

Teloz Limited- Robocall Mitigation Plan

Executive Summary

Teloz Limited submitted certifications and robocall mitigation plans to the Robocall Mitigation Database (RMD). This includes expanded disclosure requirements. Teloz Limited, as a foreign voice service provider with an Operating Company Number (OCN) license, complies fully by filing initial and ongoing certifications.

Teloz Limited is dedicated to preventing illegal calls from originating on our network and monitoring inbound traffic. We leverage advanced infrastructure with full STIR/SHAKEN implementation to enhance mitigation efforts. This plan details our multi-layered approach to robocall prevention, incorporating risk-based controls and full cooperation in traceback activities.

Company Purpose and Role

Teloz Limited operates as a foreign voice service provider, delivering VoIP services. We are committed to stopping illegal calls at their source while ensuring legitimate communications remain uninterrupted. STIR/SHAKEN compliance and an OCN license, we focus on robust upstream and downstream vetting to maintain network integrity.

Governance and Compliance Structure

- **Zero-Tolerance Policy:** Teloz Limited enforces a strict policy against illegal robocalling, spoofing, and abusive practices.
- **Compliance Officer Responsibilities:** A designated officer oversees RMD filings, customer onboarding, traceback coordination, and quarterly reviews. Policies are documented, annually audited, and updated per regulatory changes.

Customer Vetting (Know Your Customer)

- **Verification Process:** All new customers undergo identity confirmation, including name, email address validation, and location verification. Submissions are cross-checked against databases and third-party sources.
- **Risk Classification:** Customers are categorized as Low, Medium, or High Risk based on traffic profiles, reseller status, and exposure. High-risk entities require enhanced due diligence and management approval.
- **Ongoing Monitoring:** Renewing customers face annual re-verification to ensure compliance.

Customer Agreements and Terms of Service

All customers must agree to Teloz Limited's Terms of Service (TOS) prior to activation. Key prohibitions include:

- Providing altered, deceptive, or false information about sender identity or call origin.
- Engaging in "autodialing" and/or "telemarketing" without consent.
- Violations trigger immediate suspension or termination, with mandatory reporting of suspected issues.

Network Monitoring and Traffic Controls

Our systems are configured for active oversight:

- **Blocking Mechanisms:** Invalid ANI is blocked; spoofed or unallocated caller IDs are rejected in real time.
- **Daily Analytics:** Potential spam indicators are monitored, with flagged ANIs blocked promptly.
- **Pattern Detection:** Real-time analysis identifies anomalies like sudden spikes, short-duration calls, or sequential dialing. Suspicious patterns trigger automated suspension pending review.
- **DNC Enforcement:** Network-wide integration prevents calls to registered Do Not Call numbers.
- **Mass Calling Monitoring:** Continuous monitoring for mass calling events, coordination with the Industry Traceback Group (ITG), trusted third parties, and federal agencies to mitigate fraudulent calls.
- **Do Not Originate (DNO) Blocking:** In coordination with the ITG, blocking of government impersonation calls, "call back" Direct Inward Dial (DID) numbers used in scams (including one-ring scams), and numbers associated with mass robocalling campaigns identified by trusted third parties.
- **Cease-and-Desist Response:** Readiness to conduct additional network-level blocking in response to FCC "cease-and-desist" letters if recipients fail to undertake remedial measures.

Traceback and Enforcement Cooperation

- **Response Protocol:** All traceback requests from the FCC, U.S. Telecom, law enforcement, or authorized entities are resolved within 24 hours.
- **Investigation Process:** We suspend suspected accounts during reviews, terminate confirmed violators permanently, and provide data/technical assistance.
- **User Feedback:** Mechanisms encourage reporting of suspicious calls, with prompt investigations and actions.

Continuous Improvement and Training

- Staff receive regular training on FCC regulations and prevention techniques.
- Customers are educated on compliance obligations to foster responsible usage.

- Audits ensure program effectiveness, with updates within 10 business days of material changes.
- **Program Updates and Collaboration:** Regular updates to our robocall mitigation program following industry best practices. Collaboration with industry stakeholders to combat illegal robocalling, contributing to the eradication of illegal robocall traffic and protecting consumers from unwanted and fraudulent calls.