

Robocall Mitigation Program Description

Clictree LLC

Filed pursuant to 47 C.F.R. § 64.6305

Filer Information

Legal Name of Filer: Clictree LLC

Business Address: 310 East Brinkerhoff Avenue, Palisades Park, NJ 07650

FCC Registration Number (FRN): 0038470175

Operating Company Number (OCN): 463M (assigned by NECA, effective July 10, 2026; IPES category)

Provider Type: Voice Service Provider (originating)

Point of Contact for Robocall Mitigation / Traceback: Steve Almonte, Chief Executive Officer, (201) 365-8124, steve@clictree.com

I. Overview and Purpose

Clictree LLC (the “Company” or “Provider”) submits this Robocall Mitigation Program description in accordance with the Federal Communications Commission’s (“FCC”) rules under 47 C.F.R. § 64.6305 and the TRACED Act. This document sets forth the Company’s current policies and procedures, which the Company considers to constitute reasonable steps to avoid originating illegal robocall traffic on its network. The Company is committed to following these practices and to cooperating fully with the FCC, law enforcement, and the Industry Traceback Group (“ITG”) in identifying and stopping any illegal robocallers that may attempt to use its services.

The Company provides voice services to business customers and may, in the future, originate voice traffic for its own internal business campaigns. The Company operates its own voice infrastructure built on Asterisk, FreePBX, and OpenSIPS, and it interconnects with an upstream SIP trunk / wholesale carrier for connectivity to the public switched telephone network. Because the Company controls its own softswitch and session border / proxy layer, it applies call routing controls, concurrent-call and rate limiting, and traffic monitoring directly within its own network.

II. Caller ID Authentication (STIR/SHAKEN) Status

The Company operates its own voice infrastructure and is subject to the STIR/SHAKEN caller ID authentication requirements. The Company has been assigned Operating Company Number (OCN) 463M by the National Exchange Carrier Association (NECA), effective July 10, 2026, under the IPES category. Because the prerequisites to obtaining a Service Provider Code (SPC) token are now satisfied or actively in progress, the Company does not claim, and no longer relies upon, the SPC token access extension previously available under 47 C.F.R. § 64.6304(b).

The Company has not yet completed STIR/SHAKEN implementation on its network. Having obtained its OCN, the Company is in the process of (1) registering with the Secure Telephone Identity Policy Administrator (STI-PA), currently iconectiv; (2) obtaining an SPC token against OCN 463M; and (3) obtaining a certificate from an approved Secure Telephone Identity Certification Authority (STI-CA). The Company’s Asterisk and OpenSIPS environment supports STIR/SHAKEN signing and will be configured to sign outbound calls using the Company’s own certificate upon issuance. Consistent with the FCC’s third-party authentication rules effective September 18, 2025, the Company will sign calls using its own SPC token and certificate and will make its own attestation decisions, even where a third-party vendor hosts

the signing workflow. The Company is diligently pursuing completion of STIR/SHAKEN implementation and will update this description and its Robocall Mitigation Database certification within the timeframe required by the Commission's rules upon completing implementation.

During the interim period before STIR/SHAKEN signing is active on its network, the Company relies on the robocall mitigation program described below, which it considers to constitute reasonable steps to avoid originating illegal robocall traffic. The Company only permits calls to be originated using telephone numbers that it or its customer legitimately owns or is verifiably authorized to use, and it does not engage in, and contractually prohibits its customers from engaging in, illegal caller ID spoofing.

III. Reasonable Steps to Avoid Originating Illegal Robocalls

A. Know Your Customer (KYC) Procedures

Before provisioning voice service to any customer, and consistent with its obligations under 47 C.F.R. § 64.1200(n)(4), the Company performs reasonable due diligence to verify the identity and legitimacy of each customer. These steps include:

- Collecting and verifying the customer's legal business name, business address, and a valid business point of contact;
- Identifying the nature of the customer's business and the intended use case for the voice service, including the types of calls to be made and the consent basis the customer relies on to place those calls;
- Requiring each customer to enter into a written service agreement (acceptable use / terms of service) that expressly prohibits the origination of illegal robocalls, illegal spoofing of caller ID, and any calling that violates the Telephone Consumer Protection Act (TCPA), Do-Not-Call rules, or other applicable federal or state law;
- Requiring customers to represent and warrant that they have obtained any legally required prior express consent before placing calls or texts, and that they will honor opt-out and Do-Not-Call requests; and
- Confirming that each customer uses only telephone numbers it owns or is authorized to use as caller ID.

B. Know Your Upstream Provider

The Company connects to the public switched telephone network through its upstream SIP trunk / wholesale carrier, 382 Communications. Before establishing interconnection with any upstream provider, the Company confirms that the provider is a legitimate, established carrier and, where applicable, that the provider is listed in the Robocall Mitigation Database and maintains its own robocall mitigation obligations. The Company will apply comparable diligence before adding any additional upstream or underlying carrier, and it relies on its upstream provider for downstream traceback cooperation as part of its overall mitigation program.

C. Affirmative Measures to Prevent Customers From Originating Illegal Robocalls

The Company takes affirmative, effective measures to prevent its customers from originating illegal robocalls, including:

- Contractual prohibitions on illegal robocalling and spoofing, with the right to immediately suspend or terminate any customer that violates these terms;

- Reservation of the right to require additional documentation of consent or calling authority from any customer whose traffic raises concern;
- Prompt suspension of a customer's ability to originate calls upon a credible indication that the customer is originating illegal robocalls; and
- Maintaining records sufficient to identify the originating customer of any call for traceback purposes.

D. Call Analytics and Blocking

The Company does not currently use a dedicated third-party call analytics or blocking vendor. Because it operates its own infrastructure, the Company applies controls directly within its Asterisk, FreePBX, and OpenSIPS environment, including call routing rules, concurrent-call and rate limiting, and the ability to block or reject traffic associated with abuse. These controls are used together with the manual monitoring practices described in Section IV below. The Company will evaluate adopting a dedicated third-party analytics solution as its call volume grows, and it will update this filing within the required timeframe if it engages such a vendor.

IV. Ongoing Monitoring Practices

The Company reviews call detail records (CDRs) and platform usage reporting on a recurring basis to detect calling patterns consistent with illegal robocalling. In its monitoring, the Company gives particular attention to indicators such as: (1) unusually high call volume or large bursts of traffic in short timeframes; (2) high volumes of short-duration calls and low call-completion rates; (3) sequential or patterned dialing of called numbers; and (4) calls placed using invalid, unallocated, or unauthorized calling numbers. When the Company detects activity consistent with illegal robocalling, or otherwise suspects illegal robocalling or spoofing, it promptly investigates to identify the responsible customer and takes appropriate action, which may include warning the customer, demanding proof of consent or calling authority, throttling traffic, or suspending or terminating the customer's service.

V. Commitment to Respond to Traceback Requests

The Company commits to respond within 24 hours to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group, and to cooperate fully with such entities in investigating and stopping any illegal robocallers that use its service to originate calls. The Company maintains a designated point of contact (identified above) for receiving and responding to traceback requests, and it maintains call records sufficient to trace traffic back to the originating customer.

VI. Principals, Affiliates, Subsidiaries, and Parent Companies

Clitree LLC is privately held. Principal: Steve Almonte, Chief Executive Officer. Affiliates, subsidiaries, and parent companies: None.

VII. Maintenance and Updates

The Company will keep this Robocall Mitigation Program description and its associated Robocall Mitigation Database certification current, and will update them within the timeframes required by the FCC's rules following any material change to the information contained herein.

This description is submitted in support of Clitree LLC's certification in the FCC Robocall Mitigation Database.