

Robocall Mitigation Program Statement

Techknowledge Open Systems CC

1. Company Overview

Techknowledge Open Systems CC is a foreign telecommunications service provider incorporated in South Africa. The company delivers voice services via IP-based interconnections and carries and/or processes traffic utilizing North American Numbering Plan (NANP) resources.

As a foreign voice service provider and non-gateway intermediate provider, Techknowledge Open Systems CC has implemented this Robocall Mitigation Program in accordance with 47 CFR § 64.6305. The purpose of this program is to prevent the origination, transmission, carrying, or processing of illegal robocall traffic and to ensure full cooperation with traceback and enforcement authorities.

Our mitigation framework is built upon layered technical controls, strict customer onboarding procedures, contractual safeguards, continuous monitoring, and zero-tolerance enforcement.

2. Network Access and Authorization Controls

To prevent unauthorized network access and traffic origination:

- All IP interconnections require prior written authorization before activation.
- Each approved interconnection is provisioned with defined routing permissions and class-of-service restrictions.
- Authentication credentials and access controls are periodically reviewed and updated.
- Unauthorized access attempts are automatically detected and blocked by network security systems.

These measures ensure that only approved entities may transmit traffic across our infrastructure.

3. Customer Due Diligence and KYC Compliance

Techknowledge Open Systems CC maintains a comprehensive Know-Your-Customer (KYC) program.

Customer Requirements:

- Government-issued identification (for individuals).
- Business registration documentation (for entities).
- Verified website and operational domain.
- Valid contact information.
- Description of business purpose and intended traffic profile.

Verification Process:

- Documentation is validated against government and third-party databases.
- Enhanced due diligence is performed for new customers prior to service activation.
- Annual compliance re-verification is conducted for renewing customers.

Services are provided exclusively to verified entities with legitimate communication requirements. Anonymous resellers, unverified traffic aggregators, and opaque traffic sources are strictly prohibited.

4. Contractual Safeguards

All customers must execute a binding service agreement that:

- Prohibits the origination, transmission, or facilitation of illegal robocalls.
- Requires compliance with applicable FCC regulations, including STIR/SHAKEN obligations where applicable.
- Prohibits unauthorized resale of services.
- Requires immediate reporting of suspected compliance violations.
- Mandates maintenance of an operational website and identifiable business presence.

Violations result in immediate suspension, restriction, or termination of services.

5. Caller Identification and CLI Controls

We enforce strict caller identification standards across our network:

- Invalid, spoofed, unallocated, or malformed Caller ID (ANI/CLI) is prohibited.
- Calls exhibiting suspicious CLI behavior are automatically flagged for review.
- Repeated violations result in suspension or permanent termination.

Caller ID integrity is treated as a critical compliance priority.

6. Real-Time Call Analytics and Monitoring

Techknowledge Open Systems CC utilizes proprietary analytics systems to detect and prevent illegal robocall traffic through:

- Real-time pattern recognition
- Anomaly detection algorithms
- Behavioral traffic analysis
- Daily compliance reporting

Traffic identified as suspicious is investigated immediately. Confirmed illegal sources are blocked without delay. Monitoring parameters are continuously updated to address evolving robocall methodologies.

7. Blocking and Traffic Control Measures

Our systems are configured to:

- Block invalid or malformed traffic.
- Prevent termination of clearly fraudulent traffic.

- Enforce Do Not Call (DNC) compliance where applicable.
- Dynamically block high-risk routes based on traffic behavior, complaint data, and volume thresholds.

These controls are implemented at the network level to ensure proactive mitigation.

8. Enhanced Monitoring for High-Risk Patterns

We continuously monitor for indicators commonly associated with robocall campaigns, including:

- High-volume, short-duration call patterns
- Rapid ANI rotation
- Traffic bursts outside normal behavior profiles
- Abnormal complaint ratios

Automated alerts trigger immediate compliance review and, where necessary, traffic suspension.

9. Zero-Tolerance Enforcement Policy

Techknowledge Open Systems CC maintains a strict zero-tolerance policy regarding:

- Caller ID spoofing
- Illegal robocalling
- Persistent suspicious traffic behavior

Accounts found engaging in prohibited activities are subject to immediate throttling, restriction, suspension, or permanent termination following investigation.

10. Staff Training and Regulatory Awareness

Compliance personnel and technical teams receive regular training on:

- FCC robocall mitigation requirements
- Industry best practices
- Emerging robocall tactics
- Traceback cooperation procedures

This ensures ongoing regulatory alignment and operational readiness.

11. Customer Education

We actively inform customers of:

- FCC compliance obligations
- Legal risks associated with robocalls
- Consequences of non-compliance
- Proper caller ID usage requirements

Customer awareness is considered a core component of mitigation.

12. Industry Association Participation

Techknowledge Open Systems CC is not a member of USTelecom. The company does, however, actively participate in and cooperate with industry-wide anti-robocall initiatives led by USTelecom and other industry bodies, including traceback requests, information-sharing efforts, and adoption of recommended best practices.

13. Audit, Review, and Continuous Improvement

We conduct periodic internal audits to evaluate:

- Traffic patterns and customer behavior
- Effectiveness of detection thresholds
- Compliance documentation
- Mitigation performance

We continuously refine our program through updated monitoring rules, onboarding enhancements, cooperation with industry anti-robocall initiatives, and adoption of emerging mitigation technologies.