

Stuut – Robocall Mitigation Program

I. Objective

This Robocall Mitigation Program (“**Program**”) describes the policies and procedures that Stuut, Inc. (“**Stuut**”) has implemented which are designed to reduce the outbound illegal robocalls originating on its network.

II. Regulatory Compliance Statements

Stuut hereby certifies that:

- All calls originating on its network comply with this Program.
- It will respond within twenty-four (24) hours to all traceback requests from the Federal Communications Commission (“**FCC**”), law enforcement, and the industry traceback consortium, and cooperate with such entities in investigating and stopping illegal robocallers that use its service to originate, carry, or process illegal robocalls.
- Within the last two (2) years, Stuut has not been the subject of a formal FCC, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to Stuut transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, nor has it been found to have a deficient Robocall Mitigation Database certification or mitigation program description.

III. Mitigation Strategies

Stuut has taken the following steps to avoid the origination or processing of illegal robocall traffic as part of its Program:

- Customer Verification: Stuut conducts due diligence on new and renewing customers to ensure they do not use its network for illegal robocalling. Stuut's onboarding process includes collecting and verifying customer information, including, but not limited to, business identity, contact details, and the intended use of its voice services.
- Contractual Provisions: Stuut’s [Terms of Service](#) prohibit Stuut customers from using Stuut’s services in violation of applicable law. Additionally, Stuut customers provide contractual assurances that they have obtained all required consents to make artificial voice calls via Stuut’s services. These provisions prohibit Stuut customers from using Stuut’s network to originate illegal robocalls.
- Upstream Provider Procedures: Stuut has a vendor management program in place to evaluate and assess its upstream provider’s practices that is designed to ensure that its upstream providers monitor their networks and prevent their use for transmission of illegal robocalls. Stuut has written agreements in place with its vendors and related third parties. Stuut relies on its third-party voice service providers' mitigation efforts to reduce the outbound illegal robocalls originating on its network. For example, Retell AI, Inc., one of Stuut’s upstream providers, has implemented a Robocall Mitigation Certification and Plan, a copy of which is attached as **Exhibit A**.

IV. Contact Information

- Business Name: Stuut, Inc.
- Address: 373 Park Ave South, Fl 5, New York, NY 10016
- Email: legal@stuut.ai

EXHIBIT A

Retell AI, Inc. Robocall Mitigation Certification and Plan

Objective

As a key participant in the telecommunications industry, Retell AI, Inc. is committed to maintaining the integrity of the national phone network while safeguarding consumers from fraudulent or unauthorized calls. This document outlines the technical and operational strategies employed by Retell AI, Inc. to detect, prevent, and mitigate unlawful call traffic on its network.

Regulatory Compliance Statement

Retell AI, Inc. certifies that:

- All calls originating, transiting, or terminating on its network comply with this mitigation framework.
- It maintains its certification status with regulatory authorities and has not been subject to revocation.
- The company adheres to industry best practices for preventing illegal robocalls and promptly responds to traceback inquiries from regulatory bodies, law enforcement, and industry coalitions within 24 hours.
- Over the past two years, neither Retell AI, Inc. nor any associated entities have been the subject of an official investigation or enforcement action related to unauthorized call traffic, call spoofing, or non-compliance with mitigation protocols.

Mitigation Strategies

1. Customer Verification

New customers would require verifying their phone number via text message. One phone number can only be used for one user.

To enhance fraud detection, Retell AI, Inc. plans to implement Persona, an AI-driven risk assessment tool that evaluates device data, browser characteristics, IP history, mobile verification, payment details, and CAPTCHA validation. This system employs machine learning to differentiate between legitimate and suspicious activities.

2. Secure Network Access

All services are secured using Cloudflare Web Application Firewall (WAF), which restricts access from high-risk IP addresses. Requests originating from sources with a moderate risk profile require user authentication via challenge-response mechanisms.

3. Traffic Rate Control

Retell AI, Inc. employs Cloudflare Load Balancing to regulate the volume of requests sent to its network. Non-enterprise users are limited to a maximum of ten outbound calls per day to curb excessive or unauthorized call activity.

4. System Monitoring & Threat Detection

Through the Oneleet security platform, Retell AI, Inc. continuously scans for vulnerabilities and receives real-time alerts regarding potential threats. Any identified weaknesses are promptly addressed to ensure network security.

5. Incident Management & Response

Retell AI, Inc. collaborates with industry partners such as the USTA Industry Traceback Group (ITG) and telecommunications providers to investigate and respond to reports of unauthorized call activity. Reports submitted via automated systems, external analytics, or customer feedback are reviewed within 24 hours. Additionally, contracts with users and partners include acceptable use policies subject to enforcement through monitoring and manual review.

6. Data Analytics & Fraud Prevention

While Retell AI, Inc. does not utilize third-party analytics for outbound call verification, it intends to integrate Persona for customer identity validation and account security. These measures assist in detecting fraudulent account activity and preventing unauthorized access to services.

7. Employee Training & Compliance Awareness

A structured training program ensures that all employees, particularly those handling customer onboarding and renewals, understand the regulatory requirements and mitigation strategies. Staff receive instruction on identifying and addressing fraudulent activities, handling traceback requests, and complying with industry standards.

Corporate Information & Key Personnel

Legal Entity:

Retell AI, Inc.

Executive Leadership:

- **Bing Wu** – Chief Executive Officer
- **Weijia Yu** – Chief Operating Officer

Affiliated Entities:

- None

Compliance Contact

For inquiries from regulatory bodies, traceback requests, or law enforcement, please contact:

Contact Name: Weijia Yu

Title: Chief Operating Officer

Business Address: 2674 Hastings Ave Redwood City, CA 94061

Phone: +1 (310) 871-3825

Email: weijia@retellai.com

Revision History

Description	Date
Initial Documentation	Feb 27, 2025