

QuestBlue Systems, Inc is actively engaged in the following Robocall Mitigation Methods. 5/26/2025

BLACKLISTS

- Calling telephone number or prefixes
- Calling SPIDs (OCNs) that are not yours
- Calling Locations states/provinces/regions that are not identified by the client as locations.
- Improper ANI
- IP Addresses that are identified as robo callers
- Monitoring user agents that are used by robo callers. When a call is identified by a blacklisted attribute, we will block the call. Utilizing Reputation Scoring on traffic
- Constantly monitoring traffic for bad reputation Low ASR and ALOC
- Monitoring systems in place for immediate lookup of clients activity and statistics. CDR Analysis
- We are constantly engaged with CDR monitoring for identifiable markers on bad traffic.

Fully implemented on STIR/SHAKEN As we identify traffic that is not in compliance is subject to review or removal from our network.

We immediately communicate to interconnected carriers on our network.

We immediately block access to our network, and report to anyone in our carrier group what we have discovered potentially poor traffic resulting in a permanent ban on our network and portals. If we suspect anything could be wrong, we immediately contact our interconnected carriers for verification of what we found and take immediate action. Any client that is found to be in violation of our AUP will be immediately removed with zero tolerance of being allowed back on our network.

All new clients that are reselling our services are required to follow all the FCC rules for reselling telecommunications and be registered with the RMD. Even in the event we are working with a BPO and they are the end users, we still require a full RMD plan to be in place. Comments or questions can be sent to carriersupport@questblue.com

To further satisfy the FCC & the RMD specific to the following items:

- (1) *the specific reasonable steps the provider has taken to avoid originating, carrying, or processing illegal robocall traffic as part of its robocall mitigation program.*

QuestBlue specifically requests KYC along with KYCT (Know your Customers Traffic) where as a direct customer of QuestBlue must match and be current with licensing agencies along with a copy of the registered client's proof of identity, most recent three copies of other telecommunications companies used for services, provide a local contact that is in addition to a Registered Agent. The local contact must be available and with a physical US domestic address.

- (2) how it complies with its obligation to know its customers and/or upstream providers, as applicable.

QuestBlue will actively and continuously review the filings of the existing customer base and monitor for ITG notifications. Part of the KYCT (Traffic) portion, we are monitoring errors on the network where low ASR might be found in conjunction with robo-calling. When found we will block, lock and communicate to our customer to identify what has happened and why the traffic pattern has changed. As **QuestBlue is a member company of CFCA and actively participates in in global events to help prevent unwanted traffic for our own network and our upstream carriers.** <https://cfca.org/member-companies/> If a carrier was to notify QuestBlue of suspicious traffic patterns we immediately and proactively block access to our network until proven to be valid or invalid. If invalid traffic or suspicious traffic is found, an investigation is opened for QuestBlue to determine the future of this client. The outcome of the investigation will have two outcomes. Removed from our network or a documented warning where the traffic is not allowed and termination is next when not corrected. A documented warning can come from a breached system where our end user was unaware of that traffic and we assist in securing their systems against future threats. Our team provides this service at no cost to our customers to help prevent firewall breaches or poorly designed security measures on extensions.

(3) the analytics system(s) it uses to identify and block illegal traffic.

QuestBlue has engaged with telecom industry leaders to help develop internal systems to capture, monitor and filter unwanted traffic. We are actively adding blocks to any traffic with an automated method that matches low ASR, repeated calling patterns, traffic pumping, and calling numbers on a DNC among other proprietary methods available upon request to the RMD and not publicly posted to protect our methods of analyzing traffic.

(4) whether it uses any third-party analytics vendor(s) and the name(s) of such vendor(s).

QuestBlue is not using a third-party vendor.

Law Enforcement inquiries can be sent to lawenforcement@questblue.com and expected turnaround time on any inquiries is less than 24 business hours. QuestBlue complies with all inquiries.