

VORTEX RESEARCH PRIVATE LIMITED

Robocall Mitigation Plan

Robocall Mitigation Program Description

VORTEX RESEARCH PRIVATE LIMITED is an India-based licensed ISP and ITSP, providing international telecommunications. We buy communication minutes from various providers worldwide and resell them to our customers.

Either way Vortex operates at all times consistently with the rules regulations and orders of the Federal Communications Commission. We at all times consistently with the rules regulations and orders of the Federal Communications Commission. Specifically on the matters regarding short duration traffic.

Pursuant to 47 C.F.R. § 64.6305, we submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. This report describes the status of its implementation of STIR/SHAKEN and the practices and procedures we have in place to mitigate illegal robocalls.

We may modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time in order to respond to changes in its business, its capabilities and its needs.

STEPS TAKEN TO PREVENT ILLEGAL ROBOCALLS FROM ORIGINATING FROM OUR PLATFORM

Customer Documentation

We collects proof of identity & address while on-boarding a customer. Have specific agreements with the customer explaining the platform usage terms.

Illegal Robocall Mitigation:

We use several data analytics methods to detect illegal robo-calling patterns such as short but intense calling period, calls of similar length. High volume call termination to particular destination from a single or series CLI

Suspicious cases we request the carrier to verify the calling numbers and partially block & approach the carrier for resolution. Industry cooperation:

We fully cooperate in industry trace back efforts and law enforcement requests.

We allow only our CLIs which are obtained by us and if customer wish to use their CLI we have a Call OTP authentication mechanism by which they need to verify the CLI by a Call OTP which they receive on their active number.

Our network will be able to pass STIR/SHAKEN tokens as they come. We will not be modifying or changing the level of certification received. We have implemented several network-wide restrictions meant to curb any potential short-duration traffic such as: We have a network-wide ANI Blacklist. All calls from these ANI's are blocked and any calls to the DNC list are blocked.

Due diligence carried out our Customers:

Due Diligence and Customer Obligations During Onboarding

The platform we use for our VoIP Operations (Call Switching) provides us with various ways for ensuring client compliance with global telecom rules and regulations.

1. Due Diligence Processes:

- a) Spam Filtering: Spam Scout Spam Filter: Utilizes an in-house filtering solution with an evolving spam scoring and filtering algorithm and an updated database to block spam and scam calls.
- b) IPQS Spam Filter (Premium): Employs a comprehensive spam and scam filtering database to secure the network and prevent regulatory issues.

KYC (Know Your Customer):

- Utilizes Stripe and other KYC platforms to verify customer identities.
- Cross-checks company registrations to ensure legitimacy.

Real-Time Call Transcription Analysis:

- Implements Class 4 call transcription analysis to identify robocall campaigns and other malicious activities without recording audio to maintain data privacy and security.
- If flagged, customers must consent to call recording and audio analysis for fraud detection.

2. Customer Obligations:

Telecom Safety and Security Education:

- Customers are educated about their telecom safety, security obligations, and fair usage policies.

Undertaking Agreement:

- Customers sign an undertaking stating they understand and will adhere to their duties and obligations.
- Non-compliance can result in account suspension and being reported to appropriate authorities.

Fraud Detection and Reporting:

- If malicious activity is detected, customers are required to consent to call recording and audio analysis.
- Verified fraud results in the customer being reported to authorities along with documented evidence of their regulatory breaches.

Sample Contract Clauses:

1. Spam Filtering Clause:

"The Customer agrees to the implementation of Spam Scout Spam Filter and/or IPQS Spam Filter to prevent spam and scam calls. The Customer acknowledges the necessity of these filters to avoid regulatory fines and obligations."

2. KYC Compliance Clause:

"The Customer consents to KYC verification using Stripe and other platforms. The Customer's company registration details will be cross-checked to confirm legitimacy."

3. Safety and Security Undertaking:

"The Customer acknowledges receipt and understanding of their telecom safety and security obligations and fair usage policies. The Customer agrees to comply with these obligations, with non-compliance resulting in account suspension and potential reporting to authorities."

4. Consent for Call Recording:

"In cases where malicious activity is suspected, the Customer consents to the recording and analysis of their calls for fraud detection. The Customer understands that verified fraud will lead to reporting to appropriate authorities with supporting evidence."

Further monitoring and checking undertake; both automatic and manual:

Ongoing Monitoring and Checking During Client Relationship

A) Automatic Monitoring:

1. Spam Filters:

Spam Scout Spam Filter: Continuously operates with an evolving spam scoring and filtering algorithm and an updated database to block spam and scam calls in real-time.

IPQS Spam Filter (Premium): Provides comprehensive real-time filtering of spam and scam calls using the latest database to secure the network.

2. Real-Time Call Transcription Analysis:

Constantly analyzes call content to identify robocall campaigns and other malicious activities without recording audio, ensuring data privacy and security.

Automatically flags suspicious traffic based on content analysis.

3. Alert System:

The system triggers alerts if any set parameters for spam or scam traffic are breached.

Upon alert, the system informs the management and prompts whether to issue a warning to the customer.

B) Manual Checks:

1. KYC Verification Updates:

Periodic reviews of KYC information using platforms like Stripe to ensure ongoing compliance with regulatory requirements.

2. Triggered Reviews:

If automatic systems flag a customer for suspicious or malicious activities, manual intervention is initiated.

Customers flagged for running malicious or undisclosed traffic must consent to having their calls recorded and audio analyzed for fraud detection.

Manual review of documented evidence and customer activities to confirm fraud or regulatory breaches.

C) Automated Actions Upon Breach:

If a customer breaches any of the spam or scam parameters, the system can take the following automated actions:

i. Suspending Traffic: Traffic can be suspended for a specific duration.

ii. Suspending Account: The customer's account can be suspended for a specific duration.

iii. Issuing Show Cause/Investigation Notice: A show cause or investigation notice can be issued to the customer.

iv. Issuing a Warning: A warning can be issued to the customer.

D) Trigger Points for Further Monitoring:

1. Suspicious Activity Detection: Triggered when the real-time call transcription analysis identifies potential robocall campaigns or other malicious activities.
2. Customer Non-Compliance: Initiated when customers fail to adhere to telecom safety, security obligations, or fair usage policies.
3. Regulatory Updates: Triggered by changes in regulatory requirements, necessitating review and update of customer compliance status.

Also We uses internal software to monitor outbound voice traffic in real time, preventing the origination of illegal robocalls for the small portion of voice traffic that does not originate from its wholesale voice service provider clients with STIR/SHAKEN. The software provides detailed reporting, identifying suspected illegal robocalls and alerts us if we originate any calls where the calling number appears invalid, unallocated, on a Do Not Originate list, in the FCC consumer complaint database or maintains a poor reputation. We will immediately investigate identified calls to determine whether the caller seeks to originate unlawful robocalls. If we determines the calls include attempts to originate unlawful robocalls, then we either warn them to stop, block the calling and/or terminate their service as consistent with industry standard operating procedures.

We respond to all traceback requests from the Commission, law enforcement, and the registered traceback consortium, as well as cooperates with such entities in investigating and stopping any illegal Robocallers that use voice services to originate illegal calls. We will investigate all traceback requests within 48 hours and provide all the information available for the requested call. We also have the plans to integrate with the ITG to speed up the traceback requests.

Should you require any further information or assistance, please do not hesitate to contact us at admin@vortexcalls.com

We remain committed to working together with regulatory bodies and law enforcement agencies to uphold the integrity of telecommunications networks and protect consumers from fraudulent activities.