

Robocall Mitigation Plan

Company: DTA Professionals LLC d/b/a NETLEVER

Address: 1001 Rexhill Ct, Apex, NC 27502, United States

Phone: +1 (919) 336-5998

Website: <https://www.netlever.com>

Date: May 4, 2026

1. Purpose and Scope

This Robocall Mitigation Plan ("Plan") is submitted in compliance with the Federal Communications Commission (FCC) Robocall Mitigation Database (RMD) requirements pursuant to 47 CFR § 64.6305. The purpose of this Plan is to describe the policies, technical controls, and operational practices implemented by NETLEVER to prevent the origination, facilitation, or transmission of illegal robocalls.

NETLEVER provides PBX-as-a-Service (hosted business telephony) exclusively to known business customers—primarily dental practices, healthcare providers, and small businesses—typically as part of an ongoing managed IT services relationship. NETLEVER does not provide voice services to residential consumers, the general public, or marketing organizations.

2. Nature of Services Offered

NETLEVER offers hosted business telephony services using the 3CX platform. The service is:

- Limited to existing, vetted business customers
- Offered only as part of an ongoing IT and managed services relationship
- Designed solely for day-to-day business communications

NETLEVER does not offer or support:

- Mass dialing or bulk calling services
- Predictive, power, or autodialers
- Robocall platforms or robocall campaigns
- Telemarketing, lead generation, political calling, or other high-risk calling campaigns
- Application-to-person (A2P) or automated calling APIs

3. Closed System Architecture and Technical Controls

NETLEVER operates a closed, controlled voice environment with safeguards including:

-
- All calls originate from authenticated users assigned to specific customer organizations
 - Endpoints are limited to provisioned desk phones or approved softphone applications
 - User authentication is required for all extensions; anonymous SIP access is disabled
 - IP address allow-listing is enforced; calls may only originate from approved customer networks where feasible
 - Programmatic or API-based call initiation is not permitted
 - Administrative access to PBX and trunks is restricted and logged

These controls ensure that only authorized users within known customer organizations can place outbound calls.

4. Customer Vetting and Know-Your-Customer (KYC) Procedures

NETLEVER maintains formal KYC procedures to reduce the risk of illegal robocalls and misuse of service. Prior to enabling voice services, NETLEVER:

- Verifies legal identity and registration: collects the customer's legal entity name, EIN (or equivalent tax identifier), and state business registration (or professional license where applicable).
- Validates physical presence and contactability: confirms a physical service address, main business phone number, and business email domain; verifies authorized contacts (owner/manager) and at least one alternate contact.
- Confirms legitimate business purpose: documents intended use cases (e.g., appointment scheduling, patient/customer communications) and prohibits high-risk uses (telemarketing, robocalls, lead generation).
- Executes contractual controls: requires acceptance of Terms of Service and Acceptable Use Policy prohibiting illegal robocalls, spoofing, harassment, and non-compliant campaigns; includes suspension/termination and cooperation clauses.
- Validates numbers and calling identity: ensures telephone numbers used for outbound calling are assigned to the customer or otherwise authorized; documents number sources and any porting/assignment records where applicable.
- Activation review: performs an initial configuration review (PBX, trunks, call permissions) and performs test calls to confirm normal business operation.
- Ongoing re-verification: re-validates customer identity and usage at renewal or upon material changes (ownership, address, calling patterns, additional sites/extensions).

Because NETLEVER often serves as the customer's managed IT provider, customer activity and service usage are continuously observable and auditable via support interactions, provisioning records, and call detail records.

5. Analytics, Traffic Monitoring, and Abuse Prevention

NETLEVER uses a layered approach to detect and mitigate suspicious traffic:

- Platform-level monitoring: NETLEVER reviews 3CX call detail records (CDRs) and administrative logs for indicators such as unexpected call-volume spikes, unusual destination patterns, repeated short-duration calls, or attempts to bypass restrictions.
- Carrier-level analytics (third-party): NETLEVER relies on analytics and monitoring performed by its upstream carrier, Bandwidth Inc., which monitors network-level traffic patterns and signaling information and may apply carrier-grade protections and enforcement consistent with its policies and applicable requirements.
- Responsive controls: if suspicious activity is detected, NETLEVER may immediately suspend outbound calling, disable extensions, restrict destinations, require additional verification, or terminate service. NETLEVER cooperates with traceback requests, upstream providers, and regulatory authorities as appropriate.

Third-party analytics vendors: Other than Bandwidth Inc. (as upstream carrier), NETLEVER does not currently use separate third-party call analytics vendors. If NETLEVER adds any such vendor(s), NETLEVER will update its RMD filing and this Plan accordingly.

6. Upstream Provider and STIR/SHAKEN

NETLEVER does not originate calls directly to the Public Switched Telephone Network (PSTN). All outbound calls are routed through Bandwidth Inc., a voice service provider that implements the STIR/SHAKEN caller ID authentication framework.

NETLEVER relies on Bandwidth Inc. to perform STIR/SHAKEN signing and verification for outbound traffic carried to the PSTN and does not independently inject unsigned traffic to the PSTN.

7. Complaint Handling, Traceback Cooperation, and Enforcement

NETLEVER maintains a dedicated process for receiving and addressing complaints related to robocalls or misuse of voice services:

- Prompt internal investigation of complaints and customer-reported incidents
- Immediate suspension or termination of offending accounts, as warranted
- Cooperation with traceback requests from the FCC, law enforcement, or industry traceback consortiums within required timeframes

8. Commitment to Ongoing Compliance

- Maintain accurate and current information in the FCC Robocall Mitigation Database
- Update this Plan as business operations or regulatory requirements evolve
- Respond fully and promptly to FCC or law enforcement inquiries

9. Contact Information

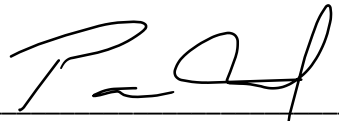
Robocall Mitigation Compliance Officer: Pablo Uribe

Email: pablo.uribe@netlever.com

Phone: +1 (252) 670-8240

10. Certification

I certify that the information contained in this Robocall Mitigation Plan is true, accurate, and complete, and that NETLEVER is committed to preventing unlawful robocalls in accordance with FCC rules and regulations.

Authorized Signatory: _____

Name: Pablo Uribe

Title: Managing Member / Compliance Officer

Date: April 10, 2026

Appendix A — Regulatory History Disclosure (for RMD filing narrative)

This appendix is provided to supply additional space for the RMD certification field that requests a description of any formal Commission, law enforcement, or regulatory agency action or investigation.

(1) Agencies involved:

Federal Communications Commission (FCC), including the Enforcement Bureau (EB).

(2) Date the action/investigation commenced:

- August 25, 2025 — In the Matter of Robocall Mitigation Database Filers, Order DA-25-694
- March 24, 2026 — In the Matter of Robocall Mitigation Database Filers, Order DA-26-282

(3) Current status of the action/investigation:

The August 2025 Order removed the Company's Robocall Mitigation Database (RMD) certification due to filing deficiencies. The March 24, 2026 Order directs the Company to cure remaining deficiencies in its RMD certification (including its robocall mitigation plan) and notify the FCC that deficiencies have been cured, or explain why the certification should not be removed.

(4) Summary of findings of wrongdoing made in connection with the action/investigation:

The FCC Orders identify deficiencies in the Company's RMD filing (including missing or insufficient required information and/or deficiencies in the filing elements required under the amended RMD rules).

(5) Whether any final determinations have been issued:

The August 2025 Order is an issued Bureau Order removing certifications from the RMD. The March 24, 2026 Order is an issued Bureau Order directing cure of deficiencies and requiring a response; continued listing/reinstatement depends on FCC review after deficiencies are cured.