Robocall Mitigation Plan

Noshertel LLC · FRN 0034165563 · FCC Form 499 Filer ID 836309 · OCN 057K

Submitted to the FCC Robocall Mitigation Database (RMD) under 47 C.F.R. § 64.6305 · Effective November 13, 2026

1. Company information

Legal name: Noshertel LLC · **Address:** 30 N Gould St Ste 100, Sheridan, WY 82801 · **Website:** www.noshertel.com

2. Services and role in the call path

Noshertel LLC (the "Company") is a U.S.-based interconnected VoIP provider, not a foreign voice service provider. It sells SIP trunking, U.S. DIDs and voice termination to business customers, including contact centers in Pakistan, India and Philipines etc that connect directly to its SIP trunks, and to foreign and domestic carriers. It is the **originating provider** for its direct customers' calls, and a **gateway provider** for calls received directly from foreign providers at its U.S. points of presence and a non-gateway intermediate provider for U.S. wholesale traffic. Customers that resell service are treated as providers (Section 5). Calls run on the Company's 46 Labs Peeredge switch in Dallas, Texas, on an all-IP network, and are handed off only to RMD-listed U.S. providers.

3. STIR/SHAKEN implementation

The Company has fully implemented STIR/SHAKEN across its network. It holds its own SPC token (OCN 057K) and signs calls with its own certificate from Telonium, an STI-PA-approved certification authority. Telonium's STI-AS signs under a written agreement, and the Company makes every attestation decision (47 C.F.R. § 64.6301(b)).

- **A:** a verified direct customer using a Company-assigned or verified number.
- **B:** a verified direct customer whose number is still being verified, under a documented exception; otherwise the call is rejected.
- **C:** unauthenticated calls with U.S. NANP caller IDs received from foreign providers (47 C.F.R. § 64.6302(d)).

Each signed call carries an origin tied to its customer or upstream trunk. Identity headers are passed downstream unaltered.

4. Know your customer

Before activating a business customer, the Company verifies the legal entity (for example, SECP and NTN records in Pakistan, or MCA, PAN and GST records in India), its address and each principal's government ID, with a live video check for offshore contact centers (47 C.F.R. § 64.1200(n)(4)). It records call purposes, volumes, dialer type, any prerecorded or AI voice, and consent and do-not-call practices. It verifies the right to use each number and allow-lists only those numbers in Peeredge. It screens the

customer and its principals against FCC enforcement actions, traceback history, OFAC lists and its internal blocklist.

High-risk customers start under volume limits for 90 days. Contracts require compliance with the TCPA, the Telemarketing Sales Rule and the Truth in Caller ID Act; prohibit spoofing, number rotation and unapproved resale; and allow immediate suspension. Customers are re-verified annually.

5. Know your upstream provider

The Company accepts traffic from another provider only if that provider's RMD filing appears and has not been removed (47 C.F.R. §§ 64.6305(g), 64.1200(n)(5)). Peeredge rejects calls with U.S. NANP caller IDs from any trunk not marked RMD-verified. Compliance rechecks upstream providers weekly, after FCC removal orders, and before dormant accounts are reactivated. Before interconnection, the Company reviews the provider's registration, licenses, principals, mitigation plan, SPC token status and KYC practices. Contracts require providers to keep their RMD filing current, send only authorized caller IDs, refuse traffic from unlisted providers, answer traceback requests within 24 hours, and accept immediate suspension.

6. Call analytics and monitoring

Peeredge (46 Labs) provides near real-time reporting and automated alerts for every customer and upstream trunk. The NOC reviews alerts within 2 hours, including average call duration under 30 seconds, answer-seizure ratio under 15%, volume spikes, heavy caller ID rotation, invalid or DNO caller IDs, neighbor spoofing, and downstream SIP 603+ rejections.

7. Call blocking and response to illegal traffic

- **DNO blocking.** In compliance with 47 CFR § 64.1200(o), we screen all inbound voice traffic at the network ingress point against a regularly updated Do-Not-Originate (DNO) list. Inbound calls bearing caller IDs associated with invalid, unallocated, unused, or subscriber-designated inbound-only numbers are automatically blocked prior to termination, permitting only valid traffic to traverse our network.
- **FCC notices.** On a Notification of Suspected Illegal Traffic, it investigates promptly, blocks the identified and substantially similar traffic where it is the gateway or originating provider, and reports to the Enforcement Bureau on time. It blocks traffic from any upstream provider named in a Final Determination Order (EB Docket No. 22-174) within 30 days (47 C.F.R. § 64.1200(n)(2)–(3)).
- **Escalation.** Suspected illegal traffic is suspended pending review. Confirmed illegal traffic, spoofing or non-cooperation leads to termination and blocklisting.
- **Safeguards.** The Company never blocks 911 calls and makes all reasonable efforts not to block PSAP or government emergency numbers. It returns SIP 603+ for analytics-based blocks and passes 603+ responses back unaltered.

8. Traceback commitment

The Company commits to respond fully and within 24 hours to all traceback requests from the Commission, civil and criminal law enforcement, and the industry traceback consortium, and to

cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls. It is registered in the Industry Traceback Group portal, monitors the dedicated email ID 24/7, and keeps CDRs for at least 24 months.

9. Recordkeeping and updates

KYC and KYUP files, contracts, traceback records and blocking decisions are kept for at least four years, and third-party authentication agreements for two years after they end. Staff are trained every year. The Company updates its RMD filing and CORES information within 10 business days of any change, and recertifies by March 1 each year.

10. Prior enforcement actions

In the two years before this filing, neither the Company nor any entity sharing common ownership, management, directors or control with it has been the subject of a formal Commission, law enforcement or regulatory agency action or investigation with findings of actual or suspected wrongdoing for facilitating illegal robocalls or spoofing, or for a deficient RMD certification or mitigation program description.

11. Officer certification

I, Muhammad Tabish Khan, CEO of Noshertel LLC, certify on the Company's behalf that all calls it originates, or carries as a gateway provider, are subject to the program in this Plan; that it has fully implemented STIR/SHAKEN and signs calls with a certificate obtained using its own SPC token; that no prior RMD certification of the Company has been removed by Commission action, and it is not prohibited from filing in the RMD; and that the information in this Plan and its RMD filing is true, complete and correct. I declare under penalty of perjury that the foregoing is true and correct. Executed on November 13, 2026.

Signature:  .

Name: Muhammad Tabish Khan

Title: CEO