

Softtop Limited

Robocall Mitigation Program Description

Foreign Voice Service Provider & Non-Gateway Intermediate Provider

1. Introduction & Regulatory Status

Softtop Limited is a foreign telecommunications service provider headquartered in Hong Kong. The company delivers voice services via IP-based interconnections. As a **Foreign Voice Service Provider** and **Non-Gateway Intermediate Provider**, Softtop Limited maintains this Robocall Mitigation Program in compliance with **47 CFR § 64.6305**. The purpose of this program is to prevent the origination, carriage, or processing of illegal robocall traffic and to ensure full cooperation with traceback and enforcement authorities.

2. Governance & Compliance Oversight

Softtop Limited maintains a strict zero-tolerance policy toward:

- Illegal robocalling
- Caller ID spoofing
- Unauthorized traffic transmission
- Fraudulent telecom practices

A designated Compliance Officer is responsible for:

- Maintaining FCC Robocall Mitigation Database (RMD) filings
- Overseeing customer vetting and onboarding controls
- Coordinating traceback responses
- Conducting quarterly compliance reviews
- Ensuring regulatory monitoring and updates

All compliance policies are formally documented and reviewed annually or upon regulatory amendments.

3. Customer Vetting & Onboarding Controls

Prior to service activation, enhanced due diligence procedures are conducted. Mandatory onboarding requirements include:

- Executed service agreement containing anti-robocall provisions
- Verified company registration documentation
- Beneficial ownership disclosure (where applicable)
- Government-issued identification and address verification (KYC)
- Operational website and business activity verification
- Written traffic usage declaration, including call purpose

Customers are risk-classified (Low / Medium / High) based on:

- Traffic volume projections
- Reseller status
- Geographic exposure
- Historical industry risk indicators

4. Network Authorization & Access Controls

To prevent unauthorized call origination or routing:

- All IP interconnections require explicit pre-authorization
- Defined routing permissions and class-of-service restrictions are assigned
- SIP authentication credentials are regularly reviewed
- Unauthorized access attempts are automatically blocked
- Network access policies are periodically audited

5. Traffic Authentication & Caller ID Validation

Layered validation mechanisms are implemented to detect and prevent spoofed or invalid traffic:

- Automatic blocking of invalid, unallocated, or malformed Caller ID/ANI
- Rejection of known fraudulent numbering ranges
- Geographic consistency checks where technically feasible
- Real-time flagging of suspicious CLI patterns

6. Call Analytics & Fraud Detection

Softtop Limited utilizes internal analytics systems for:

- Real-time anomaly detection
- Behavioral traffic pattern monitoring
- Short-duration call ratio analysis
- Sequential dialing detection
- Rapid ANI rotation detection
- Complaint ratio monitoring

Daily reports are generated and reviewed. Confirmed suspicious traffic is blocked immediately.

Detection algorithms are updated periodically to address evolving robocall tactics.

7. Invalid Traffic Blocking & DNC Compliance

Our network enforces:

- Blocking of invalid terminations
- Rejection of unauthorized outbound traffic
- Dynamic route suspension when risk thresholds are exceeded
- Rate limiting for new customers

- CLI reputation scoring mechanisms

Where applicable, Do Not Call (DNC) compliance requirements are enforced in accordance with regulatory standards.

8. Zero-Tolerance Enforcement Policy

Entities found to engage in illegal robocalling, spoofing, or related abusive activity are subject to:

- Immediate traffic suspension
- Account throttling or restriction
- Permanent termination upon confirmation of violation

Repeat offenders are permanently blocked from the network.

9. High-Risk Traffic Controls

Enhanced safeguards apply to high-risk routes, including:

- Volume-based thresholds
- Dynamic behavioral blocking
- Real-time alerting
- Increased monitoring frequency
- Complaint-triggered investigation protocols

10. Training & Awareness

Personnel receive periodic training covering:

- FCC robocall mitigation regulations
- Industry best practices
- Fraud detection methodologies
- Regulatory updates

Customer education materials are provided to promote compliance and responsible traffic usage.

11. Audit & Continuous Improvement

Regular internal audits are conducted to evaluate:

- Traffic integrity
- Effectiveness of mitigation controls
- Compliance adherence
- Onboarding risk controls

Mitigation procedures are enhanced as needed to address new threats or regulatory updates.

12. Traceback & Regulatory Cooperation

Softtop Limited fully cooperates with:

- The U.S. Traceback Consortium
- The Federal Communications Commission (FCC)
- Law enforcement agencies
- Authorized regulatory bodies

Traceback requests are:

- Acknowledged within 24 hours
- Investigated promptly
- Supported with relevant call detail records
- Escalated for immediate suspension where appropriate

Confirmed violators are permanently terminated. Records are retained to support investigative processes.

13. Ongoing Commitment

This Robocall Mitigation Program:

- Is actively implemented
- Is regularly reviewed for effectiveness
- Supersedes all prior versions
- Reflects current FCC requirements effective February 2026

Softtop Limited remains committed to preventing illegal robocalls and maintaining full compliance with **47 CFR § 64.6305**.