

Robocall Mitigation Program

KD Molle Enterprises Inc

FCC Registration Number (FRN): 0038315735

Business Address: 17802 Rose St, Hesperia, CA 92345

Implementation Type: Partial STIR/SHAKEN – Performing Robocall Mitigation

1. Introduction and Purpose

KD Molle Enterprises Inc (“the Company”) is committed to preventing the origination and transmission of illegal robocalls on its network. In compliance with the Pallone-Thune TRACED Act and the requirements set forth by the Federal Communications Commission (FCC) in 47 CFR § 64.6305, this Robocall Mitigation Program outlines the reasonable steps the Company undertakes to avoid originating illegal robocall traffic.

The Company operates as a reseller of wholesale voice services and relies on upstream voice service providers for call authentication under the STIR/SHAKEN framework. This document describes the Company's practices, policies, and procedures to ensure compliance with applicable federal telecommunications law.

2. Scope of Program

This program applies to all outbound voice traffic originated, processed, or transmitted by KD Molle Enterprises Inc, including calls made by its customers through the Company's platform. The program covers both domestic and international calls destined to the United States Public Switched Telephone Network (PSTN).

3. Know Your Customer (KYC) Procedures

The Company performs due diligence on all customers prior to enabling outbound voice services. KYC procedures include:

- Verification of the customer's legal business name, address, and registration documents.
- Collection of a valid Employer Identification Number (EIN) or equivalent foreign business identifier.
- Confirmation of a direct contact name, phone number, and email address for the customer's responsible officer.
- Execution of an Acceptable Use Policy (AUP) in which the customer certifies compliance with all applicable laws, including the TCPA, TSR, DNC Registry, and Truth in Caller ID Act.
- Ongoing monitoring of customer traffic patterns to identify anomalies consistent with illegal robocalling.

4. Call Authentication and STIR/SHAKEN

The Company does not directly control the infrastructure required to sign calls under the STIR/SHAKEN framework. Pursuant to 47 CFR § 64.6301(b), call authentication is performed by the Company's upstream voice service providers, which are FCC-registered and maintain valid SHAKEN certificates. The Company ensures that all outbound traffic is routed exclusively through upstream providers that implement STIR/SHAKEN authentication and are listed in the FCC Robocall Mitigation Database.

5. Traceback Compliance

The Company commits to fully cooperate with the Industry Traceback Group (ITG) administered by USTelecom. Upon receipt of a traceback request, the Company will:

- Acknowledge receipt of the traceback request within 24 hours.
- Identify the originating customer or upstream source of the call in question.
- Provide complete Call Detail Records (CDRs), including originating IP, timestamps, caller ID, and destination number.
- Take immediate corrective action, including suspending or terminating service to customers identified as sources of illegal traffic.
- Retain all traceback-related records for a minimum of two (2) years.

6. Network Monitoring and Enforcement

The Company employs real-time and periodic monitoring of its voice network to detect indicators of illegal robocall traffic, including:

- Abnormally high call volumes from a single source in a short time window.
- Short average call duration (ACD) patterns consistent with automated dialing of uninterested recipients.
- Spoofed or invalid caller IDs not associated with customer accounts.
- Calls to numbers on the National Do-Not-Call (DNC) Registry without documented consent.
- Patterns of customer complaints or analytics flags from downstream carriers.

When suspicious traffic is detected, the Company reserves the right to rate-limit, suspend, or permanently terminate the offending customer account, and to notify upstream providers and the ITG as appropriate.

7. Customer Acceptable Use Policy

All customers of KD Molle Enterprises Inc must execute an Acceptable Use Policy prior to activation. The AUP prohibits the following conduct:

- Origination of illegal robocalls as defined under 47 U.S.C. § 227 and related regulations.
- Caller ID spoofing for fraudulent or harmful purposes in violation of 47 U.S.C. § 227(e).
- Calls to numbers listed on the National DNC Registry without valid prior express written consent or applicable exemption.
- Calls using automatic telephone dialing systems or artificial/prerecorded voices to wireless numbers without consent.
- Any use of the service that violates federal, state, or local law.

8. Record Retention

The Company retains Call Detail Records (CDRs) for all outbound traffic for a minimum of 12 months. Customer onboarding documentation, AUP agreements, and KYC records are retained for the duration of the business relationship plus two (2) years following termination.

9. Program Governance and Point of Contact

This Robocall Mitigation Program is owned and maintained by the Company's executive leadership. The designated point of contact for all robocall mitigation, traceback, and compliance matters is:

Kevin Molle

Chief Executive Officer
KD Molle Enterprises Inc
17802 Rose St, c/o Kevin Molle
Hesperia, CA 92345
Phone: (310) 810-1910
Email: kevin@kdmeinc.com

10. Certification

The undersigned officer of KD Molle Enterprises Inc certifies, under penalty of perjury, that the Company has implemented the Robocall Mitigation Program described herein, that the program is reasonably designed to prevent the origination of illegal robocalls, and that the Company will comply with the requirements of 47 CFR § 64.6305 and respond to all lawful traceback requests in a timely manner.

Signed: Kevin Molle

Title: Chief Executive Officer

Date: April 18, 2026