

Robocall Mitigation Plan

Business Information

Unity Wireless Inc.
21113 Johnson St
Unit 101
Pembroke Pines FL 33029

Contact Information

Bilal Saleh
President
9545363231
bilal@unitywireless.com

Overview

In the Commission's recent 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;
- "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 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

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

business relationship with Unity Wireless in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

Unity Wireless's KYC program involves obtaining specific subscriber information when payment is made for services. This process includes collecting such information such as:

- physical business location;
- contact person(s);
- nature of the customer's business.

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, Unity Wireless provides the following information concerning its upstream voice service carrier.

Unity Wireless has one upstream provider from which it receives voice traffic:

UVNV, Inc. d/b/a Plum
1550 Scenic Ave. Suite 100
Costa Mesa CA 92626
Dave Bergin
daveb@plum.mobi

Unity Wireless 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 Unity Wireless, and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to Unity Wireless. Unity Wireless 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")

Unity Wireless maintains an AUP that subscribers must sign before being permitted to use Unity Wireless's network. Among other things, the AUP prohibits:

- Using the Device or Services to impersonate any person or entity;
- Using the Services to distribute, publish, send, or engage in: (i) commercial, marketing, advertising, or promotional communications or solicitations to any person without the person's consent; (ii) spam, chain mail, bulk messages, automatically generated messages, numerous copies of the same or substantially similar messages, empty messages, or messages that contain no substantive content; and (iii) telemarketing, autodialed, or prerecorded communications. This includes using our mail servers or another site's mail server to relay messages without the express permission of the account holder or the site.

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

Mitigation During Service

Unity Wireless 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 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 number validation via SMS; and
- requiring authentication to initiate any call, or a whitelist of originating numbers that is under customer's control.

Analytics for Monitoring Traffic

Unity Wireless works with its upstream provider to identify behaviors which indicate illegal call activity. Examples of calling patterns monitored:

- anomalies in cost generated by calls from a single customer;
- 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).

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, Unity Wireless works with its upstream provider 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;
- 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.

Because Unity Wireless does not have the infrastructure to implement STIR/SHAKEN, no third-party vendors are involved in Unity Wireless's analytics.

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

Unity Wireless works with its upstream provider to investigate suspicious activity found by the carrier's monitoring systems or reported to Unity Wireless by subscribers or third parties. The investigation could potentially result in opening a traceback request or with Unity Wireless 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 Unity Wireless contracts governing the transport of voice calls, Unity Wireless will endeavor to contractually require Unity Wireless's subscribers to cooperate in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered our network.

Blocking

Unity Wireless will implement Do Not Originate requests it receives from the ITG. Unity Wireless's upstream provider has mechanisms to automatically block suspicious calls using internal analytics. If Unity Wireless and/or its upstream carrier identifies suspected robocalling patterns that are confirmed with further investigation, Unity Wireless will take appropriate action which may include suspending or terminating the subscriber's use of Unity Wireless Unity Wireless's service. Unity Wireless 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. Unity Wireless 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, Unity Wireless 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 Bilal Saleh

I, Bilal Saleh, President of Unity Wireless, do hereby certify, under penalty of perjury, the following:

- (1) Unity Wireless, 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) Unity Wireless 's Business name and primary address are as follows:

Unity Wireless Inc.
21113 Johnson St
Unit 101
Pembroke Pines FL 33029
- (3) Unity Wireless has no other business names in use.
- (4) Unity Wireless has not previously used any other business name.
- (5) Unity Wireless has the following owners, directors, officers, or affiliates: Bilal Saleh, Yazan Saleh, Mingle Mobile, LLC. None of these persons/entities have had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (6) 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.
- (7) Unity Wireless's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- (8) Unity Wireless has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (9) Unity Wireless is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (10) Unity Wireless is not required to have and does not have an operating company number.



7/22/2024

Bilal Saleh