Testimony of

Sarah Leggin
Vice President, Regulatory Affairs
CTIA

on

Stopping Illegal Robocalls and Robotexts: Progress, Challenges, and Next Steps

Before the
U.S. House of Representatives Committee on Energy & Commerce
Subcommittee on Oversight & Investigations

June 4, 2025

Chairmen Palmer and Guthrie, Ranking Members Clarke and Pallone, and Members of the Subcommittee, on behalf of CTIA and the wireless industry, thank you for the opportunity to testify today.

CTIA commends the Energy and Commerce Committee for its leadership in protecting Americans from the scourge of illegal and unwanted robocalls and robotexts. Thanks to this Committee's actions, the TRACED Act provided the Federal Communications Commission ("FCC") with new tools to combat illegal robocalls. Under this framework, the wireless industry is helping lead the way in advancing consumers' control of the voice calls they receive. And with your support, the wireless industry is combatting billions of spam and scam text messages each month using innovative solutions that are helping prevent bad actors from corrupting the trusted environment of text messaging. We balance these steps with our ongoing support for legitimate calls and messages to help ensure that consumers get the communications they want.

Consumers rely on wireless more than ever before for voice calls and text messaging. As reported last year, Americans devoted nearly 2.4 trillion minutes to voice calls, and they exchanged more than 2.1 trillion text messages, or more than 67,000 messages every second – and texts have a 98 percent open rate, evidencing how much consumers read and trust their texts. Unfortunately, bad actors know how much consumers value and rely on wireless voice and text messages. As they have increased their deceptive efforts, we have increased our efforts and our success in combatting them. As just one example, wireless providers blocked over 55 billion scam and spam texts in 2024, while at the same time ensuring trillions of legitimate texts go through.

Of course, there is more to do. And working together with Members of this Committee, the FCC, the Federal Trade Commission ("FTC"), the Department of Justice ("DOJ"), state attorneys general, and our partners throughout the voice and text messaging ecosystems, we are making headway in fighting bad actors and maintaining consumer trust in voice services and text messaging.

The Wireless Industry is Helping to Lead the Fight Against Robocalls.

Although automated calls from banks, pharmacies, airlines, schools, and others can enhance consumer welfare, too many automated calls are intrusive. We all know the type – a call that comes with a robotic or familiar voice and an enticing offer or one that tries to scam us into disclosing personal data. These calls are consumer pain points.

In response, wireless providers spearheaded the development of the STIR/SHAKEN framework years ago and led the way in implementing it, consistent with the directives of the bipartisan TRACED Act. As this Subcommittee is aware, STIR/SHAKEN helps identify callers and reduce caller ID spoofing as a key part of the industry's multipronged defense against illegal and unwanted robocalls. Congressional adoption and the FCC's implementation of the TRACED Act ensured this framework is now a critical component throughout voice networks, and STIR/SHAKEN has been a key step to restoring consumer trust in voice services.

Complementing STIR/SHAKEN, wireless providers and their ecosystem partners launched a range of powerful tools to regain consumer control over the calls they receive. These include robust know-your-customer practices, innovative call-blocking, tracing back illegal robocalls to identify bad actors, and robust robocall mitigation programs. AT&T's ActiveArmor, for example, features automatic fraud and spam call blocking and is included free with its plans. T-Mobile offers a variety of tools including Scam ID and Scam Block as well as a free Scam Shield app to help consumers identify and stop unwanted calls. Verizon engages in network-level blocking of highly-suspect traffic based on analytics and also offers Call Filter, an enhanced call labeling and blocking service, at no charge. In fact, wireless providers block, label, or identify over 45 billion scam calls each year while also working hard to ensure legitimate calls are completed. The FCC has recognized the success of these solutions and encouraged all voice service providers to take similar actions, using powerful analytic tools to complete legitimate calls while increasingly blocking illegal calls.

CTIA and its wireless partners are embarking on the next generation of call authentication – Branded Calling. We know that the majority of calls from unknown numbers are not answered today, and consumers are more likely to answer and engage with a call if they know the brand name of the caller. CTIA has developed a branded calling solution that leverages the STIR/SHAKEN framework to deliver trusted visual information to consumers' smartphones that helps assure them that a call is coming from a verified source. This solution is called Branded Calling ID™ – or "BCID™." BCID™ delivers verified, robust, and secure identity information including: (1) caller display name (*e.g.*, "Home Depot"); (2) call logo; and (3) call reason (*e.g.,* "Order Ready for Pickup"). With trusted, branded caller information, consumers can make more informed choices about whether to pick up the phone, reducing the risk of being bothered by spam or scam calls.

Notwithstanding all of the solutions discussed above, we know that bad actor robocallers will continue to find ways to call consumers. To that end, wireless providers are key partners in USTelecom's Industry Traceback Group ("ITG") to identify, block, or take enforcement actions against bad actors. CTIA's member companies and their partners across the voice ecosystem also continue to work to ensure that overseas counterparts take effective measures to mitigate foreign-originated illegal robocalls. Providers balance these steps with efforts to ensure that legitimate calls, including public safety calls, are protected.

These efforts have yielded promising results. In fact, according to ITG's latest report, "[t]raceback-powered enforcement [has] led to sharp declines in numerous illegal robocall campaigns." Robocall complaints to the FTC have also decreased steadily, reaching a six-year low in 2024. We are proud of this progress.

The Wireless Industry Is Committed to Maintaining Consumer Trust in Text Messages.

Today, wireless text messaging is one of the most popular and trusted forms of communication among American consumers. Americans exchanged 2.1 trillion text messages in 2023, and 90 percent of Americans use their phones to text at least monthly. The consumer trust that the wireless industry has built is why messaging boasts a 98% "open rate." This is much higher than email, with a 20 percent open rate and 6 percent response rate. As these stats show, consumer trust in wireless text messaging remains high, and the wireless industry works collaboratively and innovatively to keep it that way.

As a result, CTIA and its member companies understand the importance of investing in proactive, multi-layered measures that include sophisticated tools, industry best practices, and public-private partnerships to protect consumers from spam and scam text messages.

At the outset, it is important to note that consumers' positive assessment of text messaging stems in part from the fact that messaging does not carry the same regulatory burdens as voice services. In contrast to voice services, where common carrier regulations impeded voice service providers from blocking unwanted robocalls, text messaging operates in a light-touch regulatory regime that has enabled wireless providers to be nimble and innovative in crafting solutions to protect consumers from a flood of spam and scam text messages. Wireless providers have not been forced to seek a government agency's permission to block or take action against illegal text messaging and bad actors; they do so proactively and aggressively to the benefit of consumers. And this has worked exceedingly well.

Wireless providers successfully prevent billions and billions of spam text messages from ever reaching consumers each year. In 2024 alone, wireless providers blocked more than 55 billion scam and spam robotexts. And blocking is only one part of the broader effort to make sure the wireless industry's playbook evolves to keep up with bad actors' changing tactics.

First, wireless messaging technologies and up-front vetting and verification practices help thwart bad actors before they can even send scam or spam text messages. As a threshold protection, wireless messaging technologies require valid originating information, such as a legitimate telephone number. As a result, number spoofing has not plagued text messaging as it has with robocalling. Instead, impersonation scams – where bad actors try to trick consumers into thinking that a trusted entity like their bank is contacting them – have been more prevalent. To address this issue, wireless providers and their ecosystem partners require businesses and other message senders to disclose information about themselves and their campaign before they can send high volumes of text messages. This process has helped to weed out and prevent many bad actors from blasting out mass spam text messages.

Second, many different entities help make messaging work, both with respect to innovating messaging platforms and consumer protection. The messaging "pie" is expanding, including not only SMS/MMS text messaging offered by wireless providers, but also new platforms, like over-the-top ("OTT"), online and app-based messaging platforms, and recently-launched Rich Communications Service ("RCS"). Unfortunately, that also means that bad actors have more ways to target consumers, and their ambitions are not limited to any particular technology platform. This means all messaging providers – including RCS, OTT, and online platforms – are part of the team effort to prevent spam messages and deter bad actors from targeting consumers through messaging.

Next, CTIA's *Messaging Principles & Best Practices* for the messaging ecosystem offers industry-led guidance to vindicate consumer preferences, while supporting innovative, legitimate communications. The *Best Practices* are widely adopted throughout the messaging ecosystem and focus on the key tenet of consent: Consumers should have control over the texts they receive, with the ability to opt-out at any time. Through these and other principles, including those addressing privacy and security, the *Best Practices* help prevent consumers from receiving unwanted messages while promoting innovation that allows consumers to get the messages they do want.

CTIA is gratified that its efforts were recently recognized by a coalition of six national consumer advocate organizations:

> [T]exting currently remains a valuable and trusted method of communication in the United States, largely because of the best practices developed by CTIA and adopted by its members and their partners. . . . [T]he entire texting ecosystem would be a disaster if fewer industry-developed restrictions against unwanted texts were applied.[1]

CTIA continues to update the *Messaging Principles and Best Practices* – for example clarifying who qualifies as a non-consumer sender to help ensure all types of entities understand what guidance applies to them as they set up their messaging campaigns.

Wireless providers and their messaging partners also deploy vast security and fraud prevention teams using the latest innovative technologies, machine learning and AI, and other spam mitigation tools to protect consumers through real-time analysis and other defense solutions. To enhance these protections, wireless providers have set up a common means for consumers to report unwanted text messages – 7726 (SPAM) – and partner with Apple and Google to make it easier for consumers to “Report Junk” directly through the wireless messaging applications that are built into most of our wireless phones. Wireless providers use this reported data to constantly evolve spam mitigation tools in real-time and keep pace with the constantly changing tactics of bad actors. And when wireless providers receive complaints about texts with suspicious URLs or domains, their teams investigate the website to determine if the link is intended to support fraudulent efforts. If so, wireless providers can share that link with Google’s Safe Search list so it can be blocked by most internet browsers.

The wireless industry and their messaging partners are constantly evolving and enhancing their tools, including by responsibly leveraging AI in myriad applications throughout the wireless ecosystem to prevent fraud, robocalls, and robotexts, strengthen cybersecurity, and more. CTIA and its member companies are mindful of both the benefits and risks of AI, and they are incentivized to strike the right balance in promoting innovative uses while fighting bad actors. We support the Administration’s efforts to accelerate AI innovation through its AI Action Plan and AI R&D Plan, Congress’ efforts to avoid a patchwork of state legislation on AI, as well as the FCC’s bipartisan decision last year establishing clear guidance on the use of AI that has already helped the FCC and industry protect consumers from bad actors using AI voice-generating tools that fall within the scope of the TCPA. We look forward to further developments like these that promote AI innovation rather than regulations focused on addressing AI-enabled robocalls and text messages.

Notwithstanding all of these tools, bad actors continue to seek out ways to get spam and scam text messages through to consumers. To complement industry tools and best practices, CTIA launched the Secure Messaging Initiative ("SMI") to help the FCC, FTC, DOJ, and other law enforcement agencies identify and go after bad actors. The SMI leverages the additional information available in the texting ecosystem (i.e., not just phone number and provider name) that is not accessible in the voice context to help identify suspected bad actors and refer those to law enforcement for investigation. SMI participants also share suspected spam and scam messages and techniques to more rapidly and effectively shut down spam activity, while targeting the senders of unwanted or fraudulent messages.

Through the SMI, we have already traced over 172,000 robotexts and made over a dozen referrals for enforcement actions to our partners at the FCC, FTC, DOJ, and the 50-state attorneys general enforcement task force. Collectively, these efforts are helping to enhance efforts to stop scammers and maintain consumer trust in wireless text messaging.

Congress, the FCC, the FTC, DOJ, and other authorities can contribute to this fight by encouraging industry efforts to coordinate and facilitate broad-based sharing information about bad actors through CTIA's SMI. And enforcement authorities like the FCC, FTC, DOJ, and state AGs should continue to "throw the book" at those that seek to harm consumers through illicit messaging. As noted above, the wireless industry is coordinating with federal and state authorities to stop bad actors who may be violating these rules. And government and industry alike have a role to play when it comes to educating consumers to protect themselves and encouraging broader adoption of industry best practices, including CTIA's *Messaging Principles and Best Practices* and industry vetting and monitoring tools, that enable the wireless industry to identify and stop bad actors.

CTIA and the wireless messaging ecosystem remain vigilant in seeking to combat scam and spam messaging, and we are pleased there was a nearly 40% drop in consumer complaints about text messages to the FCC and the FTC between 2021 and 2023. Collaboration and information sharing across the wireless messaging ecosystem, cross-sector partners, and law enforcement agencies will help us continue to maintain consumer trust in wireless messaging by targeting bad actors and thwarting their evolving tactics.

Congress Should Consider Ways to Boost Efforts to Fight Robocalls and Robotexts.

The TRACED Act was landmark legislation that has encouraged the adoption of innovative technologies and solutions that are having positive results. CTIA offers a few suggestions on how this Committee can build on this positive framework to address the enduring problem of robocalls and robotexts.

First, we support the Administration's efforts to do more to protect consumers and our voice and text networks. As Chairman Carr noted in his first Commission-level action as Chair, "[c]racking down on illegal robocalls will be a top priority at the FCC,"[2] and we support this effort. Second, we share the goal of cracking down on consumer fraud, as reflected in Ranking Member Pallone's *Do Not Disturb Act*.

Finally, we value our partnerships with law enforcement and encourage Congress to take steps to promote more action against the bad actors behind illegal robocalls and robotexts. Many agencies are working to fight consumer fraud, but many lack the personnel or resources to bring cases. Congress could have agencies report on their current consumer fraud resources and actions and leverage that information collection to identify areas that could use more support. With more resources for enforcement at the federal and state levels, Congress can help take more bad actors off the field and stop illegal robocalls and robotexts at the source.

* * *

The wireless industry is proud of our efforts to reduce the volume of illegal robocalls and prevent spam and scam text messages from reaching consumers. We know there is more work to do to protect consumers, and with the support of this Committee, the wireless industry can continue to lead in mitigating efforts by bad actors.

Thank you for the opportunity to testify today. We look forward to working with you to continue to protect consumers from intrusive and illegal robocalls and robotexts.

[1] Letter from Margot Saunders, Senior Counsel, National Consumer Law Center, to Marlene Dortch, Secretary, FCC, CG Docket No. 21-402 et al., at 2 (filed Mar. 6, 2024).

[2] Press Release: First Commission-Level Vote Under Chairman Carr Proposes A Nearly $4.5 Million Fine Stemming From Apparently Illegal Robocall Scheme (Feb. 4, 2025), https://docs.fcc.gov/public/attachments/DOC-409354A1.pdf.