



Rhonda J Johnson
Executive Vice President
Federal Regulatory Relations

AT&T Services, Inc.
601 New Jersey Ave., NW
Suite 500
Washington, DC 20001

T: 415.244.7681
rhonda.j.johnson@att.com
att.com

July 15, 2024

Chairwoman Jessica Rosenworcel
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Dear Chairwoman Rosenworcel:

On behalf of AT&T, I am writing in response to your June 26th letter to AT&T CEO John Stankey inquiring about the company's efforts to combat illegal robocalls, especially those using artificial intelligence (AI) generated voices.

We share your concern about unlawful and unwanted robocalls and commend the Commission's leadership on this issue, which, together with the efforts of industry and the Industry Traceback Group (ITG), has decreased the number of illegal robocalls in the United States by 80 percent since February 2021.¹ AT&T has done, and will continue to do, its part in the fight against illegal and unwanted robocalls, including those using AI generated voices.² Indeed, since 2016, AT&T has blocked or labeled over 80 billion calls.

The following describes the numerous actions AT&T has taken to combat illegal robocalls and provides answers to your questions.

First, AT&T has a robust and highly effective robocall program to identify and block illegal robocalls on its network. AT&T reviews a broad set of aggregated data to identify suspicious calling patterns indicative of robocalls and blocks those calls that are highly likely to be illegal. We continuously refine our analytics to identify and block more illegal robocalls.

Second, AT&T offers its consumers call blocking options. AT&T ActiveArmor Mobility Security, which automatically blocks suspected fraud calls and labels calls that are identified as a spam risk, is provided to AT&T wireless customers. The accompanying free app allows customers to customize their robocall protection, manage nuisance calls, and create a personal block list. For AT&T Phone, a consumer VoIP service, AT&T Digital Phone Call Protect automatically blocks suspected fraud calls and sends a caller ID alert if a call appears to be unwanted.

This year, AT&T and TransUnion jointly announced that they are offering a service that allows AT&T wireless customers to see the name and brand logo of participating businesses on verified incoming calls, providing customers more confidence in the identity of the caller.³

¹ See Letter of Industry Traceback Group, EB Docket No. 20-195 at 2-3 (filed May 1, 2024).

² See Comments of USTelecom – The Broadband Association, CG Docket No. 23-362 at 3 (filed Dec. 18, 2023) (noting that providers typically focus on identifying suspicious activity, patterns, and actors, rather than search for utilization of any particular technologies, such as AI).

³ See <https://newsroom.transunion.com/att-and-transunion-launch-the-industrys-first-in-network-branded-call-display-with-logos/>.

Third, AT&T is a leader in the industry's effort to address illegal spoofing. AT&T is fully committed to the Commission's STIR/SHAKEN requirements. We co-chaired the STIR/SHAKEN industry standards group and currently chair the Secure Telephone Identity Governance Authority (STI-GA) Industry Board. STIR/SHAKEN has been implemented on AT&T's Internet Protocol (IP) network,⁴ and STIR/SHAKEN verification results are shared with customers that have compatible devices, assuming the call has no other risk factors.

AT&T has also developed a technique to identify calls that spoof an AT&T wireless subscriber's number and do not include the STIR/SHAKEN indicator. Deployed in its network in late 2023, AT&T is now able to identify 98 percent of calls that spoof an AT&T wireless number calling another AT&T wireless number. We have offered to share this technique with other providers.

Fourth, AT&T takes reasonable steps to know and verify its customers. Although the specific steps vary depending on the type of service a customer buys, AT&T requires its business, postpaid wireless and broadband mass market customers to provide information sufficient to identify the customer and conduct a credit and fraud risk assessment. AT&T also has an Identify Theft Prevention Program designed to detect, prevent, and mitigate identity theft associated with postpaid consumer and business accounts. AT&T's service agreements, guides, and terms of service authorize it to terminate any customer found to be using AT&T's service for abusive, fraudulent, or unlawful purposes.

AT&T also takes reasonable steps to verify the identity of carriers, both domestic and international, that interconnect with AT&T, and to confirm that they are listed in the Commission's Robocall Mitigation Database (RMD). For international carriers, AT&T verifies that doing business with the carrier does not violate any sanctions or embargo restrictions.

Fifth, AT&T has dedicated resources to respond to the Commission's request for information related to suspected illegal robocall campaigns. AT&T has a long history of responding to the Commission's requests for information related to suspected illegal robocall campaigns submitted through established processes. This includes dedicated resources in AT&T's GFMO with specific expertise in the detection of illegal robocalls.

Sixth, AT&T strongly supports the Industry Traceback Group. AT&T was a founding member of the ITG and is currently on the ITG Steering Committee. AT&T also cooperates fully with traceback requests from the ITG, responding as expeditiously as possible, generally within less than an hour.

While AT&T is proud of what it has accomplished, we are committed to continuing to improve our tools to meet the challenge of combating illegal and unwanted robocalls. We are continuously innovating and partnering with others to combat illegal and unwanted robocalls. In this regard, AT&T is a member of (and helped develop the framework for) One Consortium, the newly formed international consortium designed to fight illegal and unwanted voice calls and

⁴ The Commission's rules provide an exception for implementation of STIR/SHAKEN for those portions of a provider's network that rely on technology that cannot initiate, maintain, carry, process, and terminate Session Initiation Protocol (SIP) calls subject to certain conditions. *See* 47 C.F.R. §64.6304(d).

messages on international connections.⁵ In addition, to get ahead of bad actors generating unauthorized and illegal robocalls during the upcoming election, AT&T provisioned telephone lines to itself to receive inbound calls, including in higher-risk areas, which we will monitor and use to improve the analytics for blocking and labeling calls.

AT&T also works to protect consumers from illegal and unwanted text messages. AT&T has dedicated substantial resources to guard against unlawful and unwanted text messages, including those generated with AI and message campaigns during elections. Our multi-layered defense against such messages includes tools designed to prevent unwanted text messages, technical protections including specialized spam filters, robust know your customer protocols for non-consumer messaging, collaborative efforts with the Commission and other law enforcement agencies, consumer spam reporting, and consumer education and outreach. In 2023, AT&T blocked 9.3 billion suspect text messages from reaching its customers.

In addition, AT&T requires that non-consumers sending messages to AT&T's customers comply with CTIA's Messaging Principles and Best Practices, which among other things, requires the sender obtain opt-in consent from consumers to send messages and honor opt-out/STOP requests. AT&T also requires that they comply with AT&T's Messaging Code of Conduct, which prohibits certain non-consumer messages and message campaigns.

AT&T stands ready to continue the work to combat unlawful and unwanted robocalls, whether or not they use AI. Please reach out to me if you have any further questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Rhonda Johnson", written in a cursive style.

Rhonda Johnson

Cc: Priscilla Delgado Argeris

⁵ See <https://i3forum.org/one-consortium/>