

Robocall Mitigation Program

1. Provider Identification and Scope

This Robocall Mitigation Program is submitted by the filer in connection with its registration in the FCC Robocall Mitigation Database pursuant to 47 CFR § 64.6305.

The filer is a **Voice Service Provider** that offers interconnected voice services to end-user business customers as a **whitebox reseller** of hosted voice and UCaaS services provided by an underlying, facilities-based provider (CoreDial LLC). The filer does not own, operate, or control the network infrastructure used to originate, transit, or terminate voice calls on the public switched telephone network (PSTN).

The filer does **not** implement STIR/SHAKEN and does not have the technical capability to authenticate or verify calls, as all network-level call processing and signaling functions are performed by the underlying provider and its upstream carriers.

2. STIR/SHAKEN Status

The filer has **no STIR/SHAKEN implementation**.

Pursuant to 47 CFR § 64.6301(a), the obligation to implement STIR/SHAKEN applies to voice service providers that originate, transit, or terminate SIP-based calls on IP networks they control and that are capable of performing call authentication and verification. The filer does not meet this threshold, as it does not operate SIP infrastructure, hold STI certificates, or control call attestation.

STIR/SHAKEN authentication and verification for calls associated with the filer's customers are implemented by the underlying facilities-based provider (CoreDial LLC) and its upstream carriers.

Accordingly, the filer complies with FCC robocall rules by maintaining this Robocall Mitigation Program.

3. Reasonable Steps to Prevent and Mitigate Illegal Robocalls

The filer takes reasonable and appropriate steps to prevent, detect, and mitigate the origination of illegal robocall traffic by its customers, including but not limited to the following measures:

a. Customer Vetting and Onboarding

- Verification of customer identity and business legitimacy prior to service activation
- Collection and validation of customer contact information
- Review of intended use cases for voice services
- Prohibition of robocalling, spoofing, and illegal telemarketing in customer agreements

b. Acceptable Use and Contractual Controls

- Enforcement of Acceptable Use Policies (AUPs) that expressly prohibit illegal robocalls, spoofing, and fraudulent activity
- Contractual rights to suspend or terminate service for violations
- Customer acknowledgment of compliance with applicable federal and state robocall and telemarketing laws

c. Traffic Monitoring and Abuse Detection

- Reliance on traffic monitoring, analytics, and fraud detection tools provided by the underlying provider
- Review of alerts, complaints, and anomaly indicators related to call volume, patterns, or destinations
- Investigation of suspicious or excessive calling behavior

d. Complaint Handling

- Maintenance of procedures to receive and review complaints from consumers, carriers, regulators, and industry traceback groups
- Prompt investigation of complaints associated with the filer's customers
- Escalation to the underlying provider when network-level analysis is required

4. Response to Illegal or Suspicious Traffic

When illegal or suspected robocall activity is identified, the filer takes appropriate corrective action, which may include:

- Immediate investigation of the associated customer account
- Customer notification and request for explanation or remediation
- Temporary suspension or permanent termination of service

- Coordination with the underlying provider to block or mitigate traffic
 - Preservation of relevant records related to the investigation
-

5. Traceback Cooperation

The filer commits to full cooperation with industry traceback efforts, including those conducted by the Industry Traceback Group (ITG) and USTelecom.

Traceback requests can be submitted to Jon Tice - sales@nepabiztech.com

Specifically, the filer:

- Responds promptly to traceback requests
 - Provides customer and call-related information within its possession or control
 - Coordinates with the underlying provider to obtain network-level details when required
 - Takes corrective action based on traceback findings
-

6. Ongoing Compliance and Program Maintenance

The filer reviews and updates this Robocall Mitigation Program as necessary to address changes in FCC rules, industry best practices, and operational experience.

Employees responsible for customer onboarding, support, and compliance are trained to identify potential robocall risks and to escalate issues appropriately.

The filer maintains records related to complaints, investigations, enforcement actions, and traceback responses for a reasonable period consistent with regulatory expectations.

7. Certification

The filer certifies that this Robocall Mitigation Program is implemented in good faith and reflects reasonable steps to prevent, identify, and mitigate illegal robocall traffic in compliance with 47 CFR § 64.6305.

This program is submitted in support of the filer's Robocall Mitigation Database filing and is made available to the FCC and to downstream and upstream providers upon request.