

Robocall Mitigation Program Description

Northvale Solutions LLC

Prepared for submission to the FCC Robocall Mitigation Database (RMD)

NON-CONFIDENTIAL — REDACTED VERSION

This public version describes Northvale Solutions LLC's robocall mitigation controls without disclosing security-sensitive implementation details, internal thresholds, vendor-specific configurations, or other non-public operational information.

1. Purpose and Scope

Northvale Solutions LLC maintains a robocall mitigation program designed to reduce the origination, carrying, and processing of illegal robocalls and unlawful caller-ID spoofing. The program applies risk-based controls throughout customer onboarding, traffic activation, ongoing traffic monitoring, complaint handling, traceback response, and termination or suspension of traffic when appropriate.

The controls described below are intended to be implemented consistently with applicable FCC rules and other applicable federal, state, and industry requirements. Northvale reviews and updates its controls as network conditions, regulatory requirements, and threat patterns change.

2. Customer and Traffic Onboarding Controls

- Customer identification and business-purpose review are performed before traffic is permitted, with documentation maintained as appropriate for the relationship.
- Northvale evaluates the customer's intended traffic type, calling campaigns, expected calling patterns, use of telephone numbers, and other available information to identify elevated-risk traffic.
- Customers are expected to provide accurate business and contact information and to cooperate with compliance inquiries and traceback investigations.
- Traffic may be restricted, suspended, or terminated where available information indicates unlawful calling, material policy violations, misleading caller-ID practices, or failure to address identified compliance concerns.

3. Traffic Monitoring and Detection

- Northvale monitors traffic for abnormal or high-risk calling patterns using available network and call-detail information.
- Monitoring may consider call volume, answer behavior, duration patterns, caller-ID behavior, complaint information, traceback activity, and other indicators associated with potentially unlawful or abusive traffic.
- Traffic that presents elevated risk may be subjected to additional review, increased monitoring, routing restrictions, or other mitigation measures.
- Northvale maintains records and supporting information necessary to investigate identified incidents and respond to appropriate requests from regulators, law enforcement, traceback organizations, and industry partners.

4. Caller-ID Authentication and Spoofing Controls

Where applicable to the portions of Northvale's network and traffic under its control, Northvale supports caller-ID authentication and validation practices consistent with applicable STIR/SHAKEN requirements. Northvale also uses reasonable controls to identify and address suspicious or unauthorized caller-ID use and may request supporting information when caller-ID ownership or use is questioned.

5. Complaint, Traceback, and Incident Response

- Northvale investigates credible reports of illegal robocalls, spoofing, spam, or other unlawful traffic.
- When a traceback request is received from the FCC, law enforcement, or the industry traceback consortium, Northvale will cooperate with the investigation and respond within the applicable 24-hour period required by the FCC rules.
- Northvale uses available call records, customer records, routing information, and related technical data to identify the source and relevant downstream or upstream parties involved in an incident.
- Where an investigation identifies traffic that violates applicable requirements, Northvale may block or suspend the traffic, require corrective action, place the customer under enhanced monitoring, or terminate the relationship, as appropriate.
- Northvale will cooperate with reasonable requests for information needed to investigate and stop illegal robocall activity, subject to applicable law and confidentiality requirements.

6. Blocking and Remediation

- Northvale may block numbers, routes, campaigns, customers, or traffic patterns associated with confirmed or materially suspected unlawful activity.
- Mitigation actions may include traffic suspension, route restriction, caller-ID restrictions, customer remediation requirements, enhanced verification, and termination of service.
- Previously identified abusive traffic patterns are reviewed when appropriate so that materially similar traffic can be detected and addressed.

7. Recordkeeping and Compliance Oversight

Northvale maintains appropriate records relating to customer onboarding, traffic investigations, complaints, traceback requests, mitigation actions, and material compliance incidents. Records are retained and handled in accordance with applicable legal, contractual, and internal requirements. Compliance personnel or designated management review significant incidents and remediation actions.

8. Public Disclosure / Redactions

The non-confidential version intentionally omits security-sensitive implementation details, internal monitoring thresholds, technical identifiers, customer-specific information, and other information that is not necessary for the public to understand the nature of Northvale's robocall mitigation program.

9. Program Governance and Continuous Improvement

Northvale periodically reviews its robocall mitigation controls in light of traceback activity, complaints, observed traffic patterns, regulatory developments, and changes in network or customer risk. Where weaknesses or new abuse patterns are identified, Northvale may revise its monitoring, verification, blocking, escalation, or customer-management procedures.

10. Program Commitment

Northvale Solutions LLC is committed to taking reasonable steps to significantly reduce illegal robocall activity associated with traffic that it originates, carries, or processes, as applicable to its role in the call path. Northvale will cooperate with the FCC, law enforcement, and the industry traceback consortium in investigating and stopping illegal robocallers and will respond to applicable traceback requests within the required timeframe.

Filing note: This document is a filing-ready draft based on the information currently provided. Before submission, Northvale Solutions LLC should verify that every operational statement accurately describes controls it actually maintains and that the company's RMD certification, STIR/SHAKEN status, role in the call path, responsible contact information, and other portal fields are consistent with the company's current FCC records.

Reference: FCC Robocall Mitigation Database requirements and current FCC guidance. See 47 CFR § 64.6305 and the FCC's Robocall Mitigation Database filing materials.