

NEXDIAL INC.

Robocall Mitigation Program Description

Prepared for review in connection with an FCC Robocall Mitigation Database (RMD) filing

Legal entity	NexDial Inc.
Business address	6844 Bardstown Rd, Louisville, KY 40291, USA
Website	https://www.nexdial.us
Robocall mitigation contact	Mario Gobran, Compliance Contact mario.gobran@nexdial.us +1 806 602 4040
Version / status	October 22, 2026

1. Purpose and scope

This program is designed to reduce the risk that NexDial Inc. voice services or traffic under its control are used to originate, carry, or process illegal robocalls, caller-ID spoofing, fraud, or other unlawful calling activity. It applies to the voice-service activities and call paths for which NexDial is responsible. If a third-party carrier operates part of the call path, NexDial documents that provider's role and the controls allocated to it; NexDial remains responsible for its own applicable obligations.

2. Customer onboarding and Know Your Customer controls

- Before enabling voice traffic, obtain and review the customer's legal business name, business address, responsible contact, service use case, relevant ownership information, and the identity of the party authorized to control the account.
- Determine whether the proposed calling use case involves telemarketing, prerecorded or artificial voice, automated dialing, lead generation, call transfers, or other higher-risk traffic. Request evidence of the customer's authority to use the presented calling numbers and, where applicable, records demonstrating consent and compliance with Do-Not-Call requirements.
- Reject, delay, or restrict activation when identity, number ownership, traffic purpose, consent evidence, or other material information cannot be reasonably verified. Re-review accounts when ownership, campaign, volume, complaint patterns, or traffic purpose materially changes.
- Contractually prohibit illegal robocalls, unlawful caller-ID spoofing, fraud, harassment, and traffic that violates applicable FCC, FTC, TCPA, state, or other applicable requirements. Reserve the right to pause or terminate service and block traffic when credible indicators of abuse appear.

3. Caller-ID, number authorization, and Do Not Originate controls

- Permit outbound caller-ID numbers only where the customer or its authorized provider has documented authority to use them. Investigate complaints of spoofing or unauthorized number use and block or remove numbers that cannot be validated.
- Maintain and update a reasonable Do-Not-Originate (DNO) screening process appropriate to NexDial's role. Apply screening to applicable outbound traffic using reliable number-status information, verified subscriber or number-allocatee requests, and applicable FCC/provider blocking directives. Keep records of list updates and related blocking actions.
- Do not block emergency calls to 911. Make reasonable efforts to avoid blocking calls from public safety answering points and government emergency numbers.

4. Traffic monitoring, analytics, and escalation

- Review available call-detail records, provider dashboards, complaint reports, and available traffic analytics for suspicious patterns. Indicators may include sudden or unexplained volume spikes, unusually high short-duration calling, rapid repeated dialing, excessive failed calls, abnormal calling rates, inconsistent caller-ID use, unusual destination patterns, and spikes in consumer or carrier complaints.
- Use monitoring tools provided by upstream carriers and any analytics tools actually deployed by NexDial. The final filed plan must identify the actual tools or vendors used; do not list a vendor or feature unless NexDial has verified access to it.
- Escalate suspected illegal traffic to the compliance contact and the relevant upstream provider. Depending on the risk, promptly hold, limit, block, or suspend the campaign, calling number, customer account, or route while investigating. Record the alert, investigation, decision, and remediation.

5. Know your upstream provider procedures

- Before using an upstream voice provider, document its legal name, contacts, service role, and the route or traffic it supplies. Review its applicable FCC RMD status and retain a record of the review where required.
- Maintain written service arrangements that identify responsibility for caller-ID authentication, traffic screening, abuse escalation, and traceback cooperation. Obtain written confirmation of which party performs STIR/SHAKEN signing for relevant routes and retain supporting documentation.
- Do not knowingly continue routing traffic through a provider when credible information indicates that the provider is unregistered when registration is required, has been delisted, refuses traceback cooperation, or is facilitating illegal traffic. Escalate and suspend the affected route as appropriate.

6. Traceback requests and cooperation

- The designated contact for robocall mitigation matters is Mario Gobran, Compliance Contact (mario.gobran@nexdial.us; +20 127 595 1199), subject to confirmation that this mailbox and telephone number are actively monitored and that a backup contact is assigned.
- Route traceback requests from the FCC, law enforcement, and the industry traceback consortium immediately to the compliance contact and operations personnel. NexDial commits to respond fully and within 24 hours, preserve and provide relevant available records, cooperate with the requesting entity and upstream providers, and take effective steps to stop any identified illegal traffic.
- Maintain a log of each traceback or formal abuse request, the time received, response deadline, records reviewed, response provided, provider/customer contacts, and remediation taken.

7. STIR/SHAKEN and call authentication

NexDial must accurately identify its STIR/SHAKEN implementation status and any applicable extension or lack-of-control basis in the RMD filing. Before filing, the company must verify the actual status of each relevant network segment and obtain written evidence from any third-party provider that signs calls on NexDial's behalf. This plan does not assert that NexDial itself has implemented STIR/SHAKEN or that any specific extension applies.

8. Records, training, and periodic review

- Keep customer-verification records, number authorization and consent records where applicable, upstream-provider reviews, relevant call-detail records, complaints, DNO changes, traffic alerts, traceback correspondence, and enforcement actions under a documented retention schedule consistent with applicable law and contracts.
- Train personnel who onboard customers, provision service, manage traffic, or handle complaints on these controls and escalation procedures. Review the program at least quarterly and after a material change in services, vendors, network routing, or legal requirements.
- The compliance contact is responsible for coordinating reviews, tracking remediation, updating this plan when operations change, and ensuring material RMD information is updated within applicable FCC deadlines.