

SignalForge Networks

RMDB Plan

1. Purpose and Scope

Objective: Prevent our network from originating, carrying, or terminating illegal robocalls (including spoofed, unsolicited, or fraudulent calls in violation of TCPA, Truth in Caller ID Act, and FCC rules).

Scope: Applies to all voice services we provide or facilitate, including origination, termination, transit, and any interconnected VoIP traffic.

Commitment: We will not knowingly originate or transmit illegal robocall traffic and will take reasonable steps to identify, block, and mitigate such traffic.

2. Organizational Responsibilities

Robocall Mitigation Team:

Designated Compliance Officer: Gabriel Izard (engineering, operations, legal/compliance).

Training: Annual training for relevant staff on robocall indicators, FCC rules, and internal procedures.

Monitoring & Reporting: Monthly reviews of mitigation effectiveness; immediate escalation for high-risk incidents.

3. Key Mitigation Technologies & Practices

Implement a layered approach combining authentication, analytics, and blocking:

Caller ID Authentication (STIR/SHAKEN):

If subject to full implementation: Use our own SPC token and certificate (no

outsourcing attestation decisions post-September 2025 rules).

Attest calls per ATIS standards (A = full authentication, B = partial, C = gateway/no auth).

For non-full implementation providers: Certify partial/complete status or alternative mitigation in RMD.

Display verified caller name/info on terminating calls when A-level attestation is received (per ongoing proposals).

Call Traffic Analysis & Analytics:

Real-time monitoring for patterns: high call volumes/short duration, sequential dialing, invalid numbers, high-risk prefixes.

Use AI/ML-based anomaly detection for spam/scam signatures.

Reputation scoring of originating numbers (integrate lists like Do Not Originate, known spam databases).

Blocking & Filtering:

Immediate block of traffic from providers not listed in the FCC Robocall Mitigation Database.

Block invalid numbers (unallocated, disconnected).

Block known robocall patterns (e.g., >X calls/minute per number).

Honor government traceback requests within 24 hours.

Traceback Participation:

Respond fully and promptly to all FCC/government traceback requests.

Maintain logs for traceability (caller ID, origination point, timestamps).

Customer/Subscriber Protections:

Offer call-blocking/labeling tools to end users.

Educate customers on reporting suspicious calls.

Third-Party Traffic Management:

Contractual requirements with upstream/downstream partners to comply with FCC rules.

Reject traffic from non-RMD-listed entities.

Monitor and audit partners.

4. Ongoing Monitoring, Review & Updates

Metrics tracked:

Volume/percentage of blocked illegal traffic.

Traceback response times.

Customer complaints related to unwanted calls.

Review cadence: Quarterly internal audits; annual full plan review.

Updates: Revise plan within 10 business days of material changes (e.g., new tech, regulatory updates); refile in RMD as required.

Continuous improvement: Incorporate FCC guidance/best practices (expected from Wireline Competition Bureau in 2026), industry threat intelligence, and evolving scam tactics.

5. Compliance & Enforcement Readiness

RMD Filing:

Maintain current, accurate certification in the Robocall Mitigation Database.

Include detailed description of above practices (avoid generic/vague language — FCC penalizes deficient plans heavily in 2025–2026).

Update within 10 business days of changes.

Use secure access (moving toward 2FA/multifactor per 2026 rules).

Recordkeeping: Retain evidence (logs, configs, contracts) for audits/enforcement.

Consequences of non-compliance: We understand that inaccurate filings can lead to removal from RMD, traffic cutoff, and substantial fines (higher base fines effective February 2026).

6. Additional Best Practices

Proactively report deficient upstream providers via FCC mechanisms.

Participate in industry efforts (e.g., call authentication extensions to international gateways).

Stay current with FCC dockets (e.g., proposals on foreign-originated calls, branded calling enhancements).

Conduct periodic penetration testing / red-team exercises for spoofing vulnerabilities.