

ZIVA TELECOM

ROBOCALL MITIGATION PLAN

1. PRINCIPLE OBJECTIVE & SCOPE

ZIVA TELECOM maintains a strict zero-tolerance policy against the transmission of illegal robocalls, deceptive caller identification (spoofing), and telemarketing traffic that violates federal mandates.

1.1 Operational Role Framework

ZIVA TELECOM primarily operates as a Wholesale Voice Provider and Intermediate Carrier. Any end-user services are provided only through approved business relationships and remain subject to all applicable TCPA, DNC, and consent requirements. Because our network handles diverse traffic routing paths, these mitigation protocols are enforced globally across all network layers. Every packet transiting our switches must comply with the Telephone Consumer Protection Act (TCPA), national Do-Not-Call (DNC) regulations, and active opt-in consent verification standards.

1.2 Upstream Carrier Restrictions

ZIVA TELECOM categorically rejects traffic interconnections from any service provider, gateway, or international carrier that does not maintain an active, compliant registration within the Federal Communications Commission (FCC) Robocall Mitigation Database (RMD).

2. CALL AUTHENTICATION FRAMEWORK (STIR/SHAKEN)

2.1 Full Implementation Statement

ZIVA TELECOM certifies Complete STIR/SHAKEN Implementation across its entire switching infrastructure. This architecture relies on zero technical exemptions, conditional routing, or feasibility modifications. ZIVA TELECOM maintains active SPC tokens and STIR/SHAKEN certificates through authorized industry governance and certificate authorities and performs periodic certificate lifecycle reviews

2.2 Token Attestation Level Criteria Attestation levels are automatically assigned based on our direct validation of the caller's identity and number assignment:

- **Level A (Full Attestation):** Executed when ZIVA TELECOM has directly provisioned and allocated the telephone number block to a customer whose business legitimacy has passed our comprehensive vetting process.
- **Level B (Partial Attestation):** Executed when a client has passed complete background screening and provides verified digital or documentary proof establishing their explicit right-of-use or ownership of the specific outbound Caller ID.
- **Transit & Gateway Scrutiny:** ZIVA TELECOM does not generate Level C attestations. Any inbound intermediate traffic carrying a Level C signature from an upstream provider is isolated by our signaling layer, subjected to enhanced deep-packet analysis, and restricted or dropped if it exhibits suspicious origin profiles.

2.3 Unsigned Traffic Policy

Traffic received without valid STIR/SHAKEN authentication is subject to enhanced compliance review, fraud scoring, traceback analysis, and route-level monitoring. High-

risk unsigned traffic may be blocked, rejected, restricted, or suspended pending investigation.

3. SUBSCRIBER IDENTIFICATION & VERIFICATION (KYC)

No customer accounts or SIP trunks are provisioned without completing our mandatory corporate onboarding sequence. Prospective clients must submit verifiable business documentation, which is manually audited against federal databases to confirm current compliance:

- Legal Formation & Accountability: Verification of state-level corporate registry files and active Federal Employer Identification Numbers (EIN).
- Federal Registry Validation: Verification of the applicant's FCC Registration Number (FRN) and active status in the FCC Form 499 Filer Database (confirming updates for the current annual filing cycle).
- Location Verification: Mandatory submission of physical operational address documents (such as utility bills or commercial property leases).
- Industry Vetting: Requirements for verifiable, active U.S.-based Tier-1 or Tier-2 telecommunications carrier references to substantiate operational standing.
- Policy Review: Mandatory technical audit of the applicant's internal robocall prevention practices to ensure they mirror FCC guidelines.

4. NETWORK ANALYTICS & TRAFFIC SCREENING

4.1 Real-Time Telemetry Tracking Our Network Operations Center (NOC) runs continuous heuristic analysis on live call streams. Automated alarms and programmatic traffic throttling are triggered based on deviations from standard commercial benchmarks:

- Connection Efficiency: Monitoring Answer Seizure Ratios (ASR) for unnatural drops that signal automated scanning.
- Conversational Metrics: Tracking Average Call Duration (ACD) to flag conversational length distributions indicative of automated dialers.
- Volumetric Spikes: Immediate isolation of sudden, sub-second bursts of high-volume outbound dial attempts.
- Source Validation: Real-time checking of signaling data to capture unallocated prefixes, invalid numbering formats, or restricted inbound identifiers.

4.2 Automated Mitigation Integrations The signaling architecture incorporates real-time database queries to drop unvetted traffic at the border:

- DNO Registries: Integration with industry Do-Not-Originate databases to block calls spoofing inbound-only numbers.

- Reputation Blacklists: Continuous, automated logic feeds that block traffic coming from known malicious Media IPs and suspicious Originating Company Numbers (OCNs).

5. REPEATED VIOLATIONS & ENFORCEMENT ESCALATION

ZIVA TELECOM operates a strict Three-Stage Enforcement Protocol for any customer network originating traffic that generates validated industry complaints or official federal traceback inquiries:

STAGE 1: FORMAL NOTICE & AUDIT] Urgent compliance alert issued. Client must isolate the offending traffic source and deliver a written remediation plan within 24 hours.

STAGE 2: ADMINISTRATIVE SUSPENSION] Triggered by a second infraction. Trunks are administratively disabled pending a manual audit of the client's onboarding controls.

STAGE 3: PERMANENT TERMINATION] Triggered by a third infraction. Immediate cancellation of all Master Service Agreements and permanent blacklisting from the network.

6. INDUSTRY COOPERATION & TRACEBACK SERVICE LEVEL AGREEMENTS

ZIVA TELECOM is dedicated to maintaining clean, transparent traffic lanes across the public switched telephone network (PSTN).

- 24-Hour Resolution Guarantee: ZIVA TELECOM guarantees a complete, conclusive response to all official data inquiries from the Industry Traceback Group (ITG) and law enforcement within 24 hours of the initial request.
- Upstream Tracing: Compliance personnel are equipped to immediately pull upstream Call Detail Records (CDRs) and trace signaling logs back to the exact point of network entry.
- Regulatory Transparency: Fully detailed tracing data, identity documents, and call records are securely formatted and delivered to regulatory bodies upon receipt of a lawful order.

7. INFORMATION MANAGEMENT & RECORD RETENTION

To comply with 47 CFR § 64.6305, ZIVA TELECOM securely stores all operational metadata, verification histories, and system logs for a mandatory minimum period of two (2) years.

Retained materials include:

- Complete Call Detail Records (CDRs) and SIP signaling properties.
- Cryptographic token logs and STIR/SHAKEN attestation assignments.
- Incoming industry traceback requests alongside our submitted compliance evidence.
- Customer onboarding files, including corporate EIN, FRN, and Form 499 verification certificates.
- False-positive connection reports and associated technical resolution logs.

8. CORPORATE IDENTITY & CONTACT TRANSPARENCY

ZIVA TELECOM maintains absolute public transparency regarding its corporate operations, compliance points of contact, and physical presence.

8.1 Registry Profile Details

- Corporate Entity Name: ZIVA TELECOM
- Official Headquarters: 7901 4TH ST N STE 300, ST PETERSBURG, FL 33702
- Tax Identification Number: EIN 33-3304553
- Commission Registration: FRN 0036662740
- Telecommunications Filer Identification: FCC Form 499 Filer ID 837419 (Maintained with fully updated, active status for the current 2026 filing period)