

Robocall Mitigation Plan

Business Information

Faith Wireless LLC
1307 Hodges Street
Raleigh, NC, 27604

Contact Information

Christian Massi
Co-Founder
215-779-3205
christian.massi@faithwireless.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 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

Faith Wireless LLC ("Faith Wireless") is a small prepaid-only VSP dedicated to stopping illegal calls from traversing our network and monitoring the calls coming into our network. Faith Wireless is a "pure reseller" that has no control over the infrastructure necessary to implement STIR/SHAKEN. As such, Faith Wireless was previously exempt from the FCC's STIR/SHAKEN rules. The R&O requires that pure resellers such as Faith Wireless now file RMPs. This document delineates Faith Wireless's RMP. Because Faith Wireless does not have access to the necessary infrastructure, it relies on its upstream carrier to assist in robocall mitigation. As delineated herein, Faith 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 Faith Wireless in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

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

- customer's name;
- physical address; and
- contact person(s).

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

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

Airespring, Inc.
600 Cleveland Street
Suite 226
Clearwater FL 33755
Brad Port
brad.port@airespring.com

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

Mitigation During Service

Faith 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

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

Faith 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, Faith Wireless will devote sufficient resources to provide prompt and complete resources to traceback requests. Faith Wireless 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.

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

Blocking

Faith Wireless will implement Do Not Originate requests it receives from ITG. If Faith Wireless and/or its upstream carrier identifies suspected robocalling patterns that are confirmed with further investigation, Faith Wireless will take appropriate action which may include suspending or terminating the subscriber's use of Faith Wireless Faith Wireless's service. Faith 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 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. Faith Wireless 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, Faith 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 Christian Massi

I, Christian Massi, Co-Founder of Faith Wireless, do hereby certify, under penalty of perjury, the following:

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

Faith Wireless LLC
1307 Hodges Street
Raleigh, NC, 27604
- (3) Faith Wireless has no other business names in use.
- (4) Faith Wireless has not previously used any other business name.
- (5) The following persons/entities own more than 10% of Faith Wireless each: Ian Durant, Christian Massi.
- (6) The following persons exercise management and control over Faith Wireless: Ian Durant, Christian Massi.
- (7) Faith Wireless has no parent companies, subsidiaries, or affiliates.
- (8) None of the persons/entities in items 5 – 6 above have had their licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (9) 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.
- (10) Faith Wireless's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- (11) Faith Wireless has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (12) Faith Wireless is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (13) Faith Wireless is not required to have, and does not have an operating company number.

Christian Massi

Christian Massi

04/06/2026