

Robocall Mitigation Plan

NexDial Communication LLC

Prepared for RMD Filing

This plan establishes NexDial Communication LLC's documented approach to preventing, detecting, investigating, and mitigating illegal robocall traffic. It is structured for the FCC Robocall Mitigation Database framework and 47 CFR § 64.6305.

1. Executive Summary

NexDial Communication LLC maintains a structured Robocall Mitigation Program designed to protect consumers, preserve the integrity of voice communications, and reduce the risk that its services are used to originate, carry, or process illegal robocall traffic.

The program is built around customer and upstream-provider controls, call authentication and caller-ID integrity, traffic analytics and detection, blocking and incident response, consumer complaint handling, and documented regulatory cooperation.

2. Regulatory Alignment

NexDial's RMD program is designed around the FCC framework requiring covered voice-service providers to maintain a robocall mitigation program and describe the specific reasonable steps used to mitigate illegal robocalls.

- Maintain a written robocall mitigation program appropriate to NexDial's actual role in the voice-call chain.
- Apply reasonable controls to prevent illegal robocall traffic from entering or moving through NexDial's services.
- Maintain customer and upstream-provider controls appropriate to the risk of the services provided.
- Use analytics, monitoring, authentication, and blocking controls where applicable to NexDial's network architecture.
- Maintain a documented traceback process with a commitment to respond fully within 24 hours.
- Review and update this plan when material changes occur.

3. Program Governance & Accountability

Function	Responsibility
Program Owner	NexDial management / designated compliance owner
Traceback Response	Designated compliance or network-response contact
Technical Review	Designated telecom/network operations lead
Customer Risk Review	Designated onboarding/compliance reviewer
Escalation	Compliance → Network Operations → Management

4. Customer & Upstream Provider Controls

NexDial will use a risk-based onboarding and monitoring process to reduce the likelihood that customers or upstream providers use its services for illegal robocall campaigns.

- Collect and retain sufficient customer identification and contact information before enabling applicable voice services.
- Review the customer's intended use, business purpose, expected traffic patterns, and calling model.
- Require customers to agree to applicable acceptable-use and anti-illegal-traffic requirements.
- Review unusual, high-volume, rapidly changing, or elevated-risk traffic.
- Maintain records identifying relevant upstream providers and traffic relationships.
- Suspend, restrict, or terminate traffic when investigation reasonably indicates illegal activity or a material policy violation.

5. Call Authentication & Caller-ID Integrity

NexDial will use applicable caller-ID authentication and verification controls consistent with its actual service role and network architecture. Any STIR/SHAKEN status reported in the FCC filing must be verified before certification.

- Maintain controls designed to reduce unauthorized caller-ID spoofing.
- Use STIR/SHAKEN where applicable to NexDial's network and regulatory role.
- Monitor authentication-related anomalies and suspicious caller-ID patterns.
- Restrict traffic that fails required identity or authorization checks.
- Coordinate with relevant upstream or downstream providers when caller-ID integrity concerns arise.

6. Robocall Detection, Analytics & Blocking

NexDial will maintain monitoring and analytics appropriate to the scale and architecture of its voice services to identify traffic patterns reasonably indicative of illegal robocall activity.

- Monitor abnormal call-volume spikes and unusual destination patterns.
- Evaluate short-duration, high-frequency, or other suspicious calling behavior.
- Use internal or third-party analytics where appropriate.
- Maintain configurable risk thresholds and periodically review their effectiveness.
- Block, throttle, quarantine, or otherwise restrict high-risk traffic when justified.
- Use human review and exception procedures where appropriate to reduce false positives.
- Document material mitigation actions and the reasons for intervention.

7. Consumer Protection & Complaint Handling

- Maintain a documented channel for receiving reports of unwanted, spoofed, or suspicious calls.
- Log material complaints and preserve relevant information where available.
- Prioritize reports involving coordinated campaigns, spoofing, impersonation, fraud, or high-volume calling.
- Investigate credible complaints and correlate them with customer and traffic records.
- Escalate confirmed or high-confidence illegal activity for immediate mitigation.
- Use complaint trends to improve monitoring, customer review, and risk controls.

8. Traceback Response & Cooperation

24-Hour Traceback Commitment

NexDial Communication LLC commits to respond fully and within 24 hours to traceback requests from the FCC, law enforcement, and the registered industry traceback consortium, and to cooperate in investigating and stopping illegal robocall traffic using NexDial's services.

- Maintain a monitored contact for traceback requests.
- Treat traceback requests as priority compliance events.
- Identify relevant customer, routing, account, and call-detail information available to NexDial.
- Provide a complete response within the required 24-hour window.
- Escalate urgent matters to management and technical personnel.
- Document the request, investigation, response, and mitigation steps.

9. Illegal Robocall Incident Response

Stage	Action	Objective
Detect	Identify suspicious traffic through analytics, complaints, traceback, partner notices, or internal review.	Early identification
Validate	Review customer identity, traffic behavior, caller-ID information, routing, and records.	Reduce false positives
Contain	Apply blocking, throttling, suspension, quarantine, or other controls.	Stop harmful traffic
Investigate	Determine source, scope, duration, and mechanism.	Establish facts
Remediate	Correct configuration, update controls, educate customer, or terminate service.	Prevent recurrence
Document	Preserve an incident record with dates, findings, and actions.	Create audit trail
Learn	Use material incidents to improve controls.	Continuous improvement

10. Records, Evidence & Retention

- Customer onboarding and verification records.
- Customer agreements and applicable acceptable-use restrictions.
- Upstream-provider identification and due-diligence records.
- Material alerts, investigations, blocks, suspensions, and remediation actions.
- Traceback requests and responses.
- Material consumer complaint investigations.
- Periodic compliance reviews and plan updates.
- Evidence supporting FCC RMD certification statements, including technical/STIR-SHAKEN information where applicable.

11. Monitoring, Testing & Continuous Improvement

- Periodically review customer-risk controls and high-risk traffic patterns.
- Review analytics thresholds and blocking rules for effectiveness.
- Test traceback escalation so responsible personnel can respond within 24 hours.
- Review material incidents and update procedures when weaknesses are identified.

- Review this plan at least annually and after material changes to services, network architecture, providers, or FCC requirements.

12. Implementation & Compliance Calendar

Phase 1 — Establish: Confirm service role, network architecture, customer controls, upstream-provider inventory, and traceback contacts.

Phase 2 — Deploy: Enable and validate applicable authentication, analytics, monitoring, alerting, and blocking controls.

Phase 3 — Test: Conduct operational tests for suspicious traffic and traceback response; document results.

Phase 4 — Certify: Verify RMD information, technical status, plan accuracy, and authorized certification before filing.

Ongoing: Monitor traffic, investigate incidents, maintain evidence, respond to traceback, and update the program.

13. Pre-Filing RMD Certification Checklist

- Confirm the legal name and FCC/CORES identifying information are accurate.
- Confirm the company's FCC FRN and filing identifiers.
- Confirm NexDial's applicable provider role(s).
- Confirm actual STIR/SHAKEN implementation status and any applicable exemption or extension.
- Confirm the plan accurately describes NexDial's real customer, upstream-provider, analytics, and mitigation controls.
- Confirm the 24-hour traceback process and monitored contact are operational.
- Confirm the final RMD information is complete and internally reviewed.
- Obtain approval from an appropriately authorized individual.
- Retain a final copy of the submitted certification and supporting records.

14. Management Review & Approval

The undersigned acknowledges that this plan is intended to describe NexDial Communication LLC's robocall mitigation controls for RMD purposes and that the final FCC certification should be submitted only after verification of the accuracy of all statements and technical classifications.

Appendix — Regulatory Reference Notes

This plan is structured around the FCC Robocall Mitigation Database framework and is intended to document specific reasonable measures used to mitigate illegal robocall traffic. The plan should be reviewed against NexDial's actual FCC filing classification and technical deployment before certification.

The supplied Infinityconnect Robocall Mitigation Program was used only as a structural reference for requested mitigation topics. This document was written specifically for NexDial Communication LLC and does not reproduce Infinityconnect's company information.