

DIGIVOICE, LLC

ROBOCALL MITIGATION PLAN

Effective Date: February 23, 2026

1. Purpose and Overview

Digivoice, LLC ("Digivoice") is committed to preventing the origination and transmission of illegal robocalls on its network. This Plan describes the policies, procedures, and technical controls Digivoice uses to identify, investigate, mitigate, and prevent unlawful calling behavior.

Digivoice has implemented STIR/SHAKEN in the IP portions of its network and maintains mitigation procedures consistent with FCC requirements and industry best practices. Digivoice leverages third-party analytics through TransNexus to continuously monitor outbound traffic and enforce threshold-based robocall mitigation controls.

2. STIR/SHAKEN and Caller ID Authentication

Digivoice supports SIP call authentication consistent with FCC rules and industry standards.

Digivoice attests calls only for authorized subscribers and validated calling numbers. Unauthorized or unvalidated numbers may be blocked or rejected.

3. Know Your Customer (KYC)

Digivoice conducts identity verification and risk assessment prior to enabling outbound calling.

Verification may include legal business name, EIN validation, business registration confirmation, website validation, intended use case confirmation, risk scoring, and screening for high-risk categories.

Subscriber profiles may be re-evaluated upon material traffic changes, complaint activity, or traceback inquiries.

4. Continuous Traffic Monitoring and Analytics (TransNexus)

Digivoice deploys the TransNexus ClearIP analytics platform as its third-party analytics provider to continuously monitor and score outbound traffic in real time.

The platform applies industry-recognized thresholds including call velocity, ASR anomalies, call duration distribution, and destination diversity.

Traffic exceeding defined risk thresholds may be automatically flagged, rate-limited, blocked, or suspended pending review. Alerts are reviewed promptly within 24 hours.

Thresholds and enforcement logic may be periodically reviewed and adjusted in coordination with industry best practices and analytics provider guidance.

5. Investigation and Enforcement

Suspicious traffic may trigger investigation including review of call records and account history.

Digivoice may contact subscribers for clarification, apply mitigation controls, rate-limit traffic, suspend service, or terminate service for confirmed violations.

Enforcement actions are documented to support compliance and traceback obligations.

6. Blocking and Do-Not-Originate Controls

Digivoice implements blocking controls and may apply Do-Not-Originate lists when available through recognized authorities.

Confirmed illegal robocall traffic is blocked at the network level, and repeat violations may result in permanent service termination.

7. Traceback Cooperation

Digivoice cooperates with the Industry Traceback Group (ITG), upstream providers, and regulatory agencies.

Traceback requests will be responded to within 24 hours.

8. Upstream Providers and Compliance Posture

Digivoice utilizes upstream providers including Bandwidth Inc., Twilio Inc., and Telnyx LLC.

These providers are selected based on participation in robocall mitigation initiatives, STIR/SHAKEN implementation, and cooperation with traceback efforts.

Digivoice coordinates with upstream providers on mitigation and enforcement when suspicious traffic is identified.

9. Plan Governance and Updates

This Plan is reviewed periodically and updated as necessary to reflect evolving FCC guidance and industry best practices.

Digivoice will update its Robocall Mitigation Database filing within 10 days of any changes to the information contained in this Plan.

10. Certification

I, Brady Miller, CEO of Digivoice, LLC, certify under penalty of perjury that this Plan accurately describes Digivoice's procedures and that STIR/SHAKEN has been implemented in the IP portions of its network in accordance with applicable requirements.

Signed: _____

Brady Miller, CEO

Date: _____