

NETWAVZ, INC.

ROBOCALL MITIGATION PROGRAM DESCRIPTION

Prepared for the FCC Robocall Mitigation Database

September 2026

Netwavz, Inc. ("Netwavz") provides interconnected voice services to end users and has selected Complete STIR/SHAKEN Implementation in its Robocall Mitigation Database certification. This document describes the reasonable steps Netwavz uses to prevent its services from being used to originate illegal robocall traffic and its procedures for responding to suspected unlawful traffic.

1. Robocall Mitigation Program

All calls originated through Netwavz's voice service are subject to Netwavz's robocall mitigation program. Netwavz maintains policies and operational practices intended to prevent customers from using its services to originate illegal robocalls, unlawful spoofing, or other prohibited calling activity. Netwavz will investigate credible reports of suspected illegal traffic and may restrict, suspend, or terminate service when necessary to stop unlawful use.

2. STIR/SHAKEN Implementation

Netwavz's underlying voice platform is provided through Talking Platforms/ioTRAN. Netwavz has been advised by its platform provider that the service applicable to Netwavz supports Complete STIR/SHAKEN Implementation. Accordingly, calls originated through the applicable IP voice platform are subject to the STIR/SHAKEN caller-ID authentication framework. Netwavz relies on the underlying platform and carrier infrastructure for the technical implementation of STIR/SHAKEN authentication.

3. New and Renewing Customer Due Diligence

Netwavz takes affirmative measures intended to know its customers and reduce the risk that its services will be used to originate illegal calls. Netwavz primarily serves residential consumers and small and medium-sized businesses and maintains an identifiable customer relationship for provisioned voice service.

- Netwavz obtains customer identity and contact information appropriate to the service being ordered, including the customer or business name, service address, telephone and email contact information, and billing information.
- Business customers may be reviewed using publicly available business information and information obtained through Netwavz's existing customer relationship, where applicable.
- Netwavz reviews service requests for inconsistencies or circumstances that reasonably indicate fraud, unlawful calling activity, or misrepresentation before or during activation.
- Netwavz maintains customer and service records sufficient to identify the subscriber associated with provisioned service and telephone numbers.
- Customer use of Netwavz voice service is subject to applicable service terms, acceptable-use requirements, and federal and state law. Illegal robocalling, unlawful spoofing, fraud, and other unlawful use are prohibited.
- Netwavz may request additional information, restrict calling, suspend service, or terminate service when activity presents a reasonable indication of unlawful or abusive use.

4. Monitoring and Call Analytics

Netwavz uses the capabilities of its underlying Talking Platforms/ioTRAN voice platform and upstream carrier infrastructure in connection with call processing, caller-ID authentication, fraud prevention, and network-level controls. Netwavz also reviews complaints, service anomalies, fraud indicators, and information received from its platform provider, carriers, regulators, law enforcement, or the Industry Traceback Group when such information indicates possible illegal traffic.

Netwavz does not represent in this filing that it operates a proprietary call-analytics platform. To the extent network-level analytics, blocking, or fraud-detection systems are applied to Netwavz traffic, those capabilities are provided through its underlying platform and carrier relationships.

5. Upstream Provider Procedures

Netwavz obtains its underlying voice platform and related wholesale voice services through Talking Platforms/ioTRAN. Netwavz maintains a direct commercial relationship with its provider and relies on that provider and its carrier relationships for underlying call transport and network functions. Netwavz will periodically review the regulatory status of providers from which it directly receives voice traffic, including applicable Robocall Mitigation Database information, and will address credible information indicating that an upstream provider is being used to carry or process a high volume of illegal traffic.

6. Complaints, Investigation, and Enforcement

When Netwavz receives a credible complaint or notice concerning suspected illegal robocall traffic associated with its service, it will review available customer and service information, relevant calling information available to it, and information supplied by its platform provider or carriers. Depending on the circumstances, Netwavz may contact the customer, require an explanation or corrective action, restrict service, suspend service, terminate service, or take other reasonable measures designed to stop the activity.

7. Traceback and Government Cooperation

Netwavz commits to respond fully and within 24 hours to traceback requests from the Federal Communications Commission, law enforcement, and the registered industry traceback consortium, and to cooperate with those entities in investigating and stopping illegal robocallers that use Netwavz service to originate calls. Netwavz will coordinate with Talking Platforms/ioTRAN and applicable upstream carriers when their records or technical assistance are necessary to investigate or trace traffic.

8. Program Review and Updates

Netwavz will review its robocall mitigation practices as its voice service, customer base, platform capabilities, regulatory requirements, and identified risks evolve. Netwavz will update its Robocall Mitigation Database filing and this program description when required to keep the filing accurate and complete.

9. Robocall Mitigation Contact

The robocall mitigation point of contact for Netwavz is the individual identified in Netwavz's Robocall Mitigation Database filing. Requests concerning traceback, suspected illegal traffic, or regulatory compliance should be directed to that contact using the information maintained in the Database.