

Robocall Mitigation Program Description

Megatel Netcom Corporation (MVNO)

1. Corporate Structure, Control Persons, and Affiliations

Megatel Netcom Corporation (“Megatel”) provides the following disclosures in compliance with 47 C.F.R. § 64.6305 and FCC guidance under the Sixth Caller ID Authentication Report and Order (FCC 23-18):

FCC Registration Number (FRN): 0018641639

Operating Company Number (OCN): 277M

Provider Type: Voice Service Provider & MVNO Provider

Control Person / Officers

- Peter Liu – Chief Financial Officer (CFO)
 - Serves as the primary control person responsible for corporate oversight, including compliance with FCC robocall mitigation requirements.

Controlling Entity

- Megatel Netcom Corporation is not owned or controlled by any parent entity.

Affiliates, Subsidiaries, and Parent Companies

- Affiliates: Eton InfoComm Technology, Eton International Inc
- Subsidiaries: Megatel Netcom (Canada) Corporation
- Parent Company: None

Megatel has implemented STIR/SHAKEN for calls originated on its network using an STI certificate issued through an authorized Certification Authority. Megatel authenticates outbound calls in accordance with applicable FCC rules and industry standards; maintains internal governance procedures to ensure that any future changes in ownership, control, or affiliations will be:

- Evaluated for robocall compliance risk, and
- Promptly updated in the FCC Robocall Mitigation Database filing as required.

2. Know Your Customer (KYC) and Customer Onboarding Controls (Enhanced Disclosure)

Megatel acknowledges that robocall risk is most effectively mitigated through robust onboarding controls and continuous customer oversight. Accordingly, Megatel has implemented a risk-based KYC framework designed to prevent bad actors from accessing its network.

2.1 Identity Verification Prior to Onboarding

Before activating any customer account, Megatel performs verification procedures including:

- Collection and validation of:
 - Legal business name and registration documents
 - Employer Identification Number (EIN).
 - Physical business address verification (no P.O. box-only onboarding)
- Identification of:
 - Authorized account representatives
- Cross-checking against:
 - Public business registries
 - Sanctions or enforcement lists where applicable

2.2 Use Case and Traffic Risk Assessment

Megatel evaluates each prospective customer's intended use of service, including:

- Nature of business (e.g., retail wireless, VoIP application, A2P messaging, outbound dialing)
- Evaluate expected call volumes, destinations, and call patterns.
- Whether the customer intends to originate high-volume outbound traffic

Customers presenting elevated risk profiles (e.g., telemarketing or lead generation) are subject to enhanced due diligence prior to approval.

2.3 Contractual Safeguards

All customers are required to enter into agreements that explicitly:

- Prohibit the origination or transmission of illegal robocalls
- Require compliance with:
 - FCC robocall mitigation rules
 - Caller ID authentication requirements
- Grant Megatel the right to:
 - Monitor traffic
 - Suspend or terminate service for violations
 - Share information with regulators or trace back entities

2.4 Post-Onboarding Monitoring

Megatel does not rely solely on onboarding controls. All customers are subject to:

- Ongoing traffic monitoring
- Behavioral analysis comparing actual traffic against expected profiles
- Immediate investigation of anomalies

Accounts exhibiting suspicious activity may be:

- Temporarily suspended
- Subject to further verification
- Permanently terminated if violations are confirmed

3. Know Upstream Provider (Carrier) Due Diligence and Oversight

Megatel recognizes that robocall compliance obligations extend to traffic received from upstream providers and has implemented controls to ensure responsible sourcing of traffic.

3.1 Upstream Provider Due Diligence

Prior to establishing relationships with upstream carriers or vendors, Megatel conducts:

- Verification of:
 - Inclusion in the FCC Robocall Mitigation Database
- Confirmation that the provider:
 - Maintains a documented mitigation program
- Review of:
 - Industry reputation
 - Known enforcement actions or compliance issues

3.2 STIR/SHAKEN and Authentication Requirements

Megatel requires upstream providers to:

- Participate in STIR/SHAKEN where technically feasible
- Provide properly authenticated traffic, including:
 - Valid attestation levels
 - Verifiable caller ID information

Traffic received without appropriate authentication is subject to:

- Enhanced monitoring.
- Potential blocking or rejection actions, including blacklist by number, prefix, IP, SPID, and user agent; conducting Do-Not-Originate enforcement and CDR-based anomaly detection, CAPTCHA/IVR gating or blocking for flagged calls if applicable.

3.3 Contractual Controls with Upstream Providers

Megatel's agreements with upstream providers include provisions that:

- Require compliance with FCC robocall mitigation obligations
- Prohibit transmission of illegal robocalls
- Require cooperation with:
 - Traceback requests
 - Regulatory inquiries
- Permit Megatel to:
 - Block or reject non-compliant traffic
 - Terminate relationships for compliance failures

3.4 Ongoing Monitoring of Upstream Traffic

Megatel continuously monitors inbound traffic from upstream providers using:

- CDR-based analytics
- Volume and pattern analysis

Providers associated with suspicious traffic patterns are subject to:

- Immediate investigation
- Escalation and remediation
- Traffic blocking or termination if necessary

4. Documentation

Megatel maintains comprehensive documentation to support its compliance posture, including:

- Customer onboarding records (KYC files)
- Upstream provider due diligence documentation
- Contracts with compliance clauses
- Traffic monitoring logs and investigation records
- Decisions related to blocking, suspension, or termination

Megatel recognizes that FCC compliance requires not only implementation of controls but also the ability to demonstrate those controls through verifiable records.

5. Analytics Systems and Third-party Vendors

Megatel uses in-house analytics to monitor call patterns, volumes, durations, and signaling anomalies. Currently, no third-party analytics vendors are used. If adopted, their names will be disclosed in future filings.

6. Commitment

Megatel affirms its commitment to maintaining a robust, risk-based, and continuously improving robocall mitigation program consistent with FCC expectations. Megatel has implemented STIR/SHAKEN using a certificate issued by an FCC-recognized Certification Authority. The certificate is maintained and renewed in accordance with industry requirements.