

Robocall Mitigation Program

Version date: March 6, 2026

Filer legal name	CYBERVOICE INC
FCC Registration Number (FRN)	0035142454
Primary compliance contact	S Feder 845 7830046 #120 info@positive.tech
RMD certification path	Voice Service Provider Filing; Option 3 – No STIR/SHAKEN Implementation

1. Purpose

This Robocall Mitigation Program describes the specific reasonable steps the filer takes to avoid originating illegal robocall traffic and its commitment to respond fully and within 24 hours to traceback requests from the Federal Communications Commission, law enforcement, and the registered industry traceback consortium.

This program is intended to support a Voice Service Provider filing in the FCC Robocall Mitigation Database under 47 CFR § 64.6305.

2. Service Model and Certification Basis

The filer offers voice service to end-user customers as a white-label reseller using the hosted SkySwitch / 2600Hz platform.

The filer does not control the underlying network infrastructure necessary to implement STIR/SHAKEN on its own network infrastructure and therefore files under Option 3 – No STIR/SHAKEN Implementation.

Certification basis: 47 CFR § 64.6305(d)(2)(i) – inability to implement STIR/SHAKEN due to lack of control over the network infrastructure necessary to implement STIR/SHAKEN.

3. Customer Acceptance and Know-Your-Customer Controls

Before activating service, the filer collects and reviews basic customer identity and business information reasonably sufficient for the type of customer being onboarded. This may include the customer's legal name, contact information, service address, business website, tax or formation information if applicable, and a description of the intended use of service.

The filer does not knowingly provide service for unlawful robocalling, spoofing, lead-generation abuse, traffic pumping, impersonation scams, or any use case that appears deceptive, abusive, or inconsistent with the customer's stated business purpose.

High-risk or unusual applicants may be asked for additional information before activation, including explanation of calling campaigns, sample scripts, proof of consent practices, or other information reasonably necessary to assess robocall risk.

Service may be declined if the filer cannot reasonably verify the customer or if the proposed use presents unacceptable robocall or spoofing risk.

4. Contractual and Policy Controls

The filer's service terms prohibit unlawful robocalls, unlawful spoofing, deceptive caller ID practices, and any traffic that violates applicable law, including the Telephone Consumer Protection Act and FCC rules.

Customers are required to use the service only for lawful communications and to cooperate with any inquiry into suspicious traffic, traceback request, complaint, or regulatory investigation.

The filer reserves the right to block, suspend, restrict, or terminate service immediately when there is evidence of unlawful robocalling, spoofing, failure to respond to an inquiry, or other misuse of service.

5. Traffic Review and Monitoring

The filer reviews account activity, complaints, traceback notices, and other available information for signs of suspicious outbound calling behavior.

Where available through internal records and platform or carrier tools, the filer reviews calling patterns that may indicate elevated robocall risk, including sudden volume spikes, unusual calling windows, short-duration high-volume campaigns, repeated calls to large numbers of destinations, invalid number usage, and mismatch between stated use and actual traffic profile.

The filer does not rely on a single indicator. Instead, the filer evaluates the totality of the information available and escalates accounts for review when suspicious patterns, complaints, or traceback notices are received.

6. Response to Complaints and Traceback Requests

The filer commits to respond fully and within 24 hours to all traceback requests from the FCC, law enforcement, and the registered industry traceback consortium.

Upon receipt of a traceback request or credible complaint, the filer will promptly review the relevant account, call detail records available to it, customer information, and any related platform or carrier information reasonably available to it.

The filer will cooperate with the FCC, law enforcement, and the industry traceback consortium in investigating and stopping illegal robocallers that use its service to originate calls.

7. Mitigation and Enforcement Actions

Depending on the facts, the filer may require additional customer documentation, place temporary restrictions on outbound traffic, block specific campaigns or numbers, suspend service, terminate service, or coordinate with the underlying platform or carrier to stop suspected unlawful traffic.

If the filer determines that a customer is engaged in illegal robocalling, unlawful spoofing, or other abusive activity, service will be blocked, suspended, or terminated as appropriate.

8. Recordkeeping

The filer maintains records reasonably necessary to support this mitigation program, including customer onboarding information, complaints received, traceback correspondence, and actions taken in response to suspicious traffic or misuse, subject to normal business record retention practices.

9. Review and Updates

This program will be reviewed and updated when there is a material change in the filer's service model, platform control, regulatory obligations, or mitigation procedures.

If the filer later obtains direct control of network infrastructure necessary to implement STIR/SHAKEN, or obtains its own SPC token and STI certificate, the filer will reassess its RMD certification and update the filing as required.

10. Company Certification Statement

The filer states that all calls it originates on its network are subject to this robocall mitigation program, that it takes reasonable steps to avoid originating illegal robocall traffic, and that it will respond fully and within 24 hours to all traceback requests from the FCC, law enforcement, and the registered industry traceback consortium, and will cooperate with such entities in investigating and stopping illegal robocallers that use its service to originate calls.

11. Quick Pre-Upload Checklist

- Replace all bracketed placeholders on page 1.
- Confirm the legal entity name exactly matches CORES.
- Confirm the FRN is a business-type FRN.
- Confirm the filer does not have its own SPC token or STI certificate before using Option 3.
- Save this document as the PDF uploaded with the RMD filing.

This document is a practical draft and should be reviewed by the filer for factual accuracy before submission.