

ROBOCALL MITIGATION PROGRAM (RMP)

FCC Robocall Mitigation Database Submission

Holding Company: Zoiko Communications Group Inc

Operating Entities: GoLite Mobile Inc; Zoiko Mobile Inc; DriverX Mobile Inc

Program Owner: Compliance & Network Integrity Division

Effective Date: 01/01/2026

1. Corporate Structure and Program Scope

Zoiko Communications Group Inc is the telecommunications holding company responsible for governance, compliance oversight, and network integrity policies across its telecommunications subsidiaries.

This Robocall Mitigation Program applies to the following entities:

- GoLite Mobile Inc
- Zoiko Mobile Inc
- DriverX Mobile Inc

All telecommunications services delivered through these subsidiaries operate under a centralized compliance, monitoring, and mitigation infrastructure.

2. Program Purpose

The purpose of this Robocall Mitigation Program is to prevent illegal robocalls, spoofed caller identification, and fraudulent voice traffic from entering or originating on the Company's network.

The Company maintains a zero-tolerance policy toward illegal robocalling.

3. Regulatory Compliance Framework

This program is designed to comply with guidance from the Federal Communications Commission Robocall Mitigation Database requirements and associated caller authentication frameworks.

The program also supports compliance with United States consumer protection regulations including the Telephone Consumer Protection Act (TCPA) and the Truth in Caller ID Act.

4. Network Integrity Commitment

Zoiko Communications Group Inc is committed to maintaining the integrity and reliability of the telecommunications ecosystem.

Illegal robocalls undermine consumer trust and harm legitimate telecommunications providers. Accordingly, the Company has implemented technical, operational, and compliance safeguards designed to prevent abuse of its network.

5. Governance and Compliance Oversight

The Robocall Mitigation Program is administered by the Compliance and Network Integrity Division.

Responsibilities include:

- implementation of mitigation policies
- oversight of customer onboarding procedures
- monitoring traffic analytics
- investigation of suspicious calling activity
- regulatory reporting and traceback responses

6. Network Role Classification

Depending on traffic flow, the network may operate in one or more roles within the U.S. voice ecosystem:

- originating service provider
- wireless MVNO operator
- wholesale VoIP provider
- intermediate carrier
- international gateway provider

7. Know Your Customer (KYC) Procedures

All customers must undergo identity verification before telecommunications services are activated.

Required documentation may include:

- legal business registration
- tax identification number
- verified business address
- authorized corporate signatories

8. Customer Traffic Profile Assessment

Customers must disclose intended telecommunications usage including:

- anticipated call volumes
- typical call duration
- geographic distribution of calls

This information establishes a baseline traffic profile used for monitoring and anomaly detection.

9. High-Risk Industry Controls

Industries historically associated with robocall abuse may be subject to enhanced due diligence.

Examples include telemarketing operations, lead generation campaigns, debt collection agencies, and financial solicitation services.

10. Carrier Partner Due Diligence

The Company performs due diligence on upstream and downstream carrier partners to ensure traffic integrity.

Carrier relationships may be suspended if traffic integrity concerns arise.

11. Traffic Monitoring Systems

Automated monitoring systems continuously analyze network traffic patterns.

Indicators monitored include:

- abnormal spikes in call volume
- excessive short-duration calls
- unusually high call failure rates
- sequential dialing patterns

12. Traffic Reputation Scoring

Customer traffic may be assigned internal risk scores based on historical behavior, complaint patterns, and call completion metrics.

13. Consumer Complaint Monitoring

The Company monitors consumer complaints related to robocalls associated with its network and analyzes complaint trends to identify potential robocall activity.

14. Mitigation and Enforcement Procedures

When suspicious traffic is detected, the Company may:

- throttle call traffic
- block call routes
- suspend customer accounts
- terminate service agreements

All mitigation actions are documented.

15. STIR/SHAKEN Caller Authentication

The Company supports the STIR/SHAKEN caller authentication framework across IP-based portions of its network.

16. STIR/SHAKEN Governance

Operational controls govern certificate management, authentication policy enforcement, and monitoring of attestation accuracy.

17. International Gateway Safeguards

Where the Company handles international traffic entering the United States network, additional safeguards and monitoring controls are implemented.

18. Sub-Provider Oversight

Customers that resell telecommunications services must implement their own robocall mitigation procedures and comply with applicable regulatory requirements.

19. Network Security Controls

Additional safeguards include SIP signalling validation, caller ID verification, rate limiting on new accounts, and automated blocking of known scam patterns.

20. Recordkeeping

The Company maintains documentation supporting robocall mitigation activities including onboarding records, traffic monitoring logs, compliance investigations, and traceback responses.

21. Staff Training

Technical and compliance personnel receive regular training on robocall mitigation procedures and regulatory obligations.

22. Continuous Program Improvement

The Robocall Mitigation Program is periodically reviewed and updated to address evolving threats and regulatory developments.

Executive Certification

Zoiko Communications Group Inc certifies that it has implemented the robocall mitigation procedures described in this document and takes reasonable steps to prevent illegal robocalls from originating on or transiting its network.

Certified by:

Lennox G. McLeod

President

Zoiko Communications Group Inc

Date: 03/13/2026