

Robocall Mitigation Program Description

Company Name: JUSI PTE. LTD.

FCC Registration Number (FRN): 0038202917

Date of Submission: March 2026

Version: 1.0

1. Introduction

JUSI PTE. LTD. (the “Company”) is a foreign voice service provider headquartered in Singapore. The Company provides mobile-application-based VoIP services, enabling end-users to place calls to US and utilize North American Numbering Plan (NANP) resources.

STIR/SHAKEN Implementation Status: The Company has selected “No STIR/SHAKEN Implementation” because it is a foreign-based entity with no physical switching facilities or domestic IP network within the United States. Furthermore, as a non-U.S. entity, the Company is currently ineligible to obtain a Service Provider Code (SPC) token from the U.S. STI-GA, which is the technical prerequisite for independent STIR/SHAKEN signing. All traffic is handed off to U.S.-based gateway providers who perform the necessary authentication before the calls enter the U.S. PSTN.

2. Know Your Customer (KYC) & Identity Verification

The Company adheres to a strict "Financial and Ecosystem-Based KYC" model. By integrating with regulated global application platforms (Apple App Store and Google Play Store), the Company ensures that every user is linked to a verified identity:

- **Platform-Level Authentication:** Access to telecommunications resources is restricted to users with active, authenticated accounts on the Apple or Google platforms. This leverages the platform providers’ existing fraud detection and identity verification systems.
- **Financial Traceability:** The Company exclusively provides premium calling features to users who have completed a verified transaction via the official App Store/Google Play billing systems. This ensures every active caller is linked to a valid payment instrument.
- **Store-Linked Traceability:** In response to authorized regulatory inquiries, the Company can provide the specific "Store-Linked ID" or "Transaction Receipt ID" associated with any call, allowing law enforcement to trace the originating party through the platform’s verified financial records.

3. Anti-Automation & Preventative Controls

To prevent the platform from being exploited by automated scripts or robocall botnets, the Company employs the following technical safeguards:

- **Persistent Hardware Binding:** The Company captures and validates OS-level unique identifiers for every registration—specifically the **Android ID (SSAID)** for Android devices and the **Identifier for Vendors (IDFV)** for iOS devices. Each user account is cryptographically bound to these hardware-linked fingerprints.
- **Hardware-Level Blacklisting:** Any device identified as a source of illegal robocalling is permanently blacklisted at the hardware ID level, preventing the offender from "account hopping" or re-registering on the same device.
- **Rate Limiting:** The Company enforces strict limits on the number of accounts and call attempts associated with a single hardware identifier (Android ID/IDFV) within specified timeframes to block high-volume automated dialing.

4. Real-Time Call Monitoring & Analytics

The Company's network operations center monitors traffic patterns to detect and mitigate illegal robocalling in real-time:

- **Short-Duration Call Analysis:** The system flags and automatically suspends accounts with an abnormally high ratio of calls lasting less than 6 seconds.
- **Call Answering Rates:** Accounts exhibiting low answering rates typical of "Scam Likely" behavior are subject to immediate manual review and potential service termination.

5. Commitment to Traceback Cooperation

The Company fully recognizes the importance of the **Industry Traceback Group (ITG)** and U.S. law enforcement efforts:

- **24-Hour Response Guarantee:** The Company commits to responding to all valid traceback requests within **24 hours** of receipt.
- **Dedicated Compliance Contact:** A designated compliance team is assigned to handle all regulatory and traceback inquiries via report@juscalls.com.
- **Full Data Disclosure:** For any identified illegal traffic, the Company will provide the UTC timestamp, SIP Call-ID, Source IP, and the associated Store-Linked ID/Device ID to facilitate the "end-to-end" tracing of the call's origin.

6. Enforcement and Mitigation Actions

The Company maintains a "Zero Tolerance" policy for illegal robocalling. Upon confirmation of a violation:

1. The associated user account is permanently terminated.
2. The associated hardware identifier (Android ID/IDFV) is globally blacklisted.
3. All remaining credits or subscriptions are forfeited to deter future abuse.