ROBOCALL MITIGATION PLAN (RMP)
NETVOICELINK

FCC RMD Filing Type: Voice Service Provider
Effective Date: March 17, 2026

---

1. COMPANY COMMITMENT & INTRODUCTION

NETVOICELINK is committed to full compliance with all Federal Communications Commission (FCC) regulations regarding robocall mitigation, caller ID authentication, and telecommunications network integrity.

This Robocall Mitigation Plan outlines the technical, operational, and procedural controls implemented by NETVOICELINK to prevent illegal robocalls and maintain compliance with FCC Robocall Mitigation Database (RMD) requirements effective February 5, 2026.

---

2. REGULATORY COMPLIANCE FRAMEWORK

NETVOICELINK complies with all FCC robocall mitigation and RMD obligations, including the following 2026 regulatory requirements:

- RMD updates required within 10 days of any change
- Annual RMD recertification due March 1 each year
- Mandatory accuracy and completeness of all submissions
- Enforcement penalties:
    - $10,000 per inaccurate or false filing
    - $1,000 per delayed update violation
- Multi-Factor Authentication (MFA) required for RMD access
- Mandatory blocking of traffic from non-listed RMD entities
- Risk of removal from RMD for non-compliance

NETVOICELINK maintains internal compliance controls to ensure continuous adherence to these requirements.

---

3. STIR/SHAKEN IMPLEMENTATION

NETVOICELINK has fully implemented the STIR/SHAKEN framework:

- Utilizes third-party SPC token and certificate authority

- Applies appropriate attestation levels to outbound calls
- Ensures caller ID authentication in compliance with FCC standards

---

4. KNOW YOUR CUSTOMER (KYC) PROGRAM

NETVOICELINK maintains a strict Know Your Customer (KYC) program to ensure all clients are properly verified before accessing services.

4.1 Identity Verification

- Business registration validation
- Government-issued ID verification (where applicable)
- Physical address confirmation

4.2 Fraud & Risk Screening

- Screening against fraud and scam databases
- Blacklist and reputation checks
- Detection of suspicious identity patterns

4.3 Risk Assessment

- Customer risk scoring prior to onboarding
- Classification based on usage patterns and traffic profile
- Enhanced due diligence for high-risk users or traffic routes

4.4 Account Approval Controls

- No service activation without successful KYC completion
- Manual compliance review for flagged applicants
- Final approval required before activation

4.5 Purpose of KYC

The KYC program ensures:

- Prevention of illegal robocall abuse
- Verification of legitimate business users
- Compliance with FCC RMD obligations
- Protection of network integrity and trust

---

5. ROBOCALL MITIGATION CONTROLS

NETVOICELINK implements layered mitigation controls as follows:

5.1 Traffic Monitoring & Analytics

- Continuous real-time monitoring of call traffic
- Detection of abnormal spikes or suspicious patterns
- Automated alerts for investigation

5.2 Call Blocking & Filtering

NETVOICELINK blocks:

- Spoofed or invalid caller IDs
- Known scam and robocall sources
- Suspicious or malicious traffic identified via analytics

5.3 Traceback Cooperation

- Responds to traceback requests within 24 hours
- Works with industry traceback organizations and regulators
- Maintains detailed investigative logs

5.4 Enforcement Actions

- Immediate suspension of suspicious accounts
- Formal investigation procedures
- Permanent termination for confirmed violations

---

6. NETWORK SECURITY SAFEGUARDS

- Secure SIP signaling protocols
- Prevention of unauthorized traffic injection
- Fraud detection and rate-limiting systems

---

7. RMD DATA INTEGRITY & MAINTENANCE

- Ensures all RMD data is accurate and up to date
- Updates submitted within 10 business days of any change

- Regular internal compliance audits
- Annual recertification completed before March 1 deadline

---

8. COMPLIANCE GOVERNANCE

NETVOICELINK maintains a structured compliance framework:

- Designated Compliance Officer
- Internal audits and monitoring
- Staff training on FCC regulations
- Documented enforcement and mitigation procedures

---

9. RECORDKEEPING & DOCUMENTATION

NETVOICELINK retains the following records:

- Customer onboarding and verification data
- Call Detail Records (CDRs)
- Network and traffic monitoring logs
- Incident and enforcement reports

All records are maintained in compliance with FCC requirements and made available upon request.

---

10. THIRD-PARTY OVERSIGHT

- Ensures all partners comply with FCC regulations
- Maintains written agreements for authentication providers
- Monitors upstream and downstream traffic sources

---

11. CERTIFICATION STATEMENT

NETVOICELINK certifies that:

- A full robocall mitigation program is implemented and operational
- All RMD submissions are accurate, complete, and truthful

- Required updates and annual recertifications will be performed on time

---

12. COMPANY CONTACT INFORMATION

Company Name: NETVOICELINK
Contact Name: Suzanne Marie Oviett
Phone: +1 646 980 5496
Email: Suzanne@netvoicelink.com
Website: www.Netvoicelink.com

---

13. CONCLUSION

NETVOICELINK is committed to preventing illegal robocalls and maintaining full compliance with FCC regulations. This Robocall Mitigation Plan will be continuously updated to reflect regulatory changes and evolving industry standards.