

Robocall Mitigation Plan

Business Information

Firepit, Inc. d/b/a Pinwheel
1250 Capital of Texas Highway South, Building 3
Suite 400
Austin, Texas, 78746

Contact Information

Dane Witbeck
CEO and Founder
404-610-7165
support@pinwheel.com

Overview

In the Commission's recent release, *Call Authentication Trust Anchor*, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd. 2573 (2023) ("R&O"), it is stated that all voice service providers ("VSPs") must file robocall mitigation plans ("RMPs") that, among other things, outline "reasonable steps" taken to avoid originating illegal robocalls.

In addition to the "reasonable steps," the FCC requires that a RMP include:

- "know your customer" procedures;
- "know your upstream provider";
- ownership information;
- a description of any call analytics system used to identify and block illegal traffic; and
- whether a third-party vendor is used and if so, the name of the vendor.

The FCC previously stated that an RMP is sufficient if the detailed practices in the plan can reasonably be expected to significantly reduce the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

Purpose

Firepit, Inc. d/b/a Pinwheel ("Pinwheel") is dedicated to stopping illegal calls from traversing our network and monitoring the calls coming into our network. Pinwheel is a "pure reseller" that has no control over the infrastructure necessary to implement STIR/SHAKEN. As such, Pinwheel was previously exempt from the FCC's STIR/SHAKEN rules. The R&O requires that pure resellers such as Pinwheel now file RMPs. This document delineates Pinwheel's RMP. Because Pinwheel does not have access to the necessary infrastructure, it relies on its upstream carrier to assist in robocall mitigation. As delineated herein, Pinwheel works closely with its upstream provider to carry out the required mitigation functions.

Overview of Pinwheel's Service Offering

Pinwheel offers the Pinwheel Home service, which is a managed, parent-controlled home phone service designed exclusively for families ("Pinwheel Home"). Pinwheel Home is a managed analog telephone adapter ("ATA") service providing a safe, parent-controlled home phone line for children

ages 8 – 12+. The product’s architecture inherently minimizes robocall risk: all calling is restricted to a caregiver-approved Safelist, international calling is disabled, and there is no capability for automated or mass dialing. Pinwheel uses Bandwidth Inc. as its sole underlying voice carrier, leveraging Bandwidth’s owned-and-operated network infrastructure, STIR/SHAKEN compliance, and robocall mitigation capabilities. Pinwheel is committed to full compliance with FCC STIR/SHAKEN and robocall mitigation requirements and is engaging a specialized telecommunications legal counsel, The CommLaw Group, and a compliance consultancy firm, The Compliance Group, to ensure all filings and certifications are properly maintained.

The following measures inherently prevent illegal robocall origination:

- **Closed Network / Safelist-Only Calling:** All outbound calls are restricted to a caregiver-approved contact list (Safelist). Users cannot dial arbitrary numbers — only pre-approved contacts and emergency services (911). This architecture eliminates the possibility of mass automated or unsolicited outbound calling.
- **Caregiver-Gated Account Provisioning:** Every Pinwheel Home account requires setup by a verified adult caregiver (18+, legal guardian). The caregiver controls all calling permissions, contact lists, and time-of-day restrictions through the Pinwheel Caregiver App.
- **No Auto-Dialing or Programmatic Calling:** The Pinwheel Home device is an ATA connected to a physical handset. It does not support auto-dialers, predictive dialers, or any programmatic/API-initiated calling.
- **International Calling Disabled:** International outbound calls are disabled entirely on the platform.
- **Upstream Carrier Protections:** Bandwidth, our underlying voice carrier, employs machine-learning-based call analytics, network traffic anomaly detection, and call-blocking tools at the network level to detect and prevent illegal traffic.
- **Volume Monitoring:** Given the residential single-line nature of Pinwheel Home, any unusual call volume or pattern would be flagged for review. The expected usage profile is low-volume residential calling.

Know Your Customer (“KYC”)

Pinwheel implements the following KYC practices for Pinwheel Home subscribers:

- **Identity Verification:** Every account must be created by an adult caregiver (18+) who is the legal guardian of the child user. Account registration requires full legal name, email address, physical service address, and payment information.
- **Payment Verification:** Subscriptions require a valid credit card or payment method tied to the caregiver’s identity. This serves as an additional layer of identity verification.
- **Service Address Registration:** Caregivers must provide and maintain a current physical service address (required for E911 compliance). This address is verified during setup.
- **Single-Line Residential Use:** Each Pinwheel Home device is tied to one phone number and one caregiver account. The service is designed and marketed exclusively for residential family use — not commercial or enterprise use.

- **Caller ID Restrictions:** Subscribers cannot modify or spoof their assigned Caller ID. The Caller ID is set to the NANP number assigned by Bandwidth and cannot be altered by the user.
- **Terms of Service / AUP Acceptance:** Caregivers must accept Pinwheel's Terms of Service, which prohibit any use of the service for unsolicited calling, telemarketing, robocalling, or any illegal purpose.
- **Prohibited Uses:** Tampering with firmware, reselling the service, or using the device with unauthorized VoIP providers is expressly prohibited and grounds for service termination.

Know Your Upstream Providers

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls, and Call Authentication Trust Anchor*, Seventh Report and Order in CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking in CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59, 38 FCC Rcd 5404 (2023), Pinwheel provides the following information concerning its upstream voice service carrier.

Pinwheel has one upstream provider from which it receives voice traffic:

Bandwidth Inc.
2230 Bandmate Way
Raleigh, North Carolina 27607
Stephen Thayer
voicsecurity@bandwidth.com

Pinwheel has a master service agreement with its upstream provider and has received assurances in writing from its officials that it has, and will continue to sign calls transmitted to Pinwheel and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to Pinwheel. Pinwheel and its upstream provider have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Acceptable Use Policy ("AUP")

As part of its Terms of Service, Pinwheel maintains an AUP that subscribers must sign before being permitted to use Pinwheel's services. Among other things, the AUP prohibits:

- Unsolicited, automated, or robocall-type calling
- Telemarketing or commercial solicitation
- Caller ID spoofing or manipulation
- Use of the service for any illegal purpose
- Tampering with device firmware or using the device with unauthorized providers
- Resale of the service

Pinwheel's contractual terms with subscribers specify that Pinwheel may take action up to suspension or termination of service for violation of the AUP.

Mitigation During Service

Pinwheel works with its upstream provider to ensure that all subscribers can report any suspicious call connected through their account and measures are set to prevent future calls from/to those individual numbers for all subscribers. When traffic analysis indicates the presence of likely illegal

robocalling, Pinwheel works with its upstream provider to follow defined procedures on investigating such subscribers. Because Pinwheel does not have the infrastructure to implement STIR/SHAKEN, no third-party vendors are involved in Pinwheel's analytics.

Pinwheel maintains the following procedures to investigate potentially illegal robocall activity:

- **Automated Monitoring:** Given the Safelist-only architecture, any call attempt to a non-approved number is automatically blocked and logged. Repeated blocked attempts would trigger review.
- **Usage Pattern Analysis:** Pinwheel monitors call logs, duration, and frequency. Any account exhibiting abnormal call volume (inconsistent with single-line residential use) is flagged for internal investigation.
- **Carrier-Level Monitoring:** Bandwidth's fraud mitigation team independently monitors network traffic for anomalies and potential illegal robocall campaigns using machine-learning tools.
- **Complaint Response:** Any consumer complaints or reports of suspicious activity related to a Pinwheel Home number are investigated promptly, with the ability to suspend service pending review.
- **Cooperation with Authorities:** Pinwheel will cooperate fully with the FCC, law enforcement, and the Industry Traceback Group in any investigation involving traffic originating from its platform.
- **Account Termination:** Pinwheel reserves the right to immediately suspend or terminate any account found to be in violation of its AUP or engaged in illegal calling activity.

Investigate Suspicious Activity

Pinwheel follows Industry Traceback Group ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, Pinwheel will devote sufficient resources to provide prompt and complete resources to traceback requests. Pinwheel will maintain a designated contact to receive and respond to ITG traceback and DNO requests.

Pinwheel commits to respond within 24 hours to all traceback requests from the FCC, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

Pinwheel works with its upstream provider to investigate suspicious activity found by the carrier's monitoring systems or reported to Pinwheel by subscribers or third parties. The investigation could potentially result in opening a traceback request or with Pinwheel contacting a subscriber to correct improper use of the applicable platform, or, if the subscriber does not respond or comply, to notify its upstream provider to block their use of the platform.

For all new and renegotiated Pinwheel contracts governing the transport of voice calls, Pinwheel will endeavor to contractually require Pinwheel's subscribers to cooperate in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered our network.

Blocking

Pinwheel will implement Do Not Originate requests it receives from ITG. Upon receipt of a DNO request, Pinwheel will block the specified number from originating on its platform within 24 hours and investigate the source of any flagged traffic. Bandwidth also maintains DNO response mechanisms at the network level.

Pinwheel's upstream provider has mechanisms to automatically block suspicious calls using internal analytics. If Pinwheel and/or its upstream carrier identifies suspected robocalling patterns that are confirmed with further investigation, Pinwheel will take appropriate action which may include suspending or terminating the subscriber's use of Pinwheel's service. Pinwheel will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement (including the state attorney general's office), as well as the FCC, and/or ITG; as well as documenting requests & actions taken in response thereto.

Plan Updates

This plan, along with industry best practices, will evolve to response to the dynamic nature of mitigating illegal robocalling. Pinwheel will monitor industry best practices and continuously improve our internal processes to ensure this plan, and our system adapts to this ever-changing issue.

In the event of any material change to this plan, Pinwheel will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.

Certification of Dane Witbeck

I, Dane Witbeck, CEO and Founder of Firepit, Inc. d/b/a Pinwheel ("Pinwheel"), do hereby certify, under penalty of perjury, the following:

- (1) Pinwheel, by virtue of its status as a "pure reseller" does not have access to the necessary infrastructure to implement STIR/SHAKEN and therefore has not implemented STIR/SHAKEN in the IP portions of its network.
- (2) Pinwheel's Business name and primary address are as follows:

Firepit, Inc. d/b/a Pinwheel
1250 Capital of Texas Highway South, Building 3
Suite 400
Austin, Texas, 78746
- (3) Pinwheel uses the following d/b/a names: "Pinwheel," "Pinwheel Home."
- (4) Pinwheel has not previously used any other business name.
- (5) Pinwheel has the following principals: Dane Witbeck, Michael Dowdle. These individuals have not had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (6) Pinwheel has no parent companies, subsidiaries, or affiliates.
- (7) The name, title, department, business address, telephone number, and email address of the individual responsible for addressing robocall-related issues are listed in the above robocall mitigation plan.
- (8) Pinwheel's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- (9) Pinwheel has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (10) Pinwheel is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (11) Pinwheel is not required to have, and does not have an operating company number.



Dane Witbeck

04/20/2026

Date: _____