

Robocall Mitigation Plan

Business Information

BuyerCall LLC



Contact Information



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;
- 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

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

Currently our system does not allow automated outbound calling. We only allow manual outbound calling by humans. We only handle a very small amount of outbound calls.

Know Your Customer ("KYC")

BuyerCall collects business and contact information for new customers. BuyerCall specializes in serving small businesses and does not at this stage allow large scale communication from any of our customer accounts. All phone numbers provisioned for a customer are assigned to a customer's account. No customer has the ability to spoof a phone number or alter the caller ID of the phone numbers assigned to them.

BuyerCall may review any customer account at any time and make a determination on customer fit. If BuyerCall finds a customer to not be a good business partner or if the customer does not adhere to our TOS, BuyerCall has the right to close the account. BuyerCall services assist small businesses with capturing and nurturing inbound leads. BuyerCall is not intended to be used to create automated robocalls or to send bulk spam messages, and doing so would lead to a violation of TOS and suspension of the customer account.

BuyerCall'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;
- credit card information;
- contact person(s).

Minutes are restricted based on the subscription. Users cannot change the CNAM and only have the option of using the originating number or tracking number as display number caller id. For larger customers we engage and operate through contracts, which require address, business name, operation officer information. Inbound and Outbound calling is only a small part of our revenue.

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

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

Bandwidth Inc
900 Main Campus Drive
Suite 100
Raleigh NC 27606
Stephen Thayer
voicesecurity@bandwidth.com

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

BuyerCall maintains an AUP that subscribers must sign before being permitted to use BuyerCall's network. BuyerCall customers are subject to all restrictions and requirements set forth in our terms of service ("TOS"). Our TOS prohibit robocalling and activities normally associated with robocalling including, but not limited to:

- 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;
- using the BuyerCall service to engage in or in connection with fraudulent activities.

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

Mitigation During Service

BuyerCall 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

BuyerCall is continuously implementing measures that allow for the monitoring of call and messaging traffic through our services. All call traffic indicative of potential illegal robocalling will be flagged. We will take all necessary steps to suspend any customer account that deems to be in violation of our TOS and that we deem as purposely performing illegal practices such as robocalling.

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

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

Currently we are not using any specific analytics systems and review logs manually. BuyerCall works with its upstream provider to investigate suspicious activity found by the carrier's monitoring systems or reported to BuyerCall by subscribers or third parties. The investigation could potentially result in opening a traceback request or with BuyerCall 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 BuyerCall contracts governing the transport of voice calls, BuyerCall will endeavor to contractually require BuyerCall's subscribers to cooperate in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered our network.

Blocking

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

I, [REDACTED], Managing Partner of BuyerCall LLC, do hereby certify, under penalty of perjury, the following:

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

BuyerCall LLC
[REDACTED]
[REDACTED]

(3) BuyerCall has no other business names in use.

(4) BuyerCall has not previously used any other business name.

(5) BuyerCall has the following owners: [REDACTED] and [REDACTED]. Neither of these persons 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) BuyerCall's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.

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

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

(10) BuyerCall does not have an operating company number and is not required to have one.


[REDACTED]