

Robocall Mitigation Plan

Business Information

EQ Telecom LLC
7533 S Center View Ct Ste N,
West Jordan, UT 84084

Contact Information

Peter Busulwa
Founder & CEO
8014384246
peterbusulwa@eqtelecom.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

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

Know Your Customer ("KYC")

EQ Telecom's KYC practices for prepaid wireless services align with standard procedures followed by U.S. prepaid providers. Using the Telgoo5 OSS/BSS platform, we collect and maintain the following customer information at the time of activation:

- Full Name
- Service Address

- Email Address
- Phone Number.

This customer information is required to establish a subscriber record and is retained for account management and compliance tracking.

Additional Controls:

- *Payment Monitoring.* Transaction processing is handled through EQ Telecom's integrated payment gateway. Payment frequency and transaction amounts are monitored through this system, and restrictions or alerts can be configured to address suspicious or excessive activity.
- *Caller ID Usage.* EQ Telecom relies on its upstream carrier for enforcement of caller ID authentication protocols, including STIR/SHAKEN compliance and robocall mitigation measures. EQ

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), EQ Telecom provides the following information concerning its upstream voice service carrier.

EQ Telecom has one upstream provider from which it receives voice traffic:

AT&T Mobility Services LLC ("AT&T")
601 New Jersey Ave, NW
Suite 650
Washington DC 20001
Adam Panagia
g03115@att.com

EQ Telecom has a master service agreement with BlueConnects, which is an MVNO aggregator/wireless reseller operating on and offering connectivity to the AT&T network. EQ Telecom received assurances in writing from BlueConnects officials that BlueConnects will assist EQ Telecom with any tracebacks requests and mitigate any illegal robocalls in close cooperation with AT&T and EQ Telecom.

Acceptable Use Policy ("AUP")

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

- Interfering with the network.
- Harassing, defrauding, intimidating, threatening, or invading the privacy of others.
- Unauthorized marketing, auto-dialing, or bulk messaging.
- Impersonation, spam, or use of bots/robots to access service.
- Altering or disguising the origin of calls or messages, including providing false caller ID information.
- Violating any applicable law, regulation, or third-party rights.
- Distributing viruses, malware, or launching denial-of-service attacks.

EQ Telecom's contractual terms with subscribers specify that EQ Telecom may take action up to suspension or termination of service for violation of the AUP. Moreover, EQ Telecom may forward relevant information to authorities when unlawful use is suspected and will comply with lawful law enforcement requests, including under the Patriot Act.

Mitigation During Service

EQ Telecom works with its MVNO aggregator, BlueConnects, 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).

EQ Telecom monitors usage activity within its platform and receives robocall mitigation alerts and traceback notices from BlueConnects. We review these reports and retain relevant subscriber-level account information to support investigations and mitigate improper use of services. EQ Telecom maintains clear customer records and supports all upstream and regulatory compliance processes as part of its robocall mitigation and customer accountability framework.

EQ Telecom works with BlueConnects to identify behaviors which indicate illegal call activity. Because EQ Telecom does not have the infrastructure to implement STIR/SHAKEN, no third-party vendors are involved in EQ Telecom's analytics. EQ Telecom works in coordination with BlueConnects to address any reported caller ID misuse or suspicious traffic patterns.

To allow for timely and comprehensive responses, EQ Telecom will devote sufficient resources to provide prompt and complete resources to traceback requests. EQ Telecom commits to responding to traceback requests fully within 24 hours.

Industry Traceback Group ("ITG")-recommended best industry practices are implemented by BlueConnects, which manages ITG participation on EQ Telecom's behalf.

EQ Telecom works with BlueConnects to investigate suspicious activity found by its monitoring systems or reported to EQ Telecom by subscribers or third parties. The investigation could potentially result in opening a traceback request or with EQ Telecom 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

EQ Telecom will implement Do Not Originate requests it receives from ITG. All Do Not Originate (DNO) requests are handled by BlueConnects, who notifies EQ Telecom of any relevant account-level action required. EQ Telecom cooperates fully with BlueConnects to address such requests.

If EQ Telecom and/or its upstream carrier or BlueConnects identify suspected robocalling patterns that are confirmed with further investigation, EQ Telecom will take appropriate action which may include suspending or terminating the subscriber's use of EQ Telecom's service. EQ Telecom 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. EQ Telecom 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, EQ Telecom 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 Peter Busulwa

I, Peter Busulwa, Founder & CEO of EQ Telecom LLC ("EQ Telecom"), do hereby certify, under penalty of perjury, the following:

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

EQ Telecom LLC
7533 S Center View Ct Ste N,
West Jordan, UT 84084
- (3) EQ Telecom has no other business names in use.
- (4) EQ Telecom has not previously used any other business name.
- (5) The following person owns more than 10% of EQ Telecom and exercises management and control over EQ Telecom: Peter Busulwa. He has not had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (6) EQ Telecom has no 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) EQ Telecom's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- (9) EQ Telecom has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (10) EQ Telecom is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (11) EQ Telecom is not required to have, and does not have an operating company number.



Peter Busulwa

Date: 10/06/2025