

Robocall Mitigation Plan & Compliance Statement

1. Role in Call Chain

iTalk Global Communications, Inc. (“iTalk”) is an Interconnected VoIP provider. iTalk functions as a “voice service provider” that originates and terminates calls for its residential customer base but does not have direct access to numbering resources.

The company is fully registered in the **Robocall Mitigation Database (RMD)** and has implemented the **STIR/SHAKEN** authentication methodology. All authenticated calls utilize a valid certificate issued by the STI-CA.

2. Company Information & Regulatory Standing

- **Parent Company:** Beijing Net263 Ltd.
 - **Affiliates:** iTalk has no affiliates providing voice telephone services within the United States.
 - **Operating Company Number (OCN):** 749J.
 - **Regulatory History:** iTalk is not currently subject to any Commission, law enforcement, or regulatory agency action or investigation regarding suspected unlawful robocalling. To date, iTalk has received zero (0) traceback requests.
-

3. Robocall Mitigation & Prevention Measures

iTalk takes affirmative, effective measures to prevent the origination of illegal calls from both new and renewing customers.

A. Know Your Customer (KYC)

iTalk exclusively serves residential customers and maintains strict onboarding protocols:

- **Identity Verification:** All customers must provide a name, physical address, and credit card information upon registration. All addresses are verified via a third-party service.
- **Technical Restrictions:** The service restricts users to a single concurrent call, preventing high-volume automated dialing.
- **Reasonable Residential Use Policy:** iTalk proactively monitors traffic to enforce this policy, which prohibits:
 - Operating call centers or support hubs.
 - Reselling services.
 - Utilizing auto-dialers, fax/voice blasts, or telemarketing tools is prohibited and technically enforced.

- **Contractual Provisions.** Customers must agree to iTalk’s terms of service that prohibit fraudulent traffic. Additionally, the terms of service provide that iTalk may suspend or terminate services for violating iTalk’s acceptable use provisions.
- **Enforcement:** iTalk monitors for abnormal patterns, such as unusual call durations, excessive forwarding, or high-frequency short-duration calls. iTalk reserves the right to warn, suspend, or terminate service to enforce compliance.
- **Anti-Spoofing:** iTalk prohibits Caller ID manipulation and utilizes industry-standard authentication technology to prevent spoofing.
- iTalk checks the **Robocall Mitigation Database** and only accepts calls from voice service providers, intermediate providers, and gateway providers if those providers are listed in the Robocall Mitigation Database.
- **Call analytics systems:** iTalk uses internally designed software to monitor customer traffic to look for robocalls and to detect any noncompliance with our “Reasonable Residential Use Policy”. The software looks for unusual call patterns, usage involving specific numbers called, average call durations, forwarding and transferring, conferencing and unusually short duration calling. Based on these factors, iTalk may determine that abnormal, unreasonable or impermissible usage is occurring, and may take appropriate steps including a warning and/or termination of service to that customer.

B. Know Your Upstream Provider

iTalk maintains high standards for its upstream partners:

- **Compliance:** All upstream providers must be registered in the Robocall Mitigation Database and maintain a reasonable mitigation plan in accordance with FCC regulations.
- **Vetting:** iTalk has maintained relationships with its primary carriers for over 10 years and is not aware of any robocalls transferred to iTalk customers from these providers.
- **Contractual Safeguards:** Contracts explicitly prohibit the transmission of illegal robocalls, providing iTalk the right to terminate service for non-compliance.
- **Ingress Monitoring:** iTalk utilizes STIR/SHAKEN attestation on ingress calls, displaying a visual verification (checkmark) for all full attestations.

C. Call Analytics & Monitoring

iTalk employs proprietary internal software to identify and block illegal traffic. This system flags non-compliance by analyzing:

- Unusual call patterns and specific number targeting.
- Average call durations and frequency of "short-duration" calls.
- Anomalous forwarding, transferring, and conferencing activity.

D. Traceback Cooperation & Mitigate

iTalk is fully committed to the integrity of the ecosystem and pledges to:

- **Commitment to Respond to Traceback Requests.** iTalk commits to respond fully and within twenty-four (24) hours to traceback requests from law enforcement, the Federal Communications Commission, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocalls that use its services to originate such calls.
- **Cooperate fully** with investigating entities to identify and stop illegal robocallers.

This Robocall Mitigation Plan describes the specific measures that iTalk has implemented as of February 10, 2026. iTalk continually evaluates the efficacy of its measures to combat bad actors and takes appropriate steps to improve these measures when needed.