

Robocall Mitigation Plan

Business Information

Phoner Holdings LLC
3909 S Maryland Pkwy
Ste 314 PMB 514
Las Vegas NV 89119

Contact Information

Robert Ryan-Umberger
General Manager
702.329.1613
rryanumberger@phonerapp.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

Phoner Holdings LLC ("Phoner") is dedicated to stopping illegal calls from traversing the network and monitoring the calls coming into our network.

As certified in the FCC's Robocall Mitigation Database, Phoner has fully implemented STIR/SHAKEN. In compliance with the R&O, Phoner submits this RMP and certification.

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 Phoner in which we transmit, originate, and/or terminate calls on behalf of the subscriber.

Phoner's KYC program involves obtaining specific subscriber information onboarding subscribers. For enterprise users, this process includes collecting such information as:

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

Account signup requires a mobile phone 2FA, a subscription to our app via Google Play or Apple App Store, and an automatic risk score calculated based on various factors. A caller ID change is only performed manually by customer service on request. Users cannot change their Caller ID.

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), at ¶¶ 49-51, Phoner provides the following information concerning its upstream voice service carrier.

Phoner has one upstream provider from which it receives voice traffic:

Bandwidth, Inc
2230 Bandmate Way
Suite 400
Raleigh, NC 27607
Stephen Thayer
Director, Fraud Operations
voicsecurity@bandwidth.com
919-704-3069

According to the Robocall Mitigation Database, Bandwidth, Inc. ("Bandwidth") is fully STIR/SHAKEN compliant and, to the best of Phoner's knowledge, information, and belief, Bandwidth has been, and will continue to, sign calls transmitted to Phoner and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to Phoner. Phoner and Bandwidth have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Acceptable Use Policy ("AUP")

Phoner maintains an AUP that subscribers must agree to before being permitted to use its software and services. The following examples are prohibited activities, but they may not be limited by the listed activities below:

- Unauthorized advertising that are unsolicited, junk mail, chain letters, pyramid schemes, phishing, sweepstakes, gambling, unauthorized commercial activities, scams and sales, chain letters,
- Hacking or disruption to the Service, servers or networks that are connected to the Service
- Caller ID spoofing or misleading recipients to the source or origin of the communication.
- Phishing to collect or harvest users' personal information, email address or other contact information.
- Criminal activity or promotion of illegal activities.
- Content that contains threats, harm, harassment, abuse, obscenity, racial hate, porn, libel, defamatory, vulgar or any other objectionable words or sentences.

- Content that creates security or privacy risk to a person.
- Any other content that Phoner deems inappropriate or objectionable and that can expose our users or Phoner to any harm or liability of any type.
- Use for high volume calling, call centers, call pumping or any use that is excessive for an individual or business usage case.

Analytics for Monitoring Traffic

Phoner works with its upstream carrier to analyze high-volume voice traffic in order to identify and monitor patterns consistent with robocalls. Phoner has have various calling rate limiters, a blocked source and destination number database. Phoner flags potential violators based on risk scores, manually review activity, and have automated traffic warning alerts. If Phoner detects a calling pattern consistent with illegal robocalls, we will identify the party and take appropriate action. High risk scores and alerts trigger a manual internal evaluation, blocking numbers and/or accounts as necessary. Appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating subscriber owns or is authorized to use the Caller ID number, and suspending or terminating the party's ability to originate calls on our system. Additionally, Bandwidth may notify us of suspicious activity or violates their AUP, which will trigger the same manual investigation and blockage as required.

Phoner utilizes the following third-party vendors for its traffic analytics: Maxmind and IPQualityScore. It also utilizes internal call analytics.

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 or her particular use case and validate that the activity belongs to that subscriber.

High risk scores that are assessed via Phoner's procedures alerts trigger a manual internal evaluation, blocking numbers and/or accounts as necessary. Additionally, Bandwidth may notify us of suspicious activity or violates their AUP, which will trigger the same manual investigation and blockage as required.

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

Phoner certifies that it will respond to all traceback requests within 24 hours of receiving same.

Blocking

Phoner has various calling rate limiters, a blocked source and destination number database, we flag potential violators based on risk, manually review activity, and have automated traffic warning alerts. Phoner will implement Do Not Originate requests it receives from the ITG or other authoritative sources. DNO requests are promptly handled by inputting them into a blocked number table. If Phoner's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Phoner will take appropriate action which may include suspending or terminating the subscriber's use of Phoner's network.

Plan Updates

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

In the event of any material change to this plan, Phoner 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 Robert Ryan-Umberger

I, Robert Ryan-Umberger, General Manager of Phoner Holdings LLC ("Phoner"), do hereby certify, under penalty of perjury, the following:

(1) Phoner has fully implemented STIR/SHAKEN in the IP portions of its network.

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

Phoner Holdings LLC
3909 S Maryland Pkwy
Ste 314 PMB 514
Las Vegas NV 89119

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

(3) Phoner 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) Phoner has the following parent companies, affiliates, and subsidiaries: Meteor Mobile Holdings, Inc., Vumber Holdings LLC.

(6) The following persons exercise management and control over Phoner:

Michael Levit, Chief Executive Officer
Dux Ghandi, Chief Financial Officer

(7) None of the persons/entities in items 5 – 7 above have had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.

(8) Phoner's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.

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

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

Robert Ryan-Umberger

Robert Ryan-Umberger

09/21/2026

Date: _____