



IXICA COMMUNICATIONS INC: Robocall Mitigation Plan

1. Purpose

This Robocall Mitigation Plan outlines the policies, controls, and enforcement mechanisms implemented by IXICA to prevent, detect, mitigate, and remediate unlawful robocall traffic across our voice network. IXICA complies with FCC 47 CFR § 64.6305, applicable STIR/SHAKEN requirements, and Industry Traceback Group (ITG) obligations.

IXICA maintains a zero-tolerance posture toward illegal robocalling, caller ID spoofing, scam campaigns, and artificial traffic pumping schemes.

2. Network Overview

IXICA operates as a VoIP and SIP trunking provider supporting enterprise, wholesale, and reseller customers.

Key controls:

- All SIP interconnections are authenticated.
- SIP signaling and media sessions are logged where technically feasible.
- Caller ID presentation is restricted to authorized and assigned numbers.
- Anonymous origination of traffic is not permitted.

3. STIR/SHAKEN Implementation

Where applicable, IXICA signs outbound traffic using STIR/SHAKEN in accordance with industry standards or relies on a third party to sign calls.

Outbound Authentication:

- A-Level (Full Attestation): Customer identity verified and number assigned by IXICA.
- B-Level (Partial Attestation): Customer identity verified but number not directly assigned.
- C-Level (Gateway Attestation): Calls entering IXICA network from a non-authenticated upstream source.

Inbound Verification where applicable:

- PASSporT validity
- Certificate trust chain integrity
- Attestation level

Calls that fail verification may be flagged, labeled, rate-limited, or blocked based on internal risk scoring policies.



4. Know Your Customer (KYC) & Customer Vetting

IXICA performs strict KYC procedures prior to service activation.

Third-Party Identity Verification includes:

- Business registration validation
- Government-issued identification (where applicable)
- Beneficial ownership verification
- Physical business address confirmation
- Legitimacy of operations screening

High-risk verticals undergo enhanced due diligence review.

Caller ID Controls:

- Numbers are only assigned to verified customers.
- Caller ID usage must match numbers assigned or explicitly authorized.
- Spoofing of unauthorized numbers is strictly prohibited.

5. In-House CDR Analytics & Traffic Monitoring

IXICA utilizes proprietary in-house Call Detail Record (CDR) analytics tools to monitor traffic patterns in real time.

Monitored Indicators include:

- Short-duration call spikes
- High call volume bursts
- Sequential dialing behavior
- Abnormal ASR degradation
- Abnormal ACD patterns
- Invalid or unassigned caller IDs
- Calls to Do Not Originate (DNO) numbers
- Rapid traffic ramp-up on newly provisioned accounts

Automated thresholds trigger immediate review by IXICA's NOC and Fraud teams.

6. Immediate Suspension & Investigation Policy

IXICA maintains a zero-tolerance enforcement framework.

If suspicious robocall or fraudulent traffic is detected:

1. Immediate Suspension: Customer traffic is suspended immediately.
2. Traffic Halt: Origination capability is disabled pending review.
3. Formal Investigation: CDRs, SIP headers, and complaint data are analyzed.
4. Customer Inquiry: Customer must provide documented evidence supporting lawful traffic

practices.

Reinstatement occurs only after satisfactory resolution. Confirmed violations result in permanent account termination and potential regulatory reporting.

7. Call Blocking & Mitigation Controls

IXICA implements layered mitigation controls including:

- Blocking calls from DNO lists
- Blocking invalid NANP formats
- Blocking known spoofing patterns
- STIR verification-based blocking (per policy)
- Rate limiting and CPS controls per account
- Traffic shaping when thresholds are exceeded
- Upstream carrier notification where appropriate

8. Traceback Cooperation

IXICA cooperates fully with:

- Industry Traceback Group (ITG)
- FCC Enforcement Bureau
- Law enforcement agencies

Traceback requests are acknowledged and responded to within the required regulatory time window. IXICA prioritizes all traceback inquiries to ensure timely compliance.

Requests are handled through CDR analysis and SIP header review to identify originating sources. Appropriate mitigation action is taken upon confirmation.

9. Record Retention

IXICA retains:

- Call Detail Records (minimum 12 months)
- SIP signaling logs (where technically feasible)
- KYC documentation and verification records
- Complaint logs
- Traceback correspondence

All records are stored securely with strict access controls.

10. Continuous Compliance & Review

IXICA regularly:

- Reviews mitigation thresholds
- Updates DNO lists



- Audits STIR/SHAKEN implementation where applicable
- Conducts compliance and fraud training
- Enhances analytics models and fraud detection methodologies

11. Certification Statement

IXICA certifies that the above mitigation practices are actively implemented and enforced to prevent the origination and transmission of unlawful robocalls on its network.

Authorized Signatory: Jenoshan Balasingam

Title: VP, Operations

Signature _____


Date: 2026-Feb-28