

Robocall Mitigation Policy

For FCC Robocall Mitigation Database (RMD) – 2026 Filing

1. Company Information

Legal Name: Coztel LLC

FCC Registration Number (FRN): 0030114557

Operating Company Number (OCN): 074K

Service Type:

- Voice Service Provider
- Non-gateway Intermediate Provider

Services Offered:

The Company provides interconnected and/or non-interconnected VoIP services and also transmits voice traffic between originating and terminating providers.

2. Purpose and Regulatory Authority

This Robocall Mitigation Policy is established in accordance with the rules and orders of the **Federal Communications Commission**, including but not limited to:

- 47 CFR §64.6305
- The TRACED Act
- FCC Orders relating to STIR/SHAKEN and the Robocall Mitigation Database

The purpose of this policy is to prevent, detect, mitigate, and remediate illegal, unwanted, and fraudulent robocalls transmitted through the Company's network.

3. STIR/SHAKEN Implementation Status

The Company certifies that it has **fully implemented STIR/SHAKEN authentication** across its IP network, consistent with FCC requirements.

Key Elements:

- Authentication of originating calls using SIP Identity headers
- Verification of incoming calls where technically feasible

- Assignment and verification of attestation levels (A, B, or C)
- Secure management of digital certificates via an approved STI-CA

STIR/SHAKEN authentication is applied to all SIP-based traffic under the Company's control unless a documented technical exception applies.

4. Role as a Voice Service Provider

As a Voice Service Provider, the Company takes reasonable and effective steps to ensure that its customers do not originate illegal robocalls.

Measures Include:

- Know-Your-Customer (KYC) and customer due diligence at onboarding
 - Verification of customer identity, business purpose, and traffic profile
 - Contractual prohibitions against illegal robocalls and spoofing
 - Ongoing monitoring of customer-originated traffic
-

5. Role as an Intermediate Provider

As an Intermediate Provider, the Company implements robust practices to avoid carrying or facilitating illegal robocall traffic.

Measures Include:

- Monitoring of transit traffic for abnormal calling patterns
 - Identification of high-risk signaling and call behavior
 - Cooperation with upstream and downstream providers
 - Rapid response to traceback requests and enforcement inquiries
-

6. Coztel's Acceptable Use Policy (AUP)

As part of its customer-onboarding process, Coztel's customers will contractually agree to various terms and conditions, including a commitment to comply with Coztel's Acceptable Use Policy (AUP). Among other things, this AUP will prohibit:

- Using the Services to engage in any activities that are illegal, abusive, false,

fraudulent, deceptive or misleading, or any activity that exploits, harms, or threatens to harm children.

- Engaging in any unsolicited advertising, marketing, or other unlawful activities using the Services, including, without limitation, any activities that violate laws applicable to advertising, electronic communications, and telemarketing, including, but not limited to, Section 5 of the FTC Act (15 U.S.C. § 45), the CAN-SPAM Act (15 U.S.C. §§ 7701-7713), the Telemarketing Consumer Fraud and Abuse Prevention Act (15 U.S.C. §§ 6101-6108), the Federal Trade Commission Telemarketing Sales Rule (16 C.F.R. § 310 et seq.), the Telephone Consumer Protection Act (47 U.S.C. §§ 227), the Federal Communications Commission regulations (47 C.F.R. 64.1200 et seq.) and orders implementing the Telephone Consumer Protection Act, and all federal and state Do Not Call and calling-time restriction laws and regulations.
- Using Coztel's Services in any way that fails to conform to any applicable industry guidelines and standards, including, without limitation, the CTIA Messaging Principles and Best Practices, Short Code Registry Best Practices, and Short Code Monitoring Handbook.
- Creating a false identity, forged email address or header, phone number, or otherwise attempting to mislead others as to the identity of the sender or the origin of a message or phone call, including failing to comply with the Truth in Caller ID Act.

Coztel's contracts with its customers will stipulate that Coztel is authorized to suspend and/or terminate all Services in the event of an AUP violation.

7. Robocall Detection and Monitoring

The Company employs a layered approach to detect and identify suspicious or unlawful traffic, including:

- Real-time traffic analytics
- Call volume, velocity, and duration monitoring
- Invalid, unallocated, or unassigned number detection
- Review of attestation inconsistencies
- Analytics-based alerts for potential robocall campaigns

Monitoring is conducted continuously and is proportional to traffic volume and risk profile.

8. Mitigation and Enforcement Actions

When suspected illegal robocall activity is identified, the Company may take one or more of the following actions:

- Immediate investigation of the traffic source
- Temporary suspension or permanent termination of service
- Blocking of specific calling numbers, prefixes, or customers
- Notification to upstream or downstream providers
- Cooperation with the FCC, law enforcement, or industry traceback groups

Mitigation actions are documented and retained in accordance with internal compliance procedures.

9. Traceback Cooperation

The Company fully cooperates with authorized traceback efforts, including but not limited to those initiated by:

- The FCC
- Industry-led traceback organizations
- Law enforcement agencies

The Company responds to traceback requests in a timely manner and provides all relevant call detail records and network information as legally permissible.

10. Recordkeeping and Documentation

The Company maintains records demonstrating compliance with this Robocall Mitigation Policy, including:

- STIR/SHAKEN implementation status
- Traffic monitoring and mitigation actions
- Customer onboarding and compliance reviews

- Traceback responses

Records are retained for a minimum period consistent with FCC rules and applicable law.

11. Annual Certification and Updates

The Company certifies that:

- This Robocall Mitigation Policy is accurate and in effect
- The Company complies with all applicable FCC robocall mitigation rules
- The information submitted to the FCC Robocall Mitigation Database is truthful and complete

The Company will **review, recertify, and update** this policy annually by **March 1**, or sooner if required by FCC rule changes.

12. Responsible Officer

Designated Compliance Officer:

Name: Atif Shahbaz

Title: CFO

Email: atif@coztel.com

Phone: 571-462-1190

The undersigned officer certifies under penalty of perjury that the Company is in compliance with FCC robocall mitigation requirements.

Certification Statement

"I certify that the foregoing Robocall Mitigation Policy is true and correct, and that Coztel LLC has implemented the practices described herein in compliance with FCC rules."

Authorized Signatory:

Name: Atif Shahbaz

Title: CFO

Date: 2/27/2026