

Robocall Mitigation Program Description

Filed with the FCC Robocall Mitigation Database pursuant to 47 CFR § 64.6305

Filer (Legal Entity Name): **Loop Voice C-Corp (“LoopVoice.ai” or the “Company”)**

FCC Registration Number (FRN): **0038559555**

Business Address: **8 The Green, Ste R, Dover, DE 19901, United States**

Robocall Mitigation Point of Contact: **Muhammad Harris Solangi, Chief Technology Officer**

Contact Email / Phone: **software@loopvoice.ai / +1 586 327 2464**

Date: **19 June 2026**

1. Overview and Company Role

LoopVoice.ai is a voice service provider that furnishes voice communications to its own end-user customers. The Company provides an AI-based voice service that its business customers use to place and receive calls. The Company does not operate or control any voice or IP network infrastructure of its own. All call origination, routing, and caller ID authentication are performed by the Company’s underlying carrier, Telnyx, which is approved by the STI-PA and is fully STIR/SHAKEN compliant. This Robocall Mitigation Program describes the reasonable steps the Company takes to avoid originating, carrying, or processing illegal robocall traffic, consistent with 47 CFR § 64.6305(a).

2. STIR/SHAKEN Status and Basis for No Implementation Obligation

The Company certifies that it has not implemented the STIR/SHAKEN authentication framework on any portion of its network. The implementation obligation under 47 CFR § 64.6301 applies to a voice service provider’s own internet Protocol network. The Company does not control the network infrastructure necessary to implement STIR/SHAKEN, as contemplated by 47 CFR § 64.6305(f)(2)(i). All calls associated with the Company’s service are originated and authenticated by Telnyx, an STI-PA-approved, fully STIR/SHAKEN-compliant carrier. Because the Company operates no IP network of its own on which to deploy the framework, it is unable to implement STIR/SHAKEN due to a lack of control over the necessary network infrastructure. The Company satisfies its obligations through the robocall mitigation measures described below.

3. Know Your Customer (KYC) Procedures

Consistent with its obligation to know its customers under 47 CFR § 64.1200(n)(4), the Company takes the following reasonable steps before and during the provision of service: [DESCRIBE YOUR ACTUAL PRACTICES — e.g., verifying the legal identity and business registration of each customer at onboarding; collecting and validating business contact details; confirming the customer’s intended use case and lawful basis for outbound calling; requiring agreement to an Acceptable Use Policy that prohibits illegal robocalling, spoofing, and calls violating the TCPA or Telemarketing Sales Rule; verifying ownership or authorized use of any caller ID/number presented; and maintaining records of customer identity and onboarding for the duration of the relationship.] The Company reserves the right to request additional documentation where a customer’s identity or calling purpose cannot be adequately verified, and to decline or suspend service in such cases.

4. Know Your Upstream/Downstream Providers

The Company’s sole underlying carrier is Telnyx, a registered U.S. voice service provider listed in the Robocall Mitigation Database and fully STIR/SHAKEN compliant. [IF YOU USE ANY ADDITIONAL CARRIERS OR PROVIDERS, LIST THEM AND CONFIRM EACH IS RMD-LISTED.] The Company does not accept or carry traffic originated by other voice service providers; it serves only its own end-user customers. The Company confirms that any provider from which it obtains origination services is appropriately registered and compliant before relying on that provider.

5. Call Monitoring and Analytics to Identify and Block Illegal Traffic

The Company takes reasonable steps to identify and stop illegal robocall traffic on its platform, including: [DESCRIBE YOUR ACTUAL PRACTICES — e.g., monitoring outbound calling patterns for anomalies indicative of illegal robocalling, such as abnormal call volumes, very short average call durations, high unanswered-call rates, and rapid number rotation; applying rate limits and velocity controls per customer; reviewing complaints and carrier notifications; and the analytics or fraud-detection system(s) used.] The Company uses the following analytics system(s)/vendor(s): [NAME ANY THIRD-PARTY ANALYTICS VENDORS, OR STATE “none; monitoring is performed in-house” / “the Company relies on Telnyx’s network-level fraud and traffic controls.”] Where the Company identifies traffic it reasonably believes to be illegal, it takes prompt action, up to and including throttling, blocking, and suspending or terminating the responsible customer’s service.

6. Cooperation with Traceback and Enforcement

The Company is committed to responding fully and within 24 hours to all traceback requests from the FCC, law enforcement, and the industry traceback consortium (USTelecom’s Industry Traceback Group), and to cooperating with those entities in investigating and stopping any illegal robocallers that use the Company’s service to originate calls. The designated point of contact identified at the top of this document monitors and responds to such requests. The Company maintains records sufficient to identify the source of traffic on its platform to support traceback efforts.

7. Acceptable Use and Enforcement

All customers are bound by the Company’s Acceptable Use Policy, which prohibits illegal robocalls, unlawful caller ID spoofing, and any calling that violates the Telephone Consumer Protection Act, the Telemarketing Sales Rule, or other applicable law. The Company enforces this policy through the monitoring described above and through suspension or termination of non-compliant customers.

8. Ownership and Management

[PROVIDE SUFFICIENT DETAIL ON OWNERSHIP AND MANAGEMENT — e.g., the legal entity name and form, the principals/officers and their roles, and any parent, subsidiary, or affiliated entities (or state “none”). This allows the Commission to confirm the filer has not been prohibited from filing in the RMD.]

9. Recordkeeping and Annual Review

The Company maintains records of its robocall mitigation practices and reviews this program at least annually, and otherwise as needed. The Company will recertify its filing in the Robocall Mitigation Database annually by the applicable deadline and will update its filing within the required timeframe if any information changes.

This Robocall Mitigation Program Description is submitted in support of the Company’s certification in the FCC Robocall Mitigation Database. The undersigned certifies that the information contained herein is true and accurate to the best of their knowledge.

Signature:  _____ Date: ____19 June 2026__

Name / Title: **Muhammad Harris Solangi, Chief Technology Officer**