



2455 Naglee Rd #274
Tracy CA 95304
+1 707-77-SONIC (76642)

16 March 2026

FRN: 0038153276

Subsonic Enterprises

Robocall Mitigation Program Description

Overview

Subsonic Enterprises operates as both a Voice Service Provider and a Non-Gateway Intermediate Provider and has implemented a robocall mitigation program designed to prevent the origination, carriage, or processing of illegal robocall traffic. The program includes customer and provider due diligence procedures, network monitoring and analytics, enforcement actions, and cooperation with industry traceback efforts.

Reasonable Steps to Avoid Originating Illegal Robocalls

As a voice service provider, Subsonic Enterprises has implemented procedures consistent with 47 CFR §64.1200(n)(4) to know its customers and reduce the risk of illegal robocall traffic originating on its network.

These procedures include but are not limited to:

- Verification of customer identity and business information
- Validation of contact details
- Review of the customer's intended use of telecommunications services
- Review of intended traffic type and calling patterns
- Review of prior telecommunications compliance history where available
- Monitoring of account activity following activation



Customers whose traffic patterns or business models present elevated risk may be subject to additional verification or monitoring.

Customer Acceptable Use and Enforcement

Subsonic Enterprises maintains terms of service and acceptable use policies that explicitly prohibit:

- Origination of illegal robocalls
- Caller ID spoofing in violation of federal law
- Use of the network for unlawful telemarketing
- Transmission of fraudulent or scam-related communications

Analytics and Traffic Monitoring

Subsonic Enterprises monitors network activity to detect suspicious or anomalous calling behavior that may indicate illegal robocall activity.

Traffic monitoring includes analysis of:

- Call volume anomalies
- Short duration or high call failure rates
- Sequential or predictive dialing patterns
- Repeated complaints associated with specific calling numbers
- Invalid, spoofed, or unassigned caller ID numbers
- Other patterns commonly associated with robocall campaigns.

These systems analyze traffic patterns and signaling data to detect indicators of robocall campaigns or caller ID spoofing. When suspicious traffic patterns are identified, the traffic may be investigated and appropriate mitigation steps may be taken.

These analytics may include internal monitoring systems and may also incorporate third-party analytics solutions where appropriate to identify, block, or mitigate illegal robocall traffic.



Where suspicious traffic is detected, Subsonic Enterprises may investigate the originating customer and take corrective action including blocking traffic, suspending service, or terminating the customer relationship.

Enforcement and Remediation

When Subsonic Enterprises identifies illegal robocall activity originating from its network, it will take appropriate remedial action, which may include:

- Blocking specific call traffic
- Suspending or terminating customer accounts
- Implementing additional monitoring
- Cooperating with regulatory enforcement authorities

Caller ID Authentication (STIR/SHAKEN)

Where supported by the network infrastructure, Subsonic Enterprises participates in the **STIR/SHAKEN framework** to authenticate caller ID information and help prevent spoofing.

Calls originating from portions of the network where STIR/SHAKEN is implemented are authenticated consistent with **47 CFR §64.6301**.

Procedures to Know Upstream Providers

In its role as a non-gateway intermediate provider, Subsonic Enterprises maintains procedures to evaluate and monitor upstream providers from which it accepts traffic.

Upstream providers must represent that they comply with applicable robocall mitigation obligations and must appear in the FCC Robocall Mitigation Database where required. Providers that fail to maintain appropriate mitigation practices or whose traffic is associated with illegal robocalls may be blocked or disconnected.



Traceback Cooperation Commitment

Subsonic Enterprises commits to respond within 24 hours to all traceback requests from the Federal Communications Commission, law enforcement agencies, and the Industry Traceback Group or any other designated industry traceback consortium.

The company will cooperate fully with traceback investigations and provide relevant call routing information or records necessary to identify the source of illegal robocall traffic.

Regulatory History

Within the previous two years, Subsonic Enterprises has not been the subject of any formal Commission, law enforcement, or regulatory agency action or investigation with findings of actual or suspected wrongdoing related to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or caller ID spoofing, or for a deficient Robocall Mitigation Database certification or mitigation program description.

Ongoing Compliance

Subsonic Enterprises continually evaluates and updates its robocall mitigation policies, monitoring procedures, and enforcement actions in order to comply with evolving regulatory requirements and industry best practices designed to combat illegal robocall activity.

The company commits to maintaining an effective robocall mitigation program and updating its Robocall Mitigation Database certification as required under **47 CFR §64.6305**.