Robocall Mitigation Program Description

FCC Compliance Document for Non-Facilities-Based Voice Resellers & PBX Providers

Document Purpose:	Robocall Mitigation Database (RMD) Compliance Filing
Provider Operating Model:	Non-Facilities-Based Reseller of PBX and Cloud Voice Services
Compliance Framework:	47 CFR § 64.6305(a) & FCC TRACED Act Mandates

1. Executive Summary & Overview

This Robocall Mitigation Program Description is maintained and enforced to satisfy the requirements established by the Federal Communications Commission (FCC) under 47 CFR § 64.6305. As a non-facilities-based reseller of cloud PBX, unified communications, and business voice services, the company does not directly own or operate core underlying voice switching fabric, local routing switches, or direct-access numbering blocks capable of generating cryptographic STIR/SHAKEN digital certificates (SPC tokens).

Instead, all call origination, network transport, and STIR/SHAKEN digital signature attestation (Level A/B/C) are executed directly by our upstream facilities-based carrier partners and underlying network providers. Nevertheless, we maintain a robust, rigorous robocall mitigation program designed to prevent illegal robocalls, verify customer identity, monitor traffic patterns, and cooperate fully with law enforcement and industry traceback bodies.

> Core Commitment: The company maintains a zero-tolerance policy for illegal robocalling, caller ID spoofing, and malicious traffic origination across its customer base.

2. Upstream Network Architecture & STIR/SHAKEN Integration

Because our service operates at the application/PBX layer:

- **Upstream Attestation:** All outbound voice traffic originating from our platform customers is handed off to fully certified, facilities-based upstream carriers that possess direct OCNs and implement full STIR/SHAKEN signing protocols.
- **Exemption Clarification:** While we do not directly implement STIR/SHAKEN signing software on local switches (as we do not own underlying network switches), our operations are fully harmonized with the upstream carrier's cryptographic validation and attestation pipelines.

3. Customer Onboarding & Know-Your-Customer (KYC) Policies

Preventing illegal robocalls begins at the point of customer acquisition. We enforce strict vetting procedures before provisioning any voice service, SIP trunk, or PBX seat:

- **Identity Verification:** We collect and verify legal business names, corporate registration details, physical operating addresses, and authorized point-of-contact information for all commercial subscribers.
- **Legitimate Use Attestation:** Customers must certify during onboarding that their calling campaigns comply with all applicable federal and state telemarketing laws, including the Telephone Consumer Protection Act (TCPA) and TSR guidelines.
- **Prohibited Use Agreements:** Service agreements explicitly prohibit unverified caller ID spoofing, autodialed debt collection campaigns without express consent, illegal robocalling, and fraudulent telemarketing.

4. Traffic Monitoring & Mitigation Procedures

We continuously monitor call traffic characteristics and customer usage patterns to detect anomalous spikes or suspicious behavior:

- **Immediate Suspension:** If an account is identified as originating illegal traffic, high-volume spam, or unauthorized spoofed Caller ID, access to outbound calling is suspended immediately pending investigation.
- **Permanent Termination:** Confirmed bad actors or fraudulent users are permanently terminated, and details are logged for potential regulatory or law enforcement reporting.

5. Traceback Cooperation & 24-Hour Incident Response

In compliance with FCC regulations and industry standards, we maintain a dedicated mechanism for receiving and responding to traceback requests:

- **24-Hour Commitment:** We commit to fully investigating and responding to all official traceback requests within 24 hours of receipt.
- **Cooperation with Investigations:** Upon identifying the source of traced illegal traffic, we provide complete customer onboarding logs, call detail records (CDRs), and upstream routing details to assist investigators in halting illegal robocall operations.

Certification & Acknowledgment:

The undersigned certifies that the statements contained herein are true, complete, and correct, and that the company maintains an active robocall mitigation program consistent with 47 CFR § 64.6305.