

ROBOCALL MITIGATION PROGRAM DESCRIPTION

Knox Landin, LLC d/b/a KLT Connect

Filed with the FCC Robocall Mitigation Database pursuant to 47 C.F.R. § 64.6305

Effective Date: September 4, 2026 | Version 1.0

1. Company Information

Legal name	Knox Landin, LLC
Doing business as	KLT Connect
Business address	3115 Northington Court, Suite 138, Florence, AL 35630
Robocall mitigation contact	MOSHIU@KNOXLANDIN.com (256) 712-2287
FCC Registration Number (FRN)	[Enter FRN]
FCC Form 499 Filer ID	[Pending – registration in progress with USAC]
Operating Company Number (OCN)	[Enter OCN or N/A]
Provider type	Non-facilities-based voice service provider (reseller). Originating provider for retail customers; non-gateway intermediate provider for traffic passed to upstream carriers. Knox Landin does not act as a gateway provider and does not accept foreign-originated traffic.
Customers served	Small businesses located in Alabama and the United States
Caller ID authentication status	[Select one: Complete STIR/SHAKEN implementation / Partial implementation / No implementation – relies on upstream carrier attestation]

2. Purpose and Commitment

Knox Landin, LLC, doing business as KLT Connect ("Knox Landin," "the Company," "we"), provides business phone service (VoIP) to small businesses. We buy phone numbers and minutes from upstream carriers and resell that service to our customers. We do not own the underlying network.

Knox Landin is committed to keeping illegal robocalls off the phone network. This document describes the specific, reasonable steps we take to make sure we do not originate, carry, or pass along illegal robocall traffic. It is filed in the FCC Robocall Mitigation Database (RMD) and will be updated within 10 business days whenever any of the information changes.

This program covers every call that originates from a Knox Landin customer and every call that passes through our platform on the way to an upstream carrier. It applies to all of our employees, contractors, and automated systems.

3. Know Your Customer (KYC) – Customer Vetting

We do not turn on service for anyone we cannot identify. Before a new account is activated, Knox Landin collects and reviews:

- The customer's legal business name, physical address, and website (if any).
- The name, phone number, and email of the person responsible for the account.
- A government-issued ID for the account owner and, for business accounts, proof of business registration (Secretary of State filing, EIN letter, or business license).
- A description of how the customer intends to use the service, including expected call volume and whether any outbound calls will be automated or use pre-recorded messages.
- Payment information tied to a verifiable card or bank account. We do not accept anonymous or prepaid-only payment for accounts with outbound calling.

Accounts are reviewed by Company management before activation. We deny service to any applicant that gives false information, cannot be verified, or appears on any industry or government list of known bad actors. High-risk use cases (high-volume outbound dialing, lead generation, debt collection, telemarketing) require written approval from Company ownership and enhanced monitoring.

4. Contract Terms and Acceptable Use Policy

Every customer must agree to Knox Landin's Terms of Service and Acceptable Use Policy (AUP) before service begins. The AUP requires customers to:

- Comply with the Telephone Consumer Protection Act (TCPA), the Truth in Caller ID Act, the TRACED Act, and all FCC rules.
- Never spoof, alter, or misuse caller ID information with intent to defraud, cause harm, or wrongfully obtain anything of value.
- Never place calls that impersonate a government agency, bank, utility, or other business without authorization.
- Use only phone numbers the customer is authorized to use as caller ID.
- Obtain any legally required consent before placing automated or pre-recorded calls.
- Cooperate promptly with any traceback or investigation request.

The AUP gives Knox Landin the right to suspend or terminate service immediately, without refund, if we believe a customer is sending illegal or suspicious traffic.

5. Upstream Carrier Requirements

Knox Landin only routes traffic to and accepts traffic from upstream providers that are listed in the FCC Robocall Mitigation Database. We check the RMD before signing with any new carrier and re-check our existing carriers at least once a year. If a carrier is removed from the RMD, we stop sending traffic to that carrier as required by FCC rules.

Our carrier agreements require the upstream provider to apply STIR/SHAKEN attestation to our calls, participate in traceback, and notify us of any complaints tied to our traffic.

6. Caller ID Authentication (STIR/SHAKEN)

As a non-facilities-based reseller, Knox Landin relies on its upstream carriers to sign calls under the STIR/SHAKEN framework. We confirm that each upstream carrier we use has a certificate from the STI Policy

Administrator and is applying attestation to our traffic. Knox Landin only allows customers to use caller ID numbers that are assigned to them through our platform, which supports the highest attestation level available from our carriers. [If Knox Landin obtains its own SPC token and signs its own calls, this section will be updated within 10 business days.]

7. Call Traffic Monitoring and Analytics

Knox Landin monitors outbound call traffic on its platform to detect patterns that suggest illegal robocalling. Our monitoring looks for:

- Sudden spikes in outbound call volume that do not match the customer's stated use.
- Very short average call durations (for example, large numbers of calls under 6 seconds).
- High percentages of calls that are unanswered, rejected, or answered by voicemail.
- Calls to a large number of unique numbers in a short time window.
- Use of caller ID numbers not assigned to the account.
- Calls to numbers on the Do Not Originate (DNO) list or to known invalid, unallocated, or unassigned numbers.

Accounts that trigger these alerts are reviewed the same business day. Based on the review, we may contact the customer, apply call-rate limits, suspend outbound calling, or terminate the account. We keep a written record of every alert and the action taken.

8. Do Not Originate (DNO) and Call Blocking

Knox Landin blocks outbound calls that use caller ID numbers appearing on an industry Do Not Originate list, including numbers assigned to government agencies and financial institutions that have asked that their numbers never be used for outbound calls. We also block calls using invalid, unallocated, or unassigned North American Numbering Plan numbers as caller ID. These blocks are applied at the platform level and cannot be turned off by the customer.

9. Traceback Cooperation

Knox Landin fully cooperates with the Industry Traceback Group (ITG), the FCC, the FTC, state attorneys general, and law enforcement. We commit to respond to every traceback request within 24 hours of receipt, and sooner when possible. Our response identifies the customer that placed the call and any upstream or downstream provider involved.

Traceback requests should be directed to the robocall mitigation contact listed in Section 1. This mailbox and phone number are monitored during business hours and checked at least once daily on weekends and holidays.

10. Handling Complaints and Illegal Traffic

When we receive a complaint, traceback request, or a notice from the FCC Enforcement Bureau about suspected illegal traffic, we follow these steps:

- Log the complaint and identify the customer account involved within one business day.
- Investigate the customer's traffic, consent records, and stated use case.

- If the traffic appears illegal, suspend outbound calling for that account immediately and give the customer notice.
- Terminate the account if the customer cannot show the traffic is lawful, or if illegal traffic continues.
- Report our findings back to the requesting agency and keep a record of the outcome.

If the FCC Enforcement Bureau notifies Knox Landin that we are carrying illegal traffic, we will investigate and respond within the deadline stated in the notice (currently 14 days) and will block the identified traffic as required.

11. Recordkeeping

Knox Landin keeps the following records for at least two years: customer KYC files, signed AUP agreements, call detail records, monitoring alerts and actions taken, traceback requests and responses, complaints and their resolution, and copies of every RMD filing. Records are stored securely and can be produced to the FCC or law enforcement on request.

12. Training and Annual Review

All employees and contractors who handle customer onboarding, support, or network operations are trained on this program when hired and at least once a year. Company ownership reviews this program annually, or sooner if FCC rules change, and updates it as needed. The RMD filing is updated within 10 business days of any change to the information in this document.

13. Certification

I certify under penalty of perjury that I am an officer of Knox Landin, LLC, that I have read this Robocall Mitigation Program Description, that the information in it is true and correct, and that Knox Landin has implemented the practices described here and will maintain them going forward.

Signature: _____

Name: [Printed name of officer]

Title: [Title]

Company: Knox Landin, LLC d/b/a KLT Connect

Date: _____