

Robocall Mitigation Plan

Business Information

Weave Communications, Inc.
1331 West Powell Way
Lehi, UT 84043

Contact Information

Erin Goodsell
Chief Legal Officer
legal@getweave.com

Overview

The FCC requires that, by February 26, 2024, all voice service providers ("VSPs") certify in the Robocall Mitigation Database that they have implemented a Robocall Mitigation Plan ("RMP") to ensure that they are not originating illegal robocalls.

The FCC requires that VSPs develop a RMP that:

- details the reasonable steps taken to avoid originating illegal robocalls;
- describe how they are meeting their existing obligations to take affirmative action to prevent new and renewing customers from originating illegal calls;
- describe any know-your-upstream provider;
- describe any call analytics systems in place designed to identify and block illegal traffic;
- demonstrates a commitment to respond to traceback requests to cooperate with investigators and stopping illegal robocalls; and
- is filed in the Robocall Mitigation Database.

The FCC states 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

Weave Communications, Inc. ("Weave") is a small VSP dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network. This document delineates Weave's RMP.

Know Your Customer

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber. A subscriber is an entity that has a business relationship with Weave in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

New Subscribers

All new subscribers go through identity verification protocols which are a mixture of algorithmic check and manual call back. A risk score is developed to ensure the

authenticity of a new subscriber. This score checks the identity marker collected during an account registration process. These include but are not limited to: name, email address, credit card information and contact phone number.

These identity markers are validated for accuracy against public and paid tools. All new subscriber activity is monitored as further explained below.

Existing Subscribers

Weave requires updates of subscribers' information on all their orders. Each order's identity markers are verified again to ensure the account is not compromised and is being used for its intended purpose.

Know-Your-Upstream-Provider

Weave has taken reasonable and effective steps to ensure that its immediate upstream providers are not using it to carry or process a high volume of illegal traffic. Weave has done this by exercising reasonable due diligence before accepting upstream traffic. Weave knows who its upstream providers are and maintains information on how to appropriately contact the upstream provider in the event Weave identifies instances of suspect activity.

Acceptable Use Policy

Weave maintains an Acceptable Use Policy ("AUP") that subscribers must sign before being permitted to use Weave's network. Among other things, this 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 Weave's service to engage in or in connection with fraudulent activities.

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

Telephone Number Authorization

A Telephone Number ("TN")-based caller identity is the originating phone number included in call signaling used to identify the caller for screening purposes that is uniquely associated with the subscriber. A subscriber is permitted to use a TN as a caller identity if a TN is directly managed by Weave and/or obtained by Weave from one of Weave's underlying carriers for use by the subscriber. In most cases, Weave directly manages the TNs used by its subscribers. Weave tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of Weave's assignment of the TN to its subscriber.

If a subscriber wishes to use a TN as a caller identity and that TN is not directly managed by Weave, then TN validation is necessary. If a subscriber's end-user can provide a valid letter of authorization that they are the authorized user of such TNs, Weave will attest calls originated with these TNs.

When originating a call, Weave checks the calling party number against Weave's inventory and will not attest the call unless the calling party number is a TN that has been properly validated.

Mitigation Through Contracts

All subscribers agree to participate in traceback requests (this is part of the Terms and Conditions which users must agree to when creating an account with us).

During Service

All subscribers can report any suspicious call connected through their account and measures are set to prevent future calls from/to that individual numbers for all subscribers (none routed by the platform from that moment on - blacklisting). These features are:

- VoIP originated calls are signed with subscriber caller ID only after TN authorization (as discussed above); and
- Requiring authentication to initiate any call.

Monitor Traffic with Analytics

- Weave does not perform any analytical traffic monitoring, with a vendor or in-house. Weave does stop load-based call abuse, inbound and outbound to protect Weave's phone systems stability.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, our risk prevention team is alerted which follows the 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;
- verifying that the call originating path is valid; and
- contacting the subscriber to understand his particular use case and validate that the activity belongs to that subscriber.

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

Weave will investigate suspicious activity found by its monitoring systems or reported to Weave by subscribers or third parties. The investigation could potentially result in opening a traceback request or with Weave contacting a subscriber to correct improper use of the platform, or, if the subscriber does not respond or comply, to block their use of the platform.

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

Blocking

When it is administratively feasible, Weave will implement Do Not Originate requests it receives from the ITG. Weave has mechanisms to automatically block suspicious calls using internal analytics. If Weave's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Weave will take appropriate action which may include suspending or terminating the

subscriber's use of Weave's network. Weave 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), to the FCC, and/or the ITG; as well as documenting requests & actions taken in response thereto. Weave will respond to traceback requests from the Commission, civil and criminal law enforcement, and the ITG within 24 hours.

Information on Principals, Affiliate, Subsidiaries, and Parent Companies

Weave Communications, Inc. is a publicly traded company listed on the NYSE as Weav. Weave currently has no affiliates, subsidiaries, or parent companies.

Weave's Executive team is led by Brett White as CEO, Alan Taylor as CFO, Erin Goodsell as CLO, David McNeil as CRO, Chris Baird as CMO, Branden Neish as CTO, Marus Bertilson as COO, and Brooke Shreeve as CPO.

Additional information about Weave Communications, Inc's leadership can be found through the SEC's website.

Regulatory Action

Weave is not subject to any regulatory or enforcement action.

Plan Updates

This plan and industry best practices must evolve to respond to the dynamic nature of mitigating illegal robocalling. Weave 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, Weave 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.