

Nedzo — Robocall Mitigation Program

Version: 1.0

Effective date: 01/01/2025

1) Company identification

Legal name: NEDZO LLC

DBA: NEDZO

FRN: 0036843290

Address: 254 Chapman Rd, Ste 208 #15526, Newark, Delaware 19702 US

Primary compliance contact (24/7): Ivo Schipper, 3023432622, ivo@nedzo.ai

Alternate contact: Denis Amaral, 3024042028, denis@nedzo.ai

Operating Company Number (OCN): N/A

RMD filing type: Voice Service Provider (originating/terminating service for end-users).

Nedzo does **not** act as an international gateway provider.

2) Certification alignment

Nedzo originates calls exclusively over IP. All outbound calls are authenticated under the STIR/SHAKEN framework before leaving our network. Authentication is performed via Nedzo's STI-AS and/or via a contracted signing-as-a-service provider that holds a valid SPC token and STI-CA certificate. Unsigned calls are not permitted to egress to the PSTN.

RMD certification selection:

Complete STIR/SHAKEN implementation.

Nedzo commits to: reasonable steps to avoid originating illegal robocalls; full cooperation with law enforcement and the Industry Traceback Group (ITG); and 24-hour response to all traceback requests.

3) Customer vetting (KYB/KYC)

Nedzo performs risk-based identity and use-case verification **before** enabling outbound calling. Minimum requirements include: verification of corporate identity (legal name, EIN, state registration, principal officers), domain-based business email, payment verification, and sanctions screening. High-risk categories require enhanced due diligence such as beneficial-owner IDs and proof of physical presence.

Use-case review is mandatory. Customers must describe purpose, target geographies, call cadence, and whether prerecorded/AI voice is used. Where required by law (e.g., telemarketing or artificial/prerecorded voice), customers must maintain and furnish proof of prior express consent. Nedzo can suspend or deny service if consent artifacts are insufficient or inconsistent with the stated use case.

Re-verification occurs at least annually or upon material change (ownership, use-case, sharp traffic shift).

4) Caller ID (A-number) control

Nedzo prevents spoofing by allowing origination **only** with numbers the caller is authorized to use.

- Numbers assigned by Nedzo are auto-authorized.
- Numbers not assigned by Nedzo require proof of right-to-use (LOA, recent bill, verified enterprise callback, or verified number hosting).
- Invalid/unallocated numbers, NANP-reserved ranges, N11 codes, emergency numbers (e.g., 911/988), and numbers on industry **Do-Not-Originate** lists are blocked.

Authorization is enforced at account and per-CLI level. Any change to authorized numbers triggers re-validation.

5) STIR/SHAKEN attestation policy

Nedzo signs calls with the highest truthful attestation the data supports:

- **A (Full):** Caller is our customer and we assigned or have verified their legitimate control of the calling number.
- **B (Partial):** Caller is our customer and we know who they are and how the call was placed, but we cannot fully verify right-to-use of the specific number; used sparingly and only after documented verification attempts.
- **C:** Not used for retail origination; reserved for transit/gateway scenarios which Nedzo does not perform.

Rich Call Data (RCD) will be included when available and appropriate, consistent with ATIS standards and downstream support.

6) Traffic monitoring and anomaly detection

Nedzo runs continuous monitoring on signaling and media metadata to detect suspect patterns. Controls include short-duration ratio analysis, answer-seizure rate trends, spike/velocity detection, neighbor-spoofing heuristics, snowshoe pattern checks, improper time-of-day calling where applicable, and repeated calling to on-file complaints or DNO destinations. Thresholds are risk-tiered by customer profile and adjusted dynamically.

Suspect traffic is immediately throttled into quarantine routes or blocked outright while compliance reviews run. We keep an auditable trail of alerts, actions, and outcomes.

7) Complaint intake and remediation

We maintain public abuse reporting channels (abuse@nedzo.ai, and web form). Complaints are correlated to CDRs and signatures. For valid issues we notify the customer, require remediation (script changes, consent proof, list hygiene), and may impose caps or blocks. Repeat or willful violations result in suspension or termination with notice to relevant peers if needed to protect the ecosystem.

8) Traceback and law-enforcement cooperation

Nedzo is committed to cooperate fully with the **Industry Traceback Group (ITG)** and regulators. We respond to traceback requests **within 24 hours**, providing originating customer, time stamps, signed Identity header details, and upstream/peer information as permitted by law. We maintain a dedicated on-call contact for nights/weekends.

Primary POC: Ivo Schipper, 3023432622, ivo@nedzo.ai

Alternate POC: Denis Amaral, 3024042028, denis@nedzo.ai

9) Upstream and downstream controls

Nedzo sends traffic only to carriers registered in the FCC Robocall Mitigation Database and requires peers to maintain STIR/SHAKEN and mitigation programs equal to or stricter than ours. Contracts require rapid suspension of abusive traffic, preservation of records, and cooperation with traceback. We perform periodic peer reviews and will reroute or cease interconnection when partners fail compliance checks.

10) International traffic

Nedzo does **not** serve as a gateway provider for international-to-U.S. ingress. If Nedzo begins any gateway function, we will make the appropriate FCC filing and adopt gateway-specific rules (including heightened vetting of foreign sources and mandatory blocking of unsigned foreign ingress).

11) Recordkeeping & retention

We retain CDRs, SIP Identity headers, attestation decisions, customer authorization artifacts, consent proofs (when provided), complaint tickets, and enforcement actions for **at least 24 months** or longer if required by law or contract. Records are encrypted at rest and access-controlled.

12) Employee training and accountability

All personnel who can enable origination or modify authorization undergo initial and annual training covering STIR/SHAKEN, TCPA/47 CFR 64.6305 obligations, DNO usage, complaint handling, and traceback procedures. Compliance KPIs are included in performance reviews. A quarterly internal audit tests adherence to this program and documents corrective actions.

13) Governance and change management

This program is owned by the Compliance Officer and reviewed at least annually or upon material regulatory change. Updates are version-controlled; customers and interconnection partners are notified when changes materially affect them.

14) Principals, affiliates, subsidiaries, parents

Principals (officers/directors/owners): [List names and titles].

Affiliates (under common control): [List or "None"].

Subsidiaries: [List or "None"].

Parent companies: [List or "None"].

(If additional space is required in the RMD form, this section may be referenced there.)

15) Statement and signature

Nedzo adopts this Robocall Mitigation Program and commits to enforce it. We understand that failure to adhere may result in blocking by downstream carriers and enforcement by the FCC.

Signed by: _____

Name: Ivo Schipper

Title: CTO

Date: 01/01/2025