

CTIA Responses to Questions for the Record

Ms. Sarah Leggin

Subcommittee on Oversight and Investigations Hearing

June 4, 2025

“Stopping Illegal Robocalls and Robotexts: Progress, Challenges, and Next Steps.”

The Honorable Russ Fulcher

1. As of April 2025, more than 221 million phone numbers are currently registered on FTC’s Do Not Call registry.

a. What types of calls does the Registry block? What calls are allowed? Why does the Registry not block spam calls?

b. Is extending the Do Not Call registry to block spam calls feasible?

The Do Not Call (“DNC”) Registry is a list of telephone numbers that telemarketers are prohibited from placing unsolicited calls to. American consumers can register their telephone number on the DNC Registry to indicate that they do not wish to receive unsolicited telemarketing calls. Consumers may consider unsolicited telemarketing calls to be a type of spam call, which would be covered by the DNC Registry’s rules. Both the Federal Trade Commission (“FTC”) and the Federal Communications Commission (“FCC”) have rules that prohibit telemarketers from placing unsolicited calls to telephone numbers on the DNC Registry. In 2023, the FCC clarified that the DNC Registry’s protections include text messages, meaning telemarketers are prohibited from sending unsolicited marketing texts to telephone numbers on the DNC Registry, in addition to unsolicited telemarketing calls.

To help balance the need for legitimate callers to reach consumers with the need to protect consumers from unsolicited telemarketing calls, the DNC Registry rules do not apply to non-marketing calls, such as prescription updates, delivery notifications, and other “transactional” calls that businesses frequently make to consumers. The DNC Registry rules also have certain exceptions, including an exception for consumer consent: If a consumer lists their telephone number on the DNC Registry and subsequently gives consent to a caller to receive telemarketing calls, the caller is allowed to contact the consumer. Of course, a consumer may later revoke their consent, at which point the caller may not contact the consumer.

Because the DNC Registry is a list of telephone numbers, the DNC Registry cannot block calls. Instead, it is an informational resource that telemarketers consult when working to comply with U.S. telemarketing laws. The DNC Registry rules protect consumers by giving consumers a private right of action to sue unsolicited telemarketing callers, and they also give the FTC or FCC authority to take enforcement action against those callers that violate the rules.

Unfortunately, bad actors seeking to send spam ignore the DNC list and other rules that protect consumers, so the best way the FTC can protect consumers is to support industry efforts to target bad actors and prioritize resources for enforcement against those scammers.

To complement the protections of the DNC Registry, the wireless industry and its partners have developed a multi-pronged approach to protect consumers from illegal and unwanted robocalls and spam and scam texts, including tools that block unsolicited telemarketing calls. For example:

- *Blocking Tools.* Wireless service providers have developed and implemented tools to give consumers more control over the calls that they receive. For example, AT&T's ActiveArmor features automatic fraud and spam call blocking; it is included free with AT&T's plans. T-Mobile offers a variety of tools – including Scam ID, Scam Block, and Scam Shield – to help consumers identify and stop unwanted calls. Verizon offers Call Filter, an enhanced call-labeling and blocking service.
- *Network Analytics.* Wireless service providers use network analytics, including those that implement machine learning or artificial intelligence, to analyze network traffic, identify calls that are highly likely to be illegal, and block such calls before they reach consumers.
- *STIR/SHAKEN.* Consistent with the directives of the bipartisan TRACED Act, wireless service providers developed and implemented STIR/SHAKEN, which is a caller ID authentication framework used to verify voice calls and inform tools that block calls.
- *Branded Calling ID™.* CTIA and its wireless partners are developing the next generation of call authentication, called “Branded Calling ID™.” Branded Calling ID™ leverages STIR/SHAKEN to deliver trusted visual information to consumers' smartphones, including a caller display name (e.g., “Home Depot”), call logo, and call reason (e.g., “Order Ready for Pickup”), all of which helps assure the recipient that the call is coming from a verified source.
- *Industry Guidelines.* Industry stakeholders have implemented “rules of the road” to guide how businesses and other organizations interact with consumers via text. For example, CTIA's *Messaging Principles and Best Practices* focus on the need for message senders to obtain consent before texting consumers. Messaging ecosystem participants enforce the *Best Practices* to help ensure that consumers receive wanted texts.
- *Consumer Reporting Tools.* Industry stakeholders have also developed consumer reporting tools to help identify spam and scam texts more quickly. For example, wireless service providers have established a common number for reporting spam messages (i.e., 7726 (SPAM)). Wireless service providers also have partnered with Apple and Google so that consumers can “Report Junk” directly through the messaging applications installed on their wireless phones. Wireless service providers use the data gathered from these tools to update their network analytics and spam mitigation tools, helping keep pace with bad actors' constantly changing tactics.
- *Secure Messaging Initiative.* CTIA launched the Secure Messaging Initiative to convene the messaging ecosystem, facilitate information sharing on suspected bad actors, and enhance law enforcement efforts to identify and go after bad actors. To date, the SMI has already traced over 172,000 robotexts and made over a dozen enforcement referrals to the FCC, FTC, Department of Justice, and 50-state attorneys general enforcement task force.

To best help protect consumers, Congress can prioritize resources for enforcement against the bad actors that are violating the DNC Registry and other rules and policies that are helping to stop scam and spam calls and texts.