

Robocalling Mitigation Plan

1. Purpose & Scope

This plan outlines the measures implemented to prevent, detect, and mitigate illegal robocalling, spoofing, and fraudulent voice traffic across our network. It applies to all inbound and outbound voice services, including **DIDs, SIP trunking, wholesale voice, and termination services**.

2. Regulatory Alignment

We align with applicable regulations and industry best practices, including:

- National telecom authority requirements (e.g. Ofcom, FCC)
- Consumer protection and anti-fraud regulations
- Industry best practices and carrier guidelines (e.g. GSMA, i3forum)

3. Customer Onboarding & Due Diligence

Robocall risk is addressed before traffic is enabled through:

- **KYC & KYB verification**
 - Company registration documents
 - Beneficial ownership details
 - Proof of address and authorised signatories
- **Use-case validation**
 - Clear description of call purpose (e.g. customer support, appointment reminders)
 - Explicit prohibition of robocalling, auto-dialling, and unsolicited calls unless legally permitted
- **Geographic & service restrictions**
 - Domestic vs international calling permissions
 - Call type limitations (mobile, landline, premium)

4. Contractual & Policy Controls

All customers are contractually bound to:

- Use services **only for lawful, consent-based calling**
- Prohibit:
 - Robocalls
 - Spoofing or unauthorised CLI manipulation
 - Artificial call inflation (ACI)
 - Scam, phishing, or impersonation calls
- Accept **immediate suspension or termination** for violations

5. Network Monitoring & Detection

We employ continuous traffic monitoring, including:

- **Real-time analytics**
 - Call velocity spikes
 - Short-duration or burst calling patterns
 - Abnormal ASR / ACD behaviour
- **CLI behaviour analysis**
 - Repeated or high-volume CLI usage
 - Invalid, unassigned, or suspicious calling numbers
- **Destination risk profiling**
 - Known fraud-prone destinations
 - Unusual time-of-day or call distribution patterns

6. Caller ID & Traffic Controls

To mitigate spoofing and abuse:

- Caller ID presentation is restricted to:
 - Allocated or verified numbers only
- Invalid, masked, or suspicious CLIs may be:
 - Blocked
 - Rate-limited
 - Subject to additional verification
- Customers are prohibited from altering CLIs without prior authorisation

7. Incident Response & Enforcement

Upon detection of suspected robocalling:

1. Immediate traffic investigation
2. Rate-limiting or temporary suspension
3. Customer notification and explanation request
4. Permanent disconnection for confirmed abuse
5. Notification of upstream carriers or regulators where required

8. Reporting & Traceback Cooperation

- Full cooperation with:
 - Regulators
 - Industry traceback initiatives
 - Law enforcement upon valid request
- Call Detail Records (CDRs) are retained in line with legal and contractual requirements

9. Continuous Improvement

- Ongoing refinement of detection thresholds
- Regular review of customer use cases
- Staff training on fraud prevention and compliance
- Periodic audits of suppliers and partners

10. Zero-Tolerance Statement

We operate a **zero-tolerance policy** toward illegal robocalling and reserve the right to block or suspend traffic without notice to protect end users, partners, and network integrity.