

Konark Telecom LLC

ROBOCALL MITIGATION PLAN FCC COMPLIANCE STATEMENT

1. INTRODUCTION

Konark Telecom LLC submits this Robocall Mitigation Plan in compliance with 47 CFR § 64.6300 et seq. This Plan outlines the policies, procedures, and technical measures implemented to prevent the origination and transmission of illegal robocalls on its network.

2. SCOPE OF SERVICES

The Company provides interconnected VoIP and related telecommunications services. This Plan applies to all voice traffic originating, transiting, or terminating on the Company's network, including retail and wholesale services.

3. ZERO-TOLERANCE POLICY

The Company maintains a zero-tolerance policy prohibiting illegal robocalls, caller ID spoofing, traffic pumping, and violations of the Telephone Consumer Protection Act (TCPA). Any violations may result in immediate suspension or termination of service.

4. CUSTOMER DUE DILIGENCE (KYC)

Prior to onboarding, the Company requires verification including corporate formation documents, identification of responsible parties, beneficial ownership disclosure, campaign descriptions, proof of consent, TCPA policies, dialing platform information, and proof of number authorization. Enhanced due diligence applies to high-risk customers.

5. STIR/SHAKEN IMPLEMENTATION

The Company has fully implemented STIR/SHAKEN authentication across all IP-based voice traffic in accordance with 47 CFR § 64.6301. The Company assigns the highest level of attestation (A-level) where it has verified the customer and their right to use the telephone numbers. Non-IP traffic is subject to additional mitigation measures.

6. CALL AUTHENTICATION AND NUMBERING CONTROLS

Caller ID information must correspond to valid, assigned, or authorized telephone numbers. The Company blocks calls with invalid, unallocated, or unauthorized numbers and prohibits caller ID manipulation without prior approval.

7. TRAFFIC MONITORING AND ANALYTICS

The Company employs traffic monitoring systems and analytics tools to detect suspicious calling patterns, including high-volume anomalies and potential robocall activity. Identified risks are investigated promptly.

8. TRACEBACK COOPERATION

The Company responds to traceback requests within 24 hours and cooperates with the Industry Traceback Group (ITG), federal and state agencies, and law enforcement. Confirmed illegal traffic is immediately blocked.

9. MITIGATION AND ENFORCEMENT

The Company implements mitigation actions including call blocking, traffic restrictions, and suspension or termination of services where unlawful activity is identified.

10. COMPLIANCE GOVERNANCE

The Company has designated a Robocall Mitigation Officer responsible for overseeing compliance, conducting audits, maintaining policies, and ensuring staff training.

11. RECORD RETENTION

The Company retains records for a minimum of five (5) years, including customer onboarding data, traffic analytics, traceback responses, and enforcement actions.

12. FCC CERTIFICATION

The Company certifies that it has fully implemented STIR/SHAKEN and has established robocall mitigation practices for any non-IP or unsigned traffic, in accordance with FCC requirements.

13. CONTINUOUS COMPLIANCE

The Company continuously monitors regulatory developments and updates its robocall mitigation practices to remain compliant with FCC rules and industry standards.