



TIN CAN ROBOCALL MITIGATION PLAN

VERSION 1

Last Updated February 27, 2026



I. Point of Contact

Recent Author:	Megan Fouty
Title:	General Counsel and Head of People and HR
Contact:	Megan Fouty, megan@tincan.kids
Policy Type:	Compliance
Version:	1.0
Last Update:	February 27, 2026
Next Review:	1-year or until superseded

II. Overview

Tin Can Untechnologies, Inc. (“Tin Can,” “we,” “our”) is a non-interconnected voice over internet protocol (“VoIP”) provider with indirect access to numbering resources through Twilio and Bandwidth.

Tin Can offers a VoIP service that reimagines the landline specifically for children and other populations for whom unrestricted two-way access to the PSTN might be deemed unsafe by their parents or caretakers. Tin Can achieves this goal by providing customers with a device that connects to the internet and functions as a VoIP device. The resulting Tin Can phone operates on Tin Can's proprietary network with its own extension number and users can only communicate with another approved Tin Can device as part of a fully closed network. This service is not a “voice service” as defined in 47 CFR § 64.1600(r) and, therefore, is not subject to the Robocall Mitigation Database (RMD) filing requirement.

In addition to the default closed Tin Can network, Tin Can also offers, as a distinct offering, the ability to whitelist a limited number of specific contacts chosen by the subscriber that do not have a Tin Can device, thereby allowing the end users (e.g., children of the subscriber) to have the restricted ability to interconnect with certain parties via the PSTN. For this limited offering, Tin Can has implemented STIR/SHAKEN caller ID authentication technology in the IP portions of its network through Twilio and Bandwidth, who certify traffic on Tin Can’s behalf, pursuant to the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act.

Tin Can certifies in the RMD and in this Robocall Mitigation Plan that it has fully implemented STIR/SHAKEN for the applicable services and has instituted a robocall mitigation program to prevent Tin Can from originating illegal robocalls. Tin Can also certifies that it has not been prohibited from filing in the RMD by any Commission action or order.

This Robocall Mitigation Plan is filed without prejudice to the merits of the pending Petition for Declaratory Ruling, requesting that the Commission declare that Tin Can’s service does not constitute an interconnected VoIP service or, in the alternative, waive such regulatory requirements applicable to interconnected VoIP services.¹

III. STIR/SHAKEN

Tin Can has implemented STIR/SHAKEN into the non-closed IP portions of our network (i.e., calls made

¹ Far Homes, Inc. d/b/a Tin Can, Petition for Declaratory Ruling, WC 25-288 (May 20, 2025), <https://www.fcc.gov/ecfs/document/105212663826316/1>.



to the limited set of whitelisted numbers over the PSTN). We are also compliant with all relevant Commission orders pertaining to caller ID authentication technology requirements.

IV. Robocall Mitigation

Tin Can has taken the following steps to prevent the origination of illegal robocalls on its network:

- By the nature of Tin Can’s services, the services functionally cannot be used to place calls using an automatic telephone dialing system or an artificial or prerecorded voice, including an AI-generated voice. The services also functionally cannot be used to place high-volume, low-duration traffic.
- Tin Can has procedures in place to confirm the identity of new and renewing Tin Can customers. For example, Tin Can collects certain customer information, including subscriber names, phone numbers, email addresses, and billing information before commencing service.
- Tin Can publishes the Tin Can Terms of Service (TOS), including the Acceptable Use Policy (AUP) incorporated therein, which governs access to and use of the Tin Can service.² The TOS requires that customers provide accurate and up-to-date information. The AUP requires that users (i) only use the services for their intended purpose; (ii) only place calls to friends and family members; (iii) not violate applicable law, including the Telephone Consumer Protection Act (TCPA) and Truth in Caller ID Act; (iv) not use the services for commercial purposes or any purpose other than normal residential use; and (v) not use the services for any harassing, threatening or intimidating purposes, among other requirements.
- Tin Can may suspend or terminate access to the Tin Can services for violations of the TOS or AUP.

Tin Can has implemented “Know Your Customer” policies:

- Tin Can contracts with a limited number of upstream and downstream providers and has a point of contact for robocall mitigation matters at each provider.
- As noted above, Tin Can collects certain customer information, including subscriber names, email addresses, and billing information.

Although it is not possible to place robocalls using Tin Can’s services, Tin Can commits to:

- Respond to traceback requests from the Commission, civil and criminal law enforcement, and the FCC-designated industry traceback consortium within 24 hours;
- Cooperate with the aforementioned entities in investigating any unlawful robocalls; and,
- Block any unlawful traffic if notified to do so by the Commission.

V. Certifications and Plan Updates

Tin Can certifies that it is not prohibited from filing in the RMD. Tin Can also certifies that it is not and has not been subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.

If there is a material change to this plan, Tin Can will file an updated Robocall Mitigation Plan with the Commission’s Robocall Mitigation Database within the regulatory period.

² Tin Can Terms of Service, <https://tincan.kids/policies/terms-of-service> (last updated Jan. 6, 2026).