

Robocall Mitigation Program for Kaidu Commercial & Trading Ltd Co.

FCC Registration Number (FRN): 0036557809

Date of Implementation: 09-16-2025

Purpose & Policy

Kaidu Commercial & Trading Ltd Co. has established policies to combat fraudulent calling. This document, formally implemented on the date above, establishes a comprehensive Robocall Mitigation Plan to ensure full and explicit compliance with all current FCC rules under 47 CFR § 64.6305(a). Our company maintains a zero-tolerance policy against illegal robocalls, spoofing, and fraud originating from our network.

1. Exemption from STIR/SHAKEN Implementation

Kaidu Commercial & Trading Ltd Co. is exempt from the mandatory implementation of the STIR/SHAKEN authentication framework pursuant to 47 CFR § 64.6304(c), the "de minimis" exemption.

This exemption applies to providers that originate 100,000 voice call minutes or less annually. Our company's internal records and billing data for the previous 12-month period indicate that we originated approximately **15,000** voice call minutes, which is significantly below the FCC's established threshold.

2. Robocall Mitigation practices - Reasonable Steps Taken

Despite this exemption, Kaidu Commercial & Trading Ltd Co. is fully committed to preventing our service from being used to originate illegal robocalls. Our robocall mitigation program includes the following reasonable steps:

a. Know Your Customer (KYC) Procedures:

- We require valid business identification and contact information (including name, physical address, and phone number) for all customers prior to activating service.
- We do not accept anonymous customers or anonymous payments.
- We assess new customer relationships to identify potential risks.

b. Secure Platform Management:

- We require the use of strong passwords for all customer accounts and administrator portals.
- We educate customers on security best practices and strongly encourage the use of multi-factor authentication (MFA) to prevent account hijacking.
- We monitor for and investigate failed login attempts that could indicate a brute-force attack.

c. Network Monitoring and Enforcement:

- We routinely monitor our network for anomalous calling patterns that are indicative of illegal robocalling, such as a sudden, massive increase in call volume, short call durations, and invalid calling number patterns.
- We review call detail records (CDRs) and maintain a direct relationship with our underlying voice service provider who alerts us to suspicious activity.
- If we identify suspicious activity, we immediately investigate and will suspend or terminate service for any customer found to be originating illegal calls.

d. Cooperation with Traceback Requests:

- We maintain detailed call records (CDRs) for all calls originated on our network for a period of not less than 6 months.
- We are committed to responding fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium (USTelecom's Industry Traceback Group).
- We will cooperate fully with such entities in investigating and stopping any illegal robocallers that use our service.

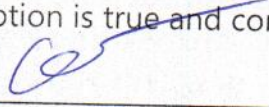
3. Point of Contact for Traceback Requests

The following person is designated as our point of contact for all official traceback requests and legal inquiries. This individual has the authority and access to investigate and respond to these requests.

- **Name:** Qingxia Wang
- **Title:** Owner
- **Email:** kaidu-lynn@kaiduweb.com
- **Phone:** (305) 477-1663

Certification:

I, Qingxia Wang, as the duly authorized representative of Kaidu Commercial & Trading Ltd Co., hereby certify that the information contained in this Robocall Mitigation Program description is true and correct to the best of my knowledge.

Signature: 

Printed Name: Qingxia Wang

Date: 09-16-2025