

LoopUp LLC — Robocall Mitigation Plan (FCC RMD)

Effective date: 12 Jan 2026 | Version: 2026.1 | Submitted by: LoopUp LLC

1. Provider Identification

Legal entity: LoopUp LLC

Operating Company Number (OCN): 302L

FRN: 0018162040

Primary website: <https://loopup.com>

24x7 abuse/traceback contact: support@loopup.com

2. Overview & Scope

This Robocall Mitigation Plan describes the controls, monitoring, authentication, and response practices LoopUp LLC applies to all outbound voice traffic that we originate to the United States public telephone network. We implement STIR/SHAKEN end-to-end using provider-owned certificates and independent attestation decisions, and we maintain a robocall mitigation program for any traffic not eligible for cryptographic authentication (e.g., non-IP legs).

3. STIR/SHAKEN Implementation

- **Certificate Ownership & SPC:** LoopUp obtains and manages its own SHAKEN certificates through the STI-PA/CA. Certificates are scoped to LoopUp's SPC/OCN 302L and maintained in an HSM/KMS with enforced key-management policies.
- **Independent Attestation Decisions:** The originating service provider (OSP) makes per-call A/B/C attestation decisions based on customer vetting, TN provenance, and call path. A-level is applied when caller identity/TN control are fully verified; B-level when partial; C-level for gateway scenarios when the caller identity cannot be sufficiently verified.
- **PASSporT Creation & Header Integrity:** For SIP traffic terminating in the US, LoopUp signs PASSporTs at the originating SBC/Application Server and ensures header integrity across interconnects. We monitor downstream verification outcomes with participating TSPs and remediate routing or attestation rules if verification failure rates exceed thresholds.

- Certificate Lifecycle: Certificates are inventoried, monitored for expiry, renewed ahead of time, and rotated per policy. CRL/OCSP checks are performed; compromised or deprecated keys trigger immediate revocation and incident response.

4. Robocall Mitigation Program (Non-IP & General Controls)

For traffic not eligible for SHAKEN authentication (e.g., TDM interconnects), LoopUp applies layered controls:

- Behavioral analytics (fraud/spam detection), anomaly scoring, call-velocity and pattern analysis
- Caller ID validation and number association checks; business number verification and registration
- Complaint-driven tuning and manual review workflows; dynamic blocking or rate-limiting of abusive traffic
- Subscriber notification and Caller ID Name override to warn end users of suspicious calls, where applicable

5. Know-Your-Customer (KYC) & Customer Vetting

Prior to enabling origination and A-level attestation, LoopUp verifies enterprise identity, business legitimacy, number right-to-use, and declared call use-cases. Vetting evidence includes legal identity records, TN assignment/LOA, and review of display identity content. High-risk use-cases are subject to enhanced due diligence and ongoing monitoring.

6. Blocking & Enforcement Policy

Any call suspected to be fraudulent, abusive, or illegal is subject to inspection, temporary suspension, blocking, and account review. Repeat or egregious violations result in disconnection and referral to enforcement authorities. Our Terms of Use communicate these conditions to customers.

7. Traceback Cooperation

LoopUp responds to traceback requests from the FCC, law enforcement, and the registered traceback consortium. We maintain logs sufficient to identify origination source, signing status, attestation, and routing metadata; we provide responses within defined SLAs.

8. Complaints & Remediation

We operate a complaint intake channel (abuse/security mailbox and phone), triage allegations within one business day, and apply corrective actions: content review, customer outreach,

temporary suspension, number re-assignment blocks, and CAPA. Complaint trends feed quarterly tuning of analytics and attestation policies.

9. Monitoring, Metrics & Audits

We monitor verification success rates with TSPs, attestation mix, signing error rates, complaint volumes, and traceback SLAs. Evidence and artifacts are retained per policy for audit. We perform pre-audit assessments and support annual audits of our STIR/SHAKEN implementation and mitigation program.

10. Recordkeeping

Artifacts retained include: certificate inventories and rotation logs; PASSporT samples; attestation rules; KYC packages; complaint and traceback logs; analytics reports; and policy/ToU acknowledgements. Retention follows our compliance schedule; evidence is accessible for audit.

11. RMD Certification Summary

LoopUp implements STIR/SHAKEN across all eligible SIP traffic we originate to the United States. We own and manage our SHAKEN certificates (OCN 302L) and make independent attestation decisions (A/B/C) per policy. For any traffic not eligible for cryptographic authentication, we operate a robocall mitigation program comprising KYC, behavioral analytics, complaint handling, traceback participation, and enforcement. We respond to traceback requests and law-enforcement inquiries within defined SLAs, and we retain evidence sufficient for audit.

12. Contacts

Regulatory contact: Andrew Bunyan, Andrew.bunyan@loopup.com

Technical/STIR-SHAKEN contact: Michael Wellington, VP Voice Architecture,
michael.wellington@loopup.com

24x7 security/abuse contact: support@loopup.com