

ROBOCALL MITIGATION PLAN (RMP)

TELQUIX

1. Company Identification

Legal Name: TELQUIX

Headquarters Address: 367 Berry St, Suite 104, Woodbridge, NJ 07095, USA

Business Type: Telecommunications / VoIP Service Provider

Service Model: Non-facilities-based provider (Reseller / SIP Trunking / Wholesale VoIP)

2. Purpose of this Robocall Mitigation Plan

This Robocall Mitigation Plan (“RMP”) is adopted in accordance with:

- **47 CFR § 64.6305** (Robocall Mitigation Database Requirements)
- **47 CFR § 64.1200** (TCPA regulations)
- **47 CFR § 64.6301–64.6306** (STIR/SHAKEN implementation framework)
- The **Pallone-Thune TRACED Act**
- FCC Report and Order FCC 20-136 and subsequent amendments

TELQUIX certifies that it has implemented a robocall mitigation program designed to prevent the origination and transmission of illegal robocalls and to comply with all FCC mandates.

3. STIR/SHAKEN Implementation

TELQUIX complies with the FCC’s STIR/SHAKEN framework requirements.

3.1 Authentication Framework

- TELQUIX utilizes STIR/SHAKEN authentication for IP-based voice traffic where technically feasible.
- TELQUIX works with upstream carriers and third-party authentication providers to ensure:
 - Caller ID authentication
 - Proper attestation levels (A, B, C)
 - Verification of inbound calls

3.2 Outbound Attestation Policy

TELQUIX assigns attestation levels based on:

- Verified customer identity
- KYC documentation review
- Business registration validation
- Traffic pattern analysis
- Contractual agreements prohibiting illegal robocalling

Full A-level attestation is only granted when TELQUIX:

- Has direct relationship with the customer, AND
- Has verified identity and right to use the calling number.

4. Robocall Mitigation Program (For Non-IP or Where STIR/SHAKEN Is Not Fully Applicable)

TELQUIX maintains a comprehensive mitigation program including:

4.1 Customer Vetting (KYC / KYB)

Before service activation:

- Government-issued identification
- Articles of Incorporation / Business Registration
- EIN verification (for US entities)
- Proof of address
- Beneficial ownership disclosure
- Detailed use-case description
- Traffic projection and call routing disclosure

High-risk verticals (lead generation, debt collection, telemarketing, political campaigns, healthcare marketing) undergo enhanced due diligence.

4.2 Contractual Controls

All customers must agree to:

- Strict prohibition of illegal robocalls
 - Compliance with TCPA
 - Compliance with TSR (Telemarketing Sales Rule)
 - Compliance with Do-Not-Call regulations
 - Indemnification clauses
 - Immediate suspension rights for violations
-

4.3 Traffic Monitoring & Analytics

TELQUIX actively monitors traffic using:

- Real-time call analytics
- Volume anomaly detection
- Short duration call ratio analysis
- High ASR/ACD irregularities
- Invalid / unallocated number detection
- Neighbor spoofing detection
- Reassigned number database monitoring
- DNO (Do-Not-Originate) list screening

Suspicious traffic triggers:

- Immediate investigation
- Temporary suspension
- Formal compliance review

4.4 Do-Not-Originate (DNO) & Known Illegal Numbers

TELQUIX blocks:

- FCC-designated DNO numbers
 - Government numbers used for spoofing
 - Invalid NANP numbers
 - Unallocated numbering resources
-

4.5 Traceback Cooperation (24-Hour Commitment)

TELQUIX maintains a strict internal policy:

- All traceback requests are acknowledged immediately.
- Full investigation is initiated upon receipt.
- Responses are provided within **24 hours** without exception.
- Supporting call detail records (CDRs) are preserved and supplied as required.

Failure to comply internally results in compliance escalation.

5. Record Retention Policy

TELQUIX retains:

- Customer onboarding documentation
- KYC records
- Call Detail Records (CDRs)
- Traffic monitoring logs
- Traceback responses

Retention period: **Minimum 24 months** or longer if legally required.

6. Know Your Upstream Providers

TELQUIX:

- Engages only with compliant upstream carriers
- Verifies upstream FCC RMD registration

- Ensures contractual robocall mitigation obligations
 - Monitors upstream routing integrity
-

7. Enforcement & Escalation Procedures

Upon detection of suspected illegal robocall activity:

1. Immediate traffic suspension
2. Formal compliance notification to customer
3. Internal compliance investigation
4. Mandatory documentation review
5. Permanent termination for confirmed violations
6. Reporting to appropriate authorities if required

Zero tolerance policy applies.

8. Certification Statement

TELQUIX hereby certifies that:

- It has implemented a robocall mitigation program compliant with **47 CFR § 64.6305**.
- It has implemented STIR/SHAKEN in accordance with FCC requirements.
- It actively mitigates illegal robocalls.
- It responds to traceback requests within 24 hours.
- It will update this plan as FCC regulations evolve.