

Robocall Mitigation Plan

Business Information

AutoBizLine, Inc.
11278 Carmel Creek Rd
San Diego, CA, 92130, USA

Contact Information

Rishan Chen
CEO
+1-858-722-3253
rishan.chen@autobizline.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 an 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 an RMP is sufficient if the detailed practices in the plan can reasonably be expected to reduce the origination of illegal robocalls and the VSP significantly complies with the practices it describes in its filing.

Purpose

AutoBizLine, Inc. ("AutoBizLine") is a small VSP dedicated to stopping illegal calls from traversing our network and monitoring the calls coming into our network. AutoBizLine is a "pure reseller" that has no control over the infrastructure necessary to implement STIR/SHAKEN. The R&O requires that pure resellers such as AutoBizLine now file RMPs. This document delineates AutoBizLine's RMP. Because AutoBizLine does not have access to the necessary infrastructure, it relies on its upstream carriers to assist in robocall mitigation and apply STIR/SHAKEN authentication where technically feasible. As delineated herein, AutoBizLine works closely with its upstream providers 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 AutoBizLine in which we transmit, originate, and/or terminate calls on behalf of the subscriber. We do not allow or support caller ID spoofing or caller name customization.

Phone calls made through the mobile app and website are intended for manual human-initiated communications. Automated robocalling is prohibited under AutoBizLine's policies. AutoBizLine does not provide automated dialing features within its mobile applications or web platform. AutoBizLine does not originate or permit autodialed, predictive dialer, automated outbound campaign, or prerecorded robocall traffic from customers. Calls are intended to be manually initiated by human users through approved applications or vetted SIP connections, subject to onboarding controls, traffic monitoring, concurrency limits, and call rate enforcement.

Users can pay for their accounts with a credit card or through Apple or Google in-app purchases. One device only allows one user to be used manually. If multiple users use one credit card, the system will be alerted, and the users might be blocked if not verified.

At the signup stage, AutoBizLine requests the following information from users:

- Name
- Email address
- Cell phone number
- IP address

As the users' usage increases, AutoBizLine asks users for more information:

- Physical address
- Occupation
- Activities description

If users made many calls (determined from the call analytics), we consider the usage as business activities and request and verify further business information before more calls are enabled:

- Business name
- Business address
- Business website
- Business industry and type
- Business registration number
- Business activities' description
- Contact person's name
- Contact person's cell phone number
- Verification code to verify with the contact person's cell phone number
- ID or business registration documents might be asked to verify the business use case

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, AutoBizLine provides the following information concerning its upstream voice service carriers.

AutoBizLine is a pure reseller and does not directly originate traffic into the Public Switched Telephone Network (PSTN). All PSTN interconnection and call authentication functions are performed by upstream voice service providers. AutoBizLine has three upstream providers that supply voice traffic entering the U.S. PSTN or are used to originate U.S. calls:

- 1) Twilio Inc
101 Spear Street, 1st Floor
San Francisco, CA 94105
Amy Holcroft
(415) 295-4909
aholcroft@twilio.com
- 2) Telnyx, LLC
311 West Superior St
Suite 504
Chicago IL 60654
Olive Morris
(312) 945-7420
olive@telnyx.com
- 3) Inteliquent, Inc.
1 North Wacker Dr, Suite 2500, Chicago, IL 60606
Stacy Graham
(217)-862-1953
fraudoperations@sinch.com

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

Acceptable Use Policy ("AUP")

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

- using the service in connection with the violation of or to violate any laws
- engaging in threatening, abusive, harassing, defamatory, libelous, malicious, deceptive, or fraudulent behavior.
- using the service in a manner that causes injury to a person or property
- using the service in any manner that violates industry standards or any third-party policies
- using the service to send spam (unsolicited bulk emails or messages)
- posting multiple messages similar in content to Usenet or other newsgroups, listservs, forums, e-mail mailing lists, or other similar groups or lists
- posting or transmitting any information or software that contains, but is not limited to, a virus, worm, cancelbot, or other harmful components
- without permission from the owner of a system or network, doing any of the following:
 - (i) accessing the system or network, (ii) monitoring data or traffic,
 - (iii) probing, scanning, and/or testing firewalls, (iv) testing the vulnerability of a system or network, or (v) breaching the security or authentication routines of a system or network

- use of any services in violation of any trademark, copyright, or any other intellectual property protection law or provision, or AUP policy of any third-party provider
- use of any Services to engage in unlawful telemarketing, robocalling, spoofing, and deceptive calling practices

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

Mitigation During Service

AutoBizLine works with its upstream providers to ensure that all subscribers can report any suspicious call connected through their account, and measures are set to prevent future calls from/to those individual numbers for all subscribers (none routed by the platform from that moment on - blacklisting).

Analytics for Monitoring Traffic

AutoBizLine works with its upstream providers to identify behaviors that indicate illegal call activity. AutoBizLine also has an analytics monitor & real-time blocking system to identify and block illegal traffic. Examples of calling patterns monitored include:

- A user has made many repetitive calls to one number in recent hours, but is not connected.
- A user has made/received many calls to/from different people and exceeded thresholds.
- A user has made consecutive calls to a range of phone numbers, i.e., number scanning.
- Anomalies in cost generated by calls from a single customer.
- Monitoring of calls-per-minute (CPM) and calls-per-second (CPS) thresholds, determined based on approved use case and account history.
- Multiple concurrent or overlapping calls on the same account pose the potential risk of not having a single subscriber using the service.
- Velocity on initiate calls (synchrony intervals, quick dialing back-to-back calls);
- Recent volumes (last 60 min) vs weekly trends;
- A large number of unique destination numbers in a time frame (total account level);
- A large number of unique source numbers in a time frame (total and account level); and
- Anomalies in call duration distribution (most calls having similar duration are not representative of residential service usage).

Such users are prevented from making further calls and asked to provide their business information with extra verification to prove their activities are legitimate:

- Business name
- Business website
- Business industry and type
- Business registration number
- Business activities description
- Contact person's name
- Contact person's cell phone number
- Verification code to verify with the contact person's cell phone number

- ID or business registration documents might be asked to verify their use case

Unverified users whose business call activities are flagged are blocked from making further calls.

Verified users are allowed to make more calls, but we periodically verify that their cell phone numbers are associated with them.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, AutoBizLine works with its upstream providers to follow defined procedures for investigating such subscribers.

AutoBizLine has an analytics system to automatically monitor users making multiple calls and identify potentially illegal robocalls. The system will automatically stop such users from making further calls, and they need to provide business information to prove their calls are legitimate. AutoBizLine also monitors the users' traffic patterns, call metadata, and complaint signals, and if the traffic is related to illegal activities, the user's account is disabled and fully blocked. Third parties can also report issues or cases to AutoBizLine, and AutoBizLine will review and handle such requests immediately.

AutoBizLine uses internal analytics and also relies on monitoring and analytics performed by upstream voice service providers.

AutoBizLine follows Industry Traceback Group ("ITG")'s recommended best industry practices and cooperates in traceback and trace-forward investigations. To allow for timely and comprehensive responses, AutoBizLine will devote sufficient resources to provide prompt and complete resources to trace-back requests. AutoBizLine will acknowledge and initiate investigation of traceback requests within one (1) business day of receipt and will cooperate with upstream providers and investigators to provide responsive information as it becomes available.

AutoBizLine works with its upstream providers to investigate suspicious activity found by the carrier's monitoring systems or reported to AutoBizLine by subscribers or third parties. The investigation could potentially result in opening a traceback request or AutoBizLine contacting a subscriber to correct improper use of the applicable platform, or, if the subscriber does not respond or comply, to notify its upstream providers to block their use of the platform.

For all new and renegotiated AutoBizLine contracts governing the transport of voice calls, AutoBizLine will endeavor to contractually require AutoBizLine's subscribers to cooperate in traceback investigations by identifying the upstream providers from which the suspected illegal robocall entered our network.

Additional Controls for SIP Trunking and PBX-Connected Customers

AutoBizLine currently provides limited SIP trunking services to a small number of vetted business customers. For SIP trunk service, additional monitoring and controls will be implemented.

For customers connecting via SIP trunking or PBX integrations, AutoBizLine applies enhanced onboarding and risk assessment procedures before service activation. These procedures are designed to reduce the risk of illegal robocall origination and include:

- Verification of business identity, including legal entity name, address, registration status, and authorized contact persons.
- Review of intended use cases, call patterns, and anticipated call volumes before provisioning SIP connectivity.
- Risk assessment based on industry classification, prior telecommunications history where available, and calling use case.
- Approval workflows for higher-risk industries or high-volume outbound calling scenarios.
- Execution of contractual agreements requiring compliance with applicable robocall laws and prohibiting automated or unlawful calling practices.
- Assignment of initial traffic limits pending satisfactory usage history.

AutoBizLine implements technical monitoring to detect abnormal traffic patterns originating from SIP-connected customers and application users. Monitoring includes:

- Calls-per-second (CPS) and calls-per-minute (CPM) monitoring at the account & trunk level.
- Concurrent call session monitoring to detect unusual call concurrency or system-driven dialing behavior.
- Automated alerts are triggered when outbound call velocity exceeds established thresholds based on account history and approved use cases.
- Progressive traffic controls, including temporary throttling, suspension, or investigation when abnormal calling activity is detected.
- Enhanced monitoring for new accounts and recently provisioned SIP trunks.

AutoBizLine utilizes internal analytics systems and upstream carrier monitoring to identify calling patterns commonly associated with illegal robocalling. Indicators include:

- Rapid sequential dialing across large blocks of telephone numbers.
- High volumes of short-duration or unanswered calls.
- Sudden increases in outbound traffic are inconsistent with approved usage.
- High ratios of unique called numbers within compressed timeframes.
- Number rotation or repeated caller ID substitution patterns.
- Call concurrency is inconsistent with manual human-initiated dialing.

When anomalous activity is detected, AutoBizLine may immediately restrict calling privileges pending investigation and subscriber verification.

AutoBizLine maintains the ability to implement technical and administrative controls in response to suspected unlawful traffic, including:

- Adjustment of call rate limits or concurrency thresholds.
- Temporary suspension of SIP trunks or application calling privileges.
- Immediate blocking of suspicious outbound traffic.
- Escalation to upstream carriers and participation in traceback investigations.
- Termination of service for confirmed violations.

Blocking

AutoBizLine will implement Do Not Originate requests it receives from the ITG. AutoBizLine's upstream providers have mechanisms to automatically block suspicious calls using internal analytics. If AutoBizLine and/or its upstream carriers identify suspected robocalling patterns that are confirmed with further investigation, AutoBizLine will take appropriate action, which may include suspending or terminating the subscriber's use of AutoBizLine's service. AutoBizLine 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. AutoBizLine maintains a single point of contact for traceback and regulatory requests

Plan Updates

This plan and industry best practices must evolve to respond to the dynamic nature of mitigating illegal robocalling. AutoBizLine 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, AutoBizLine 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.

AutoBizLine will review this plan at least annually in connection with Robocall Mitigation Database recertification.

Certification of Rishan Chen

I, Rishan Chen, CEO of AutoBizLine, do hereby certify, under penalty of perjury, the following:

- (1) AutoBizLine, 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) AutoBizLine’s Business name and primary address are as follows:

AutoBizLine, Inc.
11278 Carmel Creek Rd
San Diego, CA, 92130
USA
- (3) AutoBizLine has no other business names in use, but has a mobile app called MySecondLine app, and a child domain website called TalkHeap.com
- (4) AutoBizLine has not previously used any other business name.
- (5) Rishan Chen owns more than 10% of AutoBizLine and is its director. He has not 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) AutoBizLine’s role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- (8) AutoBizLine has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (9) AutoBizLine is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.



Rishan Chen

02 / 17 / 2026