Prepared Testimony of Kevin Rupy
Partner, Wiley Rein LLP
"Legislative Hearing on Protecting Communications Networks and Improving Connectivity"
July 22, 2026

Chairman Hudson, Vice Chairman Allen, Ranking Member Matsui, Members of the Committee, thank you for giving me the opportunity to appear before you today.

My name is Kevin Rupy, and I am a Partner in the Telecommunications, Media, and Technology Practice at Wiley Rein LLP, and I am here today in my personal capacity. The views expressed in this testimony are my own, and do not reflect the views of Wiley Rein LLP or any of its clients.

I have been working to fight illegal robocalls and fraud since 2014, when I helped to develop and oversee the efforts of the Industry Traceback Group ("ITG"), which has been the Federal Communications Commission's ("FCC") designated traceback consortium since July 2020. I am also a Board Member of the Communications Fraud Control Association, and my practice at Wiley includes working on behalf of clients to combat illegal robocalls and brand impersonation scams.

I share the Subcommittee's concerns about illegal robocalls. Indeed, consumer fraud—including but not limited to fraud perpetrated through illegal robocalls—is no longer dominated by opportunistic, one-off scam artists. Increasingly, it is perpetrated by sophisticated criminal enterprises, including organized crime networks, transnational criminal organizations, drug cartels, and hostile foreign actors operating at industrial scale. As such, this issue raises serious consumer protection and national security concerns, which is why the subcommittee is right to focus on it.

I would like to make three points today:

- Robocall enforcement works and the government should continue to strengthen effective enforcement tools.
- Because fraud is highly dynamic, industry needs flexible frameworks that allow legitimate providers and their partners to adapt to changing tactics and respond in real time.
- Collaboration between industry and government is critical to effectively combat fraud.

I. ROBOCALL ENFORCEMENT WORKS AND THE GOVERNMENT SHOULD CONTINUE TO STRENGTHEN EFFECTIVE ENFORCEMENT TOOLS.

Enforcement works—particularly when supported by sophisticated tools like traceback. Federal and state agencies, together with industry partners, have developed targeted and effective mechanisms to identify, track, and disrupt illegal calling campaigns. These tools are critical, as scams—including but not limited to those perpetrated via illegal

robocalls—are increasingly tied to sophisticated bad actors and organized criminal networks. For example:

- The Aspen Institute's National Task Force on Fraud and Scam Prevention ("National Task Force") has warned that the modern fraud ecosystem increasingly involves "North Korean hackers, Mexican cartels, Russian crime syndicates, and Triad gangs."[1]
- Law enforcement agencies have documented the involvement of Mexico-based cartels in large-scale fraud schemes targeting American consumers, including fraudulent timeshare call center operations that generated hundreds of millions of dollars in illicit proceeds.[2] The Federal Bureau of Investigation ("FBI") noted that the illicit proceeds obtained through these fraudulent telemarketing operations are "increasingly being used to fund violent cartels in Mexico."[3]
- Federal authorities have likewise highlighted the role of "Chinese criminal groups in Southeast Asia" that target consumers around the world through fraudulent calls, texts, and online communications—resulting in Americans losing an estimated $10 billion to Southeast Asia-based scams in 2024.[4]

---

[1] Aspen Institute, *United We Stand: A National Strategy to Prevent Scams*, at 8 (Sept. 30, 2025), https://www.aspeninstitute.org/publications/united-we-stand-a-national-strategy-to-prevent-scams/ ("United We Stand").

[2] FBI, *Mexican Cartels Target Americans in Timeshare Fraud Scams, FBI Warn*s (June 7, 2024), https://www.fbi.gov/news/stories/mexican-cartels-targeting-americans-in-timeshare-fraud-scams-fbi-warns (last visited July 16, 2026) ("FBI Warning"); U.S. Department of the Treasury, *Treasury Targets Cartel-Linked Timeshare Resort Defrauding U.S. Citizens* (Feb. 19, 2025), https://home.treasury.gov/news/press-releases/sb0400; Financial Crimes Enforcement Network, *FinCEN, OFAC, and FBI Joint Notice on Timeshare Fraud Associated with Mexico-Based Transnational Criminal Organizations* (July 16, 2024), https://www.fincen.gov/news/news-releases/fincen-ofac-and-fbi-joint-notice-timeshare-fraud-associated-mexico-based; see also Steve Fisher, *These Americans bought timeshares in Mexico. They were unknowingly funding a cartel*, USA Today (Feb. 22, 2024), https://www.usatoday.com/story/news/investigations/2024/02/22/thousands-of-americans-fall-prey-to-mexican-cartel-cjng-timeshare-scam/72695295007/; Maria Abi-Habib, *A Mexican Drug Cartel's New Target? Seniors and Their Timeshares* (Mar. 21, 2024), https://www.nytimes.com/2024/03/21/world/americas/mexico-timeshare-fraud-cartel.html; Dallas Express, *U.S. Sanctions CJNG Cartel For $300M Timeshare Fraud Targeting Seniors* (Aug. 13, 2025), https://dallasexpress.com/crime/u-s-sanctions-cjng-cartel-for-300m-timeshare-fraud-targeting-seniors/.

[3] FBI Warning.

[4] U.S.-China Economic and Security Review Commission, *Protecting Americans from China-Linked Scam Centers: An Update on Emerging Trends* (Mar. 5, 2026), https://www.uscc.gov/research/protecting-americans-china-linked-scam-centers-update-emerging-trends; *see also* Department of Justice, *Scam Center Strike Force Takes Major Actions Against Southeast Asian Scam Centers Targeting Americans* (Apr. 23, 2026), https://www.justice.gov/opa/pr/scam-center-strike-force-takes-major-actions-against-southeast-asian-scam-centers-targeting (discussing charges against two Chinese nationals who managed

The involvement of organized crime and sophisticated bad actors has led to staggering levels of consumer losses that represent a consumer protection problem, as well as a national security emergency. Recent survey data estimates that consumers lost approximately $68 billion to scams in 2025 alone.[5] Those losses represent more than statistics. They reflect stolen retirement savings, depleted household budgets, and substantial emotional and financial harm inflicted on millions of Americans.

Fortunately, there is also ample evidence demonstrating that aggressive enforcement actions by federal and state agencies can combat these losses and deter fraudulent robocall campaigns. For example:

- A Federal Communications Commission enforcement action targeting unsolicited robocalls related to vacation and timeshare fraud schemes resulted in those calls dropping by 50% in 2017.[6]
- Federal Trade Commission ("FTC") enforcement resulted in a 60% decline in unlawful health insurance robocalls in 2019.[7]
- Enforcement by the FCC and state attorneys general also virtually eliminated an illegal auto warranty robocall campaign that, during a three month period, placed over 5 billion auto warranty robocalls to consumers in 2021. The FCC's cease-and-desist letters and order directing all U.S.-based voice service providers to take steps to mitigate the auto warranty robocalls caused a sharp decline in illegal calls of 80% within a mere 24 hours of their issuance.[8]

These examples illustrate how enforcement and industry initiatives can disrupt ongoing fraudulent campaigns and reduce consumer exposure to scam traffic.

And industry traceback efforts have proven particularly valuable to combating unlawful robocall schemes. The ITG has explained that a mere traceback, even without a related enforcement action, can mitigate illegal robocalls.[9] Federal and state enforcement

---

a cryptocurrency investment fraud compound in Burma and the restraining of more than $700 million in cryptocurrency alleged to be tied to money laundering from cryptocurrency scams).

[5] Gallup, *United States of Scams: The Financial and Emotional Fallout*, at 3 (2026), http://gallup.com/analytics/711827/scams-in-america.aspx ("Gallup Fraud Survey").

[6] *See generally Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc.*, File No.: EB-TCD-15-00020488, Forfeiture Order, 33 FCC Rcd 4663 (2018).

[7] *See* FTC, *Enforcement: Annual Highlights 2019*, https://www.ftc.gov/reports/annual-highlights-2019/enforcement (last visited July 16, 2026).

[8] *Sumco Panama SA et al.*, File No.: EB-TCD-21-00031913, Forfeiture Order, 38 FCC Rcd 7235, ¶¶ 22–24 (2023).

[9] ITG, *For Government: Working with the Industry Traceback Group* https://tracebacks.org/for-government/ (last visited July 16, 2026) ("Tracebacks directly disrupt illegal call campaigns as most completed ITG tracebacks result in the caller kicked off of its provider's network."); *see* ITG, *2022 Year-in-Review: State of Industry Tracebacks* (Mar. 2023), https://tracebacks.org/wp-content/uploads/2023/03/ITG-2022-Year-in-Review-State-of-Industry-Traceback.pdf ("95% of completed tracebacks result in action with nearly 70% ending with the caller terminated or warned.").

authorities have direct access to traceback results in the ITG's portal, which supports FCC, FTC, and state attorneys general enforcement actions against potential scammers—from issuing cease-and-desist letters to filing lawsuits against potential bad actors.

The increasing deployment of STIR/SHAKEN call authentication technology has further bolstered these efforts. For example, the ITG leverages STIR/SHAKEN caller ID authentication information collected from providers to improve the traceback process.[10] STIR/SHAKEN data is collected at each hop in the call path, enabling analysis of signing behavior across providers and helping stakeholders to more quickly identify the source of illegal calls.[11] The continued expansion of authentication technologies has made tracebacks more efficient and more effective, thereby improving the overall enforcement ecosystem.

At the same time, American companies have increasingly pursued civil litigation, brand-protection initiatives, and technical measures against bad actors that abuse trusted brands.[12] But U.S. businesses cannot win this fight alone. Scam operations are highly sophisticated, and as illustrated above, growing evidence suggests that many modern fraud campaigns are linked to criminal syndicates, rather than individual bad actors. The FCC remains uniquely positioned to root out bad actors from the voice ecosystem at the source, and should continue to leverage its existing authorities to do so.

Congress can help too. Several provisions of the proposed Foreign Robocall Elimination Act would enhance government's ability to combat illegal robocall traffic. Directing the FCC to establish an interagency taskforce on unlawful robocalls that includes stakeholders from the private sector would promote cooperation among federal agencies and coordinated enforcement efforts. Extending the review period for the FCC's designation of the traceback consortium from one to three years would drive administrative efficiency for both the FCC and the traceback consortium. Ultimately, it would enable the designated traceback consortium to focus its efforts on finding illegal robocallers instead of participating in administrative proceedings. And the proposal to grant immunity for receiving, sharing, and publishing traceback information would further incentivize providers to aid in the fight against illegal robocalls. Lastly, the proposed legislation would add requirements to the FCC's Robocall Mitigation Database ("RMD") framework, although it should be noted that the FCC is already pursuing reforms to improve the RMD through its existing authority. These proposals include, but are not limited to, vetting entities before they are admitted into the RMD, which would ensure that bad actors cannot enter the U.S. voice network in the first place.

---

[10] *Ex parte* letter from Joshua M. Bercu, Executive Director, ITG, et al., to Marlene Dortch, Secretary, FCC, EB Docket No. 20-195, at 3 (filed May 1, 2026).

[11] *Ex parte* letter from Joshua M. Bercu, Executive Director, ITG, to Marlene Dortch, Secretary, FCC, CG Docket No. 17-97, Attach. at 5 (filed Jan. 14, 2026) ("ITG Observations").

[12] *See Marriott Int'l v. Dynasty Mktg. Grp., LLC et al.*, No. 1:21-cv-610 (E.D. Va. filed May 18, 2021); *Amazon.com Inc. et al v. Wasim et al*, No. 3:23-cv-05580 (N.D. Cal. filed Oct. 30, 2023); *Capital One Fin. Corp. v. John Does 1-10*, No. 1:26-cv-01276 (E.D. Va. filed May 12, 2026).

Congress should continue to empower the FCC and law enforcement partners by prioritizing measures that strengthen enforcement, improve traceback capabilities, and facilitate information sharing.

II. BECAUSE FRAUD IS HIGHLY DYNAMIC, INDUSTRY NEEDS FLEXIBLE FRAMEWORKS THAT ALLOW LEGITIMATE PROVIDERS AND THEIR PARTNERS TO ADAPT TO CHANGING TACTICS AND RESPOND IN REAL TIME.

A. Flexibility Is Key for Responding to Evolving Threat Vectors in Real Time.

The companies, agencies, and organizations working to protect consumers operate within legal, technical, and operational constraints. They must protect lawful communications, comply with privacy and consumer protection obligations, preserve access to wanted calls, and coordinate across complex networks and business relationships. In stark contrast, fraudsters do not operate under such constraints. When one path becomes less effective, they quickly shift to another. When one provider rejects their traffic, they look for a different route. When one script becomes recognizable, they change the story. That imbalance is one reason why Congress and regulators should be cautious about imposing static requirements on a threat environment that is constantly changing.

The ITG illustrates how this plays out in practice in its recent work. In materials filed with the FCC in early 2026, the ITG highlighted the highly dynamic nature of the illegal robocall environment, explaining that: fewer than 10 percent of tracebacks pertain to calls that originated abroad; an average of 30 or more new providers were identified in tracebacks each month; some RMD filings involved impersonation or stolen identities of providers and companies; and approximately 45 tracebacks involved spoofed calls with A-level attestation originating from compromised calling platforms.[13]

Several trends provide further examples of this dynamic environment. The ITG recently reported that fraudsters are apparently hacking private branch exchanges (“PBXs”)—the internal telephone systems used by businesses—to originate unlawful traffic by exploiting legitimate enterprise phone systems.[14] Because PBXs are used by real businesses, compromising those systems can make unlawful traffic appear to come from more ordinary sources, complicating efforts to identify and stop it.

SIM boxes have also become a fraud vector.[15] SIM boxes can be used to originate large volumes of fraudulent traffic within a carrier’s trusted network in ways that obscure the source of the calls, bypass STIR/SHAKEN checks, and make them appear more like ordinary mobile-originated communications. The ITG recently expressed its understanding that making calls in this manner is a more expensive method, perhaps

[13] ITG Observations at 3–4, 8.

[14] *Id.* at. 8

[15] *Id.* at 9.

indicating that the actors behind such calls have shifted in light of increased difficulty getting their calls through to consumers.[16] Nevertheless, these tactics can make concentrated fraudulent activity appear more diffuse, complicating detection models that are designed to identify high-volume sources.

Those trends reflect a broader shift in the fraud landscape: bad actors are moving away from easily identifiable mass-calling and towards methods that make fraudulent traffic appear more ordinary, domestic, or trusted. The FTC has also warned that scammers use voice cloning to make requests for money or information more believable, including by making a call sound like a boss asking for bank account information or a family member seeking emergency help.[17]

Despite the changing tactics of fraudsters, industry mitigation efforts have correspondingly changed in response. As an example, USTelecom reports that, as scammers have moved from foreign internet-based voice providers to SIM-box operations in the United States, the ITG and major wireless carriers created a SIM-box task force to identify and disrupt that activity.[18] That effort has produced encouraging results, including a reported decline in SIM-box-based illegal calls and potential opportunities for criminal enforcement of ordinarily unreachable foreign providers because SIM-box operations generally require some domestic physical presence.[19] In a fixed regulatory checklist, this kind of operational adaptation is difficult to capture. It depends on the ability to identify emerging patterns, share information, escalate suspicious activity, and adjust mitigation practices as bad actors change course.

Fraudsters will continue to evolve. Congress and regulators should ensure that legitimate providers, enforcement partners, and other stakeholders can adapt as quickly—or faster—than the schemes they are working to stop.

B. Congress Should Avoid Adopting Prescriptive New Rules That Burden Legitimate Companies and Do Not Aid in the Fight Against Illegal Robocalls.

The FCC's current robocall mitigation rules impose accountability on stakeholders throughout the voice network while preserving operational flexibility. Section 64.6305 of the FCC's rules, for example, requires voice service providers, gateway providers, and non-gateway intermediate providers to implement "appropriate" robocall mitigation programs, take reasonable steps to avoid originating, carrying, or processing illegal robocall traffic, respond within 24 hours to traceback requests, and cooperate with the

---

[16] *Ex parte* letter from Joshua M. Bercu, Executive Director, ITG & Jessica Thompson, Director of Traceback Operations, ITG, to Marlene Dortch, Secretary, FCC, EB Docket No. 20-195, at 3 (filed May 1, 2024).

[17] Federal Trade Commission, *Fighting back against harmful voice cloning* (Apr. 8, 2024), https://consumer.ftc.gov/consumer-alerts/2024/04/fighting-back-against-harmful-voice-cloning.

[18] USTelecom, *Illegal Robocalls and Call-Based Fraud*, (Mar. 2025), https://ustelecom.org/wp-content/uploads/2025/03/USTelecom-Illegal-Robocalls-and-Call-based-Fraud.pdf.

[19] *Id.*

Commission, law enforcement, and the industry traceback consortium.[20] The rule promotes accountability, but it leaves room for providers to tailor mitigation to their networks, customer relationships, upstream providers, analytics tools, and observed risk indicators. As illustrated above, these types of flexible approaches are the most effective.

Importantly, Congress should not look to complex compliance frameworks like the Telephone Consumer Protection Act ("TCPA") as a solution to the illegal robocall problem. The TCPA was initially passed in 1991 as a consumer protection statute to prevent families from receiving unwanted telemarketing calls at the dinner table. At its core, the TCPA establishes compliance requirements for legitimate callers, and those compliance requirements are highly complex. Coupled with the TCPA's private rights of action, which have long been abused by plaintiff's attorneys seeking enormous payouts from American businesses seeking to comply with the statute,[21] the TCPA's complex requirements make it perilous for businesses to communicate with consumers.

But as explained above, the bad actors behind illegal robocalls do not play by the same rules. As such, the TCPA's compliance mandates primarily burden legitimate callers, not the scammers who routinely disregard the rules. I encourage Congress to focus on legislation aimed directly at fraudsters and criminal enterprises, rather than retrofitting a compliance statute that bad actors will simply ignore. To this end, the QUIET Act as proposed would add yet a new layer of complexity to the TCPA, which unfortunately will only burden legitimate communications, but not slow down illegal robocallers and their accompanying schemes.

III. COLLABORATION BETWEEN INDUSTRY AND GOVERNMENT IS CRITICAL TO EFFECTIVELY COMBAT FRAUD.

Fraud enabled by illegal robocalls is not merely a voice-network problem; it is a cross-sector threat that affects financial institutions, social media platforms, the hospitality and travel sectors, and many others. Today's fraudsters are no longer relying solely on high-volume imposter calling campaigns. They are shifting to more targeted schemes that use live calls, spoofed account numbers, and emotional appeals to reach victims at

---

[20] 47 C.F.R. § 64.6305.

[21] *See, e.g.,* Chamber Institute for Legal Reform, *Expanding Litigation Pathways: TCPA Lawsuit Abuse Continues in the Wake of Duguid* (Apr. 2024), https://instituteforlegalreform.com/wp-content/uploads/2024/04/ILR-Expanding-Litigation-Pathways-April-2024.pdf; U.S. Chamber Institute for Legal Reform, *TCPA Litigation Sprawl: A Study of the Sources and Targets of Recent TCPA Lawsuits* (August 2017), https://instituteforlegalreform.com/wp-content/uploads/2020/10/TCPA_Paper_Final.pdf; U.S. Chamber Institute for Legal Reform, *Ill-Suited: Private Rights of Action and Privacy Claims* (July 2019), https://instituteforlegalreform.com/wp-content/uploads/2020/10/Ill-Suited_-_Private_RIghts_of_Action_and_Privacy_Claims_Report.pdf; U.S. Chamber Institute for Legal Reform, *Turning the TCPA Tide: The Effects of Duguid* (Dec. 2021), https://instituteforlegalreform.com/wp-content/uploads/2021/12/1323_ILR_TCPA_Report_FINAL_Pages.pdf.

moments of vulnerability. With a single call, a criminal can steal a retirement nest egg, a college savings account, or the down payment for a family home.

The scale of this harm is substantial and growing. According to new data from the FTC, Americans reported losing $3.5 billion to imposter scams alone in 2025—a three-fold increase since 2020.[22] Across all categories of fraud, reported losses reached approximately $16 billion in 2025, the highest amount ever recorded and a 25 percent increase over 2024.[23] And because many victims never report these crimes, the true losses are almost certainly far greater, as acknowledged in the recent Gallup Survey.[24]

This escalating threat demands a coordinated response. As fraud continues to evolve, accelerated by the growth of artificial intelligence, industry stakeholders and government partners must work together to detect bad actors and cut them off at the source.

The Scam Center Strike Force ("Strike Force") is an apt of example of the potential that such public-private partnerships can have—formed in November 2025, the Strike Force "combines the power, reach, and resources of the U.S. Attorney's Office with the Department of Justice's Criminal Division, the FBI, and the U.S. Secret Service to secure America against Southeast Asian cryptocurrency-related fraud and scams."[25] In addition to its partnership with the private industries, the Scam Center Strike Force collaborates with other federal partners, including the Department of State, the Department of Treasury's Office of Foreign Assets Control, and the Department of Commerce.

Notably, just last month, the Strike Force announced the results of a first-of-its-kind event combining the focus of government entities and private industries to tackle cyber-enabled and cryptocurrency fraud targeting Americans. During what was billed as "Disruption Week," the private sector took voluntary action to "interrupt millions of social media, email, and internet access accounts used by transnational organized crime

---

[22] Press Release, FTC, *FTC Data Show People Reported Losing $3.5 Billion to Imposter Scams in 2025* (June 15, 2026), https://www.ftc.gov/news-events/news/press-releases/2026/06/ftc-data-show-people-reported-losing-3-point-5-billion-imposter-scams-2025.

[23] *Id.*

[24] *See* Gallup Fraud Survey, at 9 ("The Stop Scams Alliance-Gallup estimate of about $68 billion is higher than the FTC's reported losses, totaling $16 billion in 2025. This likely reflects the number of scams that go unreported to the FTC or other federal agencies, as well as differences in the types of scams that are reported to the FTC compared with those collected on a probability-based survey, as in this study."). Indeed, The Aspen Institute Financial Security Program's Scam Prevention Initiative reports a much higher number "in 2025, criminals stole more than $3 billion every week from Americans, including seniors and veterans." Aspen Institute Financial Security Program, *The Aspen Institute Financial Security Program's Scam Prevention Initiative*, https://scamprevention.aspeninstitute.org/ ("Aspen Initiative").

[25] U.S. Attorney's Office for the District of Columbia, *Scam Center Strike Force* (June 18, 2026), https://www.justice.gov/usao-dc/scam-center-strike-force ("Scam Center Strike Force Page").

actors in Southeast Asia that were being used to defraud Americans, and the government shared information which enabled private sector actors to voluntarily freeze over $3.8 million in cryptocurrency involved in laundering of funds stolen from Americans."[26]

As of June 18, 2026, the Strike Force has restrained over $830 million in cryptocurrency from scammers by leveraging cooperation from internet service providers and social media companies.[27] Notably the Strike Force "seeks public-private partnership to ensure that these corrupt scammers will immediately be cut off, preventing the United States infrastructure from being used as a means to perpetrate fraud against Americans."[28]

Another promising model is the National Task Force.[29] The National Task Force brought together hundreds of experts to develop a national strategy to combat criminal enterprises that exploit American financial organizations, social media, communications, and retail platforms to defraud consumers. Its report, released in late 2025, calls for a whole-of-ecosystem strategy to combat fraud, and to "modernize legal frameworks, and undermine the scams business model by making it harder for transnational criminals to prey on American households."[30] The report focuses on two priorities: acting against scams and minimizing their harm, and empowering scam prevention efforts. A fraud scheme may begin with a call or text, continue through a website, messaging platform, or social media interaction, and end with a bank transfer, cryptocurrency transaction, gift card purchase, or other payment mechanism. A framework focused only on one point in that chain will leave gaps that bad actors can exploit. The National Task Force seeks to plug those gaps.

The communications industry has also worked closely with the ITG on SIM box call tracing and disruption. Those efforts have coincided with an observed decline in SIM box-related activity. [31] Federal partners have likewise collaborated with industry to break

---

[26] Press Release, U.S. Attorney's Office for the District of Columbia, *Scam Center Strike Force Announces Results of U.S. & Private Industry 'Disruption Week'* (June 3, 2026), https://www.justice.gov/usao-dc/pr/scam-center-strike-force-announces-results-us-private-industry-disruption-week.

[27] *See* Scam Center Strike Force Page.

[28] *Id.*

[29] Aspen Initiative.

[30] United We Stand.

[31] *Ex parte* letter from Joshua M. Bercu, Senior Vice President, Policy, USTelecom & Executive Director, ITG, to Patrick Webre, Acting Chief, Enforcement Bureau, FCC, EB Docket No. 20-22, at 2 (filed May 26, 2026), https://www.fcc.gov/ecfs/document/10526875506612/1.

up scam centers operating both abroad and in the United States and to take down SIM farms.[32]

These efforts demonstrate that industry is moving quickly and deliberately to respond to evolving threats. But industry cannot do it alone. Congress, the FCC, the FTC, and law enforcement can contribute to this fight by strengthening public-private partnerships and encouraging and facilitating cross-sector industry initiatives. No single sector can combat fraud alone; sustained information sharing and coordinated action across industry and government are essential to staying ahead of bad actors' evolving playbook. Congress can support this by spearheading a national fraud strategy that reflects a whole-of-government approach and elevates scams to the enforcement priority they deserve. That strategy should also emphasize cross-border enforcement, because many fraudsters operate transnationally and are not deterred by regulatory penalties alone.[33]

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

[32] Letter from Sarah Leggin, Vice President, Regulatory Affairs, CTIA, to The Honorable David Schweikert, Chairman, and the Honorable Maggie Hassan, Ranking Member, Joint Economic Committee (Mar. 25, 2026).

[33] ITG Observations at 2, 10 (explaining that traceback data demonstrates that the foreign origination of robocalls is declining and "some entities claim U.S.-based but appear to be located overseas").