexity, enabling scammers to simulate thousands of unique mobile identities and making high-volume activity look like individual callers — and generate calls from within the United States, even if the callers themselves are located abroad.

These evolutions are not accidental. Traceback and enforcement have systematically eliminated the low-hanging fruit. Enforcement actions have shut down or driven out the VoIP providers that once turned a blind eye to bad traffic or built their business on bringing it into the country. Gone are the days of blasting millions of calls through permissive internet-based voice providers. Instead, criminals have adapted, hijacking or deploying domestic infrastructure.

These trends underscore a central reality: while industry protections are essential and civil enforcement can be highly impactful, they are not sufficient on their own to deter the transnational criminal organizations orchestrating these schemes.

IV. Turning Progress into Lasting Impact

America's telecom providers have been moving aggressively to respond in the face of these evolving threats. But we cannot make arrests or prosecute the criminals — even when we identify them.

When I testified before the House Energy & Commerce Committee, Oversight and Investigations Subcommittee and the Senate Judiciary Committee nine months ago, I outlined three areas where federal action could make a meaningful difference: establishing a coordinated national anti-scam strategy, enabling greater cross-sector data sharing through a safe harbor, and scaling tools and partnerships that are already delivering results.

The Administration's March 2026 Executive Order makes important progress on that first priority and advances elements of the others. It reflects exactly the kind of whole-of-government approach this problem demands and treats scams as what they are: crimes.

The EO establishes a dedicated operational cell within the National Coordination Center to coordinate federal efforts to detect, disrupt, dismantle, and deter TCOs explicitly including private sector engagement. It also directs action to hold foreign governments accountable and to return seized assets to victims. Taken together, it signals that the Administration views transnational fraud as a national security priority, not merely a consumer protection matter.

The EO is exactly what we needed – and it could not have come at a more critical moment. Now the focus must be on ensuring that this momentum translates into sustained impact.

There are three areas where Congress can help:

- **Resource implementation and sustain pressure on cross-border criminal enforcement.** The EO rightly emphasizes enforcement and accountability, particularly for actors operating overseas. Congress can reinforce the EO and its mandate by supporting investigative capacity, prosecution, and cross-border coordination. We need prosecutors and investigators fully resourced so that they can move with urgency and work with willing partners abroad. Communications providers, including through the Traceback Group, stand ready in support.

- **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 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 must double down on proven 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 efforts designed to undermine the process and its mission.

V. Conclusion

While we've made progress together, fraud continues to take a toll on American consumers. Scam robocalls are down, enforcement actions are up, and industry tools like traceback are evolving with the threat. The Administration's March Executive Order represents real momentum toward the kind of coordinated, enforcement-first approach this problem demands, and communications providers are committed to being a constructive partner in its implementation.

But the progress in reducing illegal call volume does not mean the threat is gone. Criminal fraudsters are adapting quickly, targeting individuals, impersonating trusted institutions, and operating from beyond what they perceive as the reach of U.S. enforcement. Transnational criminal networks are abusing U.S. telecom infrastructure as one component of a broader, multi-vector attack on American consumers — encompassing crypto fraud, digital extortion, human trafficking, and more.

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

Strengthening partnerships – particularly around coordinated criminal enforcement and the legal frameworks that enable deeper collaboration – is one of the most important ways the federal government can help turn progress into lasting impact, drive real accountability, and deliver meaningful protection for the American public.

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