

Company Name: UT International Pte LTD

Address: 10 Anson Road, #35 11 International Plaza, Singapore 079903

Date: 2026-02-23

Document: Robocall Mitigation Plan (RMP)

1. Network Role and Business Model UT International ("UT") operates as a software messaging provider and Originating Voice Service Provider, allowing vetted customers to send and receive Fax and SMS communications. UT International formally identifies as a **Foreign Voice Service Provider** under FCC definitions, as it originates traffic from outside the United States. Customers do not have SIP interconnection capabilities; all service access is strictly controlled via our proprietary web portal and REST API application interfaces. UT maintains its own IP infrastructure (FreeSWITCH) and routes terminating traffic through interconnected, FCC-registered US Gateway Providers, including Tier 1 carriers, Tier 2 carriers, and Competitive Local Exchange Carriers (CLECs).

2. STIR/SHAKEN Implementation Status UT International formally files as a Foreign Voice Service Provider that has not implemented STIR/SHAKEN. UT International does not hold a direct STIR/SHAKEN Service Provider Code (SPC) token or certificate. Instead, UT relies on its interconnected US Gateway Providers as the signing entities. These gateway partners perform the technological act of authentication by signing the calls using their own STIR/SHAKEN certificates prior to termination on the US Public Switched Telephone Network (PSTN).

3. Downstream Customer Vetting (KYC) UT strictly controls access to its network to prevent illegal robocalling and CLI spoofing at the source. Our Know Your Customer (KYC) procedures include:

- **Identity Verification:** We maintain database records of all UT customers, which include, where reasonably available, the verified business name, contact name, physical address, and contact number.
- **Controlled DID Pools:** UT maintains a controlled pool of active, registered US DIDs used for outbound fax calls. DIDs are only linked to individual customers after they have undergone a vetting and approval process conducted by our sales and operations teams. Outbound DIDs are tied to active voicemail services that provide clear opt-out instructions to recipients.
- **Anti-Spoofing Controls:** Because customers connect via API/SaaS rather than SIP trunks, CLI parameters are strictly controlled at the platform level. By default, the ability for end-users to set or alter their Caller ID (CLI) is disabled to prevent anonymity and mass-spoofing. UT maintains the 'A' number for the majority of traffic; any administrative override to allow custom CLI settings is only granted following a secondary technical review and verification of the customer's specific use case and traffic profile.

4. Upstream Provider Vetting UT selects upstream telecommunications partners and routing providers from established, FCC-registered carriers, including Tier 1 carriers, Tier 2 carriers, and CLECs. Prior to interconnection, and on an ongoing basis, UT verifies that all upstream and gateway partners maintain an active, approved registration status within the FCC's Robocall Mitigation Database.

5. Active Call Analytics and Blocking Procedures UT proactively monitors network traffic using both automated safeguards and active human oversight by our Network Operations Center (NOC) to identify and block illegal traffic:

- **Strict Destination Blocking:** UT's routing tables automatically block traffic to high-risk destinations, including premium rate numbers, special numbers, and cellular networks. Any destination route with a cost exceeding \$0.25 is hard-blocked at the switch level.
- **Rate Limits and Volume Thresholds:** Automated rate limits are enforced at the API level to prevent unnatural spikes in traffic volume indicative of automated robocalling.
- **Automated Alerts and NOC Monitoring:** Our infrastructure monitors for anomalous behavior, such as high call failure rates or unusually short duration calls. Such anomalies trigger immediate system alerts. Our NOC actively monitors these alerts and performs regular spot-checks on traffic profiles. If an investigation is required, UT cross-references Call Detail Records (CDRs) with the assigned customer CLI to immediately identify the source and take mitigative action.

UT does not utilise third-party call analytics vendors; all monitoring and analysis is performed internally using our own infrastructure and NOC team.

6. Contractual Provisions and Enforcement UT International ensures it has the legal authority to immediately halt suspected illegal robocalling campaigns. All customers are bound by platform usage terms that explicitly prohibit using the service to break any laws or infringe on the legal rights of any person. UT International retains the right to immediately suspend or permanently terminate the account and API access of any customer found to be in breach of these terms or engaging in fraudulent traffic

7. Corporate Structure and Accountability

- **Designated Point of Contact:**

Name: Kasra Salehi

Position: Head of Messaging Division

Phone: +61488863155

Email: contact@utinternational.sg

- **Traceback Cooperation:** UT International actively cooperates with industry traceback efforts. We explicitly commit to responding to all traceback requests from the Industry Traceback Group (ITG), the FCC, and law enforcement agencies fully and accurately within 24 hours of receipt by identifying the upstream source or affiliated platform originating the traffic on our network.
- **Principals, Affiliates, and Enforcement History:** The controlling principal and Director of UT International is Rhett Jones. UT International has no parent company and no telecom subsidiaries or affiliates. UT International operates as a foreign provider and does not possess a US Operating Company Number (OCN). Neither UT International, Director Rhett Jones, nor any associated individuals have been the subject of any formal law enforcement or regulatory action, or investigation regarding illegal robocalls or spoofing in the prior two years.

UT International Pte Ltd certifies that the information contained in this Robocall Mitigation Plan is true, accurate, and complete as of the date of filing.