

MSQ TECHNOLOGY

Robocall Mitigation Program Description

FCC Robocall Mitigation Database (RMD)

FRN: 0038894382 | Business Address: 2451 Ellis Town Dr, Tracy, CA 95377

Effective / Filing Date: September 22, 2026

1. Provider Profile and Scope

MSQ Technology is a U.S.-based, non-facilities-based reseller of voice services serving business end users. MSQ Technology obtains telephone numbers, SIP/PSTN connectivity, and underlying carrier network services from upstream voice service providers. MSQ Technology does not operate mass-market robocalling or autodialing campaigns and does not offer its service for unlawful spoofing or illegal robocalling.

2. STIR/SHAKEN Status and Basis

MSQ Technology has not implemented the STIR/SHAKEN authentication framework on any portion of a network that it owns or controls. MSQ Technology lacks control over the network infrastructure necessary to implement STIR/SHAKEN and relies on its underlying upstream voice service providers for PSTN connectivity and the network infrastructure used for caller-ID authentication. MSQ Technology therefore files as a voice service provider without a STIR/SHAKEN implementation obligation under 47 CFR § 64.6305(d)(2)(i), based on its lack of control over the network infrastructure necessary to implement STIR/SHAKEN.

3. Reasonable Steps to Prevent Illegal Robocalls

MSQ Technology maintains a robocall mitigation program intended to prevent its services from being used to originate illegal robocall traffic. Service is provisioned for identified business customers and is not intended for anonymous, high-volume robocalling. MSQ Technology may review account identity and business information, service purpose, assigned telephone numbers, calling patterns, carrier notices, complaints, and other available information when activity raises a reasonable concern of unlawful use. MSQ Technology may restrict, suspend, or terminate service when it determines that continued service presents an unacceptable risk of illegal robocalling, unlawful spoofing, fraud, or violation of applicable law or carrier requirements.

4. Customer Identification and Service Controls

MSQ Technology provisions service to business customers through controlled account and service provisioning processes. Telephone numbers and SIP credentials are associated with customer and service records. MSQ Technology does not knowingly permit customers to use calling numbers they are not authorized to use. Where a customer requests caller-ID configuration or number assignment, MSQ Technology uses numbers associated with the customer's authorized service or numbers otherwise validated through the applicable upstream provider.

5. Monitoring, Complaints, and Escalation

MSQ Technology reviews available carrier notifications, abuse reports, customer complaints, and service records for indicators of potentially unlawful calling. Potential abuse is investigated using available account, number, call-detail, provisioning, and upstream-provider information. Depending on the circumstances, mitigation may include contacting the customer, restricting calling capability, disabling SIP credentials, suspending service, or terminating the account. MSQ Technology will preserve and provide relevant information when lawfully required and available.

6. Traceback Cooperation

MSQ Technology commits to respond fully and within 24 hours to traceback requests from the Federal Communications Commission, law enforcement, and the registered Industry Traceback Group, consistent with 47 CFR § 64.6305. MSQ

Technology will cooperate with such entities in investigating and stopping illegal robocallers that use its service to originate calls. Traceback inquiries are directed to the robocall mitigation contact identified in MSQ Technology's RMD filing.

7. Upstream Provider Cooperation

MSQ Technology relies on upstream voice service providers for underlying PSTN connectivity and caller-ID authentication functions. When investigating suspected illegal traffic, MSQ Technology will coordinate with the relevant upstream provider as necessary to identify the affected service, preserve available records, address routing or authentication issues, and stop unlawful traffic. MSQ Technology will take reasonable steps to use reputable upstream providers and will respond to material compliance or abuse notices received from them.

8. No Facilitation of Illegal Spoofing or Robocalling

MSQ Technology does not knowingly transmit, encourage, assist, or facilitate illegal robocalls or unlawful spoofing. Use of MSQ Technology services for fraudulent impersonation, unlawful caller-ID spoofing, illegal prerecorded or artificial-voice campaigns, or other unlawful calling activity is prohibited. Where MSQ Technology obtains credible evidence of such activity, it will investigate and take reasonable corrective action.

9. Program Administration and Updates

MSQ Technology will review this mitigation program as its network architecture, upstream providers, customer base, regulatory obligations, or risk profile changes. The company will update its RMD filing when required by FCC rules and will maintain the filing and required annual recertification. If MSQ Technology later obtains control over network infrastructure that changes its STIR/SHAKEN implementation obligations, it will reassess and update its certification accordingly.

Regulatory References

- 47 CFR § 64.6305 - Robocall mitigation and Robocall Mitigation Database requirements.
- FCC Wireline Competition Bureau, DA 24-73 - expanded RMD filing requirements and reasonable-steps mitigation standard.
- FCC, DA 26-72 - Robocall Mitigation Database Frequently Asked Questions for Filers (Jan. 2026).

Certification note: This document describes MSQ Technology's mitigation program for its RMD filing. The officer submitting the filing should review the document and confirm that every statement accurately reflects MSQ Technology's actual operations before certifying under penalty of perjury.