

Robocall Mitigation Plan

Business Information

HomeWAV, LLC
2020 Westport Center Dr.
Saint Louis, MO 63146

Contact Information

Alireza Khamesipour
Director of Software Engineering
844-394-6639
a.khamesipour@homewav.com

Overview

In the Commission's release, *In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking*, WC Docket No. 17-97 (rel. March 17, 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;
- 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 a 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

HomeWAV, LLC ("HomeWAV") is a small VSP, that provides outbound-only, voice communication solutions for inmates in correctional institutions. HomeWAV's voice traffic originates from a web browser/application by inmates and is transmitted to an upstream provider's servers using WebRTC. All voice calls originate only from the web browser on the locked down Windows PC, or an Android application installed on HomeWAV's custom tablets physically located in the correctional facilities that have inmate calling service provider agreements with HomeWAV. The upstream providers perform any protocol conversion needed for termination of voice traffic to PTSN.

Homewav tracks the points of origination and termination of all call traffic. To provide the service, Homewav purchases and resells hardware, and software from suppliers.

The R&O requires that all VSPs now file RMPs. This document delineates HomeWAV's RMP. Because HomeWAV does not have direct access to SIP trunks, it relies on its upstream carriers to assist in robocall mitigation. As delineated herein, HomeWAV works closely with its upstream providers to carry out the required mitigation functions.

Know Your Customer ("KYC")

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber. In HomeWAV's situation, a subscriber is an inmate who utilizes HomeWAV's system within a correctional facility that contracts with HomeWAV for the voice service described herein. Under this scenario, HomeWAV and its institutional customers, which keep records of callers and usage, always know who is utilizing its services.

Know Your Upstream Providers

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls 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* (Rel. May 19, 2023) ¶¶ 49-51, HomeWAV provides the following information concerning its upstream voice service carrier.

HomeWAV has two upstream providers from which it receives voice traffic:

1. Bandwidth Inc.
900 Main Campus Drive
Suite 100
Raleigh NC 27606
Stephen Thayer
voicsecurity@bandwidth.com
2. Twilio Inc
101 Spear Street, 1st Floor
San Francisco California 94105
Melissa Blassingame
mblassingame@twilio.com

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

Acceptable Use Policy ("AUP")

HomeWAV maintains an AUP that its institutional customers must sign before being permitted to use HomeWAV's network. Among other things, the AUP prohibits:

- providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call;
- violating any applicable local, state, or federal law;
- violating applicable industry accepted guidelines; and
- using HomeWAV's service to engage in or in connection with fraudulent activities.

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

Analytics for Monitoring Traffic

HomeWAV works with its upstream providers to identify behaviors which indicate illegal call activity. Examples of calling patterns monitored:

- multiple overlapping calls on the same account is a risk of not having a single subscriber using the service;
- velocity on initiate calls (synchron intervals, quick dialing back-to-back calls);
- recent volumes (last 60 min) vs weekly trends;
- number of unique destination numbers in a time frame (total account level);
- number of unique source numbers in a time frame (total and account level); and
- anomalies in call duration distribution (most calls having similar duration is not representative for residential service usage).

No third parties are involved in deploying HomeWAV's analytics.

Investigate Suspicious Activity

When traffic analytics indicate the presence of likely illegal robocalling, HomeWAV works with its upstream providers to follow defined procedures on investigating such subscribers.

The procedures established include but are not limited to:

- checking recent and past call detail records and benchmark against expected trends;
- checking recent and past account activity and purchases;
- investigating if any system issue generates the strange behavior; and
- verifying that the call originating path is valid.

HomeWAV follows the Industry Traceback Group's ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, HomeWAV will devote sufficient resources to provide prompt and complete resources to traceback requests.

HomeWAV works with its upstream providers to investigate suspicious activity found by the carrier's monitoring systems or reported to HomeWAV by subscribers or third parties. The investigation could potentially result in opening a traceback request or with HomeWAV 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.

Blocking

HomeWAV will implement Do Not Originate requests it receives from the ITG. HomeWAV's upstream provider has mechanisms to automatically block suspicious calls using internal analytics. If HomeWAV and/or its upstream carrier identifies suspected robocalling patterns that are confirmed with further investigation, HomeWAV will take appropriate action which may include suspending or terminating the subscriber's use of HomeWAV's service. HomeWAV 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 the ITG;) as well as documenting requests & actions taken in response thereto.

Plan Updates

This plan and industry best practices must evolve to response to the dynamic nature of mitigating illegal robocalling. HomeWAV will monitor industry best practices and continuously improve our internal processes to ensure this plan and our system adapt to this ever-changing issue.

In the event of any material change to this plan, HomeWAV 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 Morteza Sahebkar

I, Morteza Sahebkar, General Counsel of HomeWAV, do hereby certify, under penalty of perjury, the following:

(1) HomeWAV 's Business name and primary address are as follows:

HomeWAV, LLC
2020 Westport Center Dr.
Saint Louis, MO 63146

(2) HomeWAV has no other business names in use.

(3) HomeWAV has not previously used any other business name.

(4) 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.

(5) HomeWAV has three principals who own 10% or more of the company: Jay R. Johnson & Kelly L. Johnson Joint Trust – 61.86%, Daniel Farris – 10.31%, and Vanessa T. White Declaration of Trust – 10.31%. HomeWAV has no parent companies or subsidiaries.

(6) HomeWAV's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.

(7) HomeWAV has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.

(8) HomeWAV is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.

(9) HomeWAV is not required to, nor does it have, an OCN.

Morteza Sahebkar

Morteza Sahebkar
Chief Executive officer