

VAULTCOM NETWORKS INCORPORATED

ROBOCALL MITIGATION PLAN

Updated to Reflect Current FCC Robocall Mitigation Database (RMD) Requirements – 2026

I. Regulatory Background and Compliance Commitment

VaultCom Networks Incorporated (“VaultCom”) complies with 47 C.F.R. § 64.6305 and related FCC Orders requiring all voice service providers to file and maintain accurate certifications in the FCC’s Robocall Mitigation Database (RMD).

VaultCom certifies that it has fully implemented STIR/SHAKEN authentication in compliance with 47 C.F.R. § 64.6301 and that all calls originated, carried, or processed on its network are subject to an active robocall mitigation program.

VaultCom commits to maintaining accurate and timely RMD filings and updating its certification upon any material change in mitigation practices or network operations.

II. Scope of Mitigation Program

VaultCom’s mitigation program addresses unlawful calls prohibited under:

- 47 U.S.C. § 227(b) (TCPA autodialed/artificial or prerecorded voice calls)
- 47 U.S.C. § 227(e) (Truth in Caller ID Act – spoofing violations)

The program applies reasonable measures to detect, prevent, and remediate traffic reasonably suspected of violating federal law.

III. STIR/SHAKEN Implementation

VaultCom has fully implemented STIR/SHAKEN authentication across its IP network.

- All outbound IP-originated calls are signed.
- Appropriate attestation levels (A, B, or C) are applied.
- Active SPC token registration and certificate management are maintained.
- Unsigned traffic is subject to enhanced monitoring.

IV. Know Your Customer (KYC) Program

VaultCom maintains a documented KYC onboarding framework including:

- Verification of legal identity and business registration
- Intended use case documentation
- Caller ID and numbering validation
- Ongoing monitoring and periodic review of high-volume customers

Unlawful telemarketing, spoofing, scam campaigns, or fraudulent activity is strictly prohibited.

V. Know Your Upstream Provider (KYUP)

VaultCom conducts due diligence on upstream carriers including:

- Verification of RMD listing
- Confirmation of STIR/SHAKEN implementation
- Contractual mitigation obligations review

Traffic will not be routed through providers removed from the FCC RMD.

VI. Call Analytics and Traffic Monitoring

VaultCom employs layered monitoring controls including analysis of:

- High call volumes
- Short-duration patterns
- Abnormal ASR metrics
- Traffic bursts inconsistent with stated use cases

Suspicious traffic is investigated, suspended if necessary, and terminated if violations are confirmed.

VII. Traceback Cooperation Commitment

VaultCom commits to responding within 24 hours to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group.

VaultCom maintains accurate call detail records and dedicates sufficient compliance resources to ensure timely cooperation.

VIII. Recordkeeping and Documentation

VaultCom maintains documentation supporting:

- KYC procedures
- STIR/SHAKEN implementation
- Traffic analytics policies
- Enforcement actions
- Traceback responses

Records are retained consistent with regulatory requirements.

IX. Acceptable Use Policy (AUP) Enforcement

VaultCom's Acceptable Use Policy prohibits:

- Unlawful telemarketing
- Artificial/prerecorded voice campaigns without consent
- Caller ID spoofing
- Fraudulent schemes

Violations result in suspension or termination of service.

X. Ongoing Compliance and Certification

VaultCom acknowledges that RMD certifications must remain accurate and that false or incomplete filings may result in FCC enforcement action.

A designated compliance officer is responsible for regulatory oversight and RMD accuracy.

Certification

I certify under penalty of perjury that the foregoing Robocall Mitigation Plan is accurate and complete to the best of my knowledge and reflects the active compliance program of VaultCom Networks Incorporated.

Authorized Representative: *Radanga*
Rodel Danga
Title: President
Date: February 18, 2026