

ROBOCALL MITIGATION PROGRAM DESCRIPTION

Prepared for FCC Robocall Mitigation Database pursuant to 47 CFR §64.6305

Legal Business Name:	KrosWeb Enterprise Inc. (d/b/a The company)
FCC Registration No. (FRN):	0038588125
Business Address:	111 Embarcadero W, APT 1204, Oakland, CA 94607
Robocall Mitigation Contact:	Joshua Firima Jnr, CEO. joshua@krosai.com
Provider Role:	Voice Service Provider without a STIR/SHAKEN obligation (non-facilities-based reseller)
Effective Date:	June 25, 2026

1. Overview and Provider Role

KrosWeb Enterprise Inc. (“the Company”) provides communications infrastructure for AI-powered voice applications. The platform enables businesses to provision telephone numbers, connect AI agents to public telephone networks, manage voice routing, and access programmable communications services through APIs and web-based tools. For U.S. PSTN connectivity, The company currently utilizes one or more approved upstream providers. The company does not operate as a gateway provider and continuously evaluates upstream providers to support reliability, geographic coverage, and service quality.

2. Caller ID Authentication (STIR/SHAKEN) Status

The company relies on approved upstream providers to perform STIR/SHAKEN authentication for applicable U.S. traffic. Where caller ID authentication is performed by an upstream provider, The company does not independently sign calls. The company maintains policies to ensure traffic is exchanged only with trusted providers implementing applicable caller authentication requirements.

3. Know Your Customer (KYC/KYB)

The Company applies affirmative, effective measures to know its customers and vets and approves each customer before activating service. Because the Company serves a

limited population of business customers using voice service for their own ordinary communications, the Company is able to review each prospective customer individually prior to turn-up. The Company's onboarding diligence includes:

- Collecting and retaining each customer's legal business name, physical business address, and primary contact information prior to activation;
- Verifying the legitimacy of the business and confirming, where appropriate, its good standing and the nature and intended use of the requested service;
- Confirming that the customer's intended traffic is ordinary business voice communication and not high-volume automated or unlawful calling;
- Activating service only after this review is completed satisfactorily; and
- Retaining customer identification and onboarding records consistent with applicable FCC retention requirements.

4. Acceptable Use Policy

Customers are prohibited from originating unlawful robocalls, spoofing caller ID, transmitting fraudulent or deceptive traffic, violating TCPA or other applicable laws, or using The company services for scams, phishing, or International Revenue Share Fraud (IRSF). Violations may result in immediate suspension or permanent termination.

5. Robocall Mitigation Controls

The company implements layered controls including API authentication, account verification, spend controls, rate limiting, velocity monitoring, concurrent call limits, destination restrictions, anomaly detection, and manual review of suspicious activity.

6. Traffic Monitoring

The Company employs a two-layer approach to monitoring the traffic it originates. First, the Company relies on the analytics, alerts, and traceback notices provided by its underlying wholesale provider, which operates the network and observes traffic at carrier scale. Second, the Company conducts its own review of call detail records (CDRs) and call reporting generated by its hosted PBX platform (3CX) to identify anomalies.

Indicators that trigger review include:

- Sudden or unexplained spikes in call volume or short-duration call patterns;
- High volumes of calls with low answer rates or abnormal completion ratios;
- Complaints, traceback notices, or provider alerts indicating suspected illegal traffic; and

- Caller ID values inconsistent with numbers assigned to or authorized for the customer.
- Upon identifying suspicious traffic, the Company investigates promptly and takes appropriate action, up to and including suspension or termination of the offending customer and notification of the Company's underlying provider.

7. Traceback Cooperation (24hr Commitment)

The company will cooperate with lawful traceback requests from the FCC, authorized traceback organizations, law enforcement, interconnected providers, and upstream carriers. Appropriate records will be preserved and mitigation actions taken where necessary.

8. Enforcement and Remediation

Where illegal or suspicious traffic is identified, The company may issue warnings, suspend services, block traffic, terminate customer accounts, and cooperate with providers and authorities to prevent further abuse.

9. Recordkeeping, Updates and Recertification

The Company maintains records of its KYC determinations, traffic-monitoring reviews, and mitigation actions consistent with applicable FCC retention requirements. The Company will update its Robocall Mitigation Database filing within ten (10) business days of any material change to the information contained in this Program, and will recertify its filing annually as required by the Commission's rules.

10. Governance

The Chief Executive Officer is responsible for oversight of this Robocall Mitigation Program. The policy is reviewed periodically to reflect changes in applicable law, network architecture, security controls, and operational practices.

Certification

The information contained in this Robocall Mitigation Program is believed to be true and accurate to the best of the Company's knowledge and is intended to describe the reasonable steps implemented to mitigate illegal robocall traffic in accordance with applicable FCC requirements.