

Robocall Mitigation Program Description

Spool is a Voice Service Provider that facilitates user-authorized outbound calls on behalf of verified end users. All calls originated by Spool are subject to a comprehensive robocall mitigation program designed to prevent illegal robocalls, ensure accountability, and enable rapid response to traceback requests and enforcement actions.

1. User Identity Verification and Accountability

Spool requires all users to complete identity verification prior to initiating any outbound calls. This process is designed to eliminate anonymity and ensure traceability for every call originated on the platform. Identity verification includes:

- First and last name
- A verified, unique email address
- A verified callback phone number
- Financial verification via a valid credit card and billing address

Each outbound call is logged and attributable to a specific verified user account. Spool does not permit anonymous, pseudonymous, or “burner” accounts, and does not allow shared or unverified calling credentials. These controls ensure that all call activity can be traced to an accountable individual

Spool Governance & Automated En...

2. STIR/SHAKEN Compliance

Spool satisfies its STIR/SHAKEN authentication obligations through its underlying carrier, which authenticates and signs all outbound calls originated on Spool’s behalf. All calls originated by Spool are STIR/SHAKEN compliant.

3. Prohibited Call Types and Content Controls

Spool employs proactive technical and policy-based controls to prevent the origination of illegal, deceptive, or abusive calls. The platform enforces a system-level governance layer that overrides user instructions and automatically blocks prohibited activity, including:

- Unsolicited outbound telemarketing or lead-generation calls
- Impersonation of government officials, law enforcement, medical professionals, or any human identity

- Deceptive representations regarding the nature of the call or caller identity
- Facilitation of criminal activity, including fraud or sale of federally controlled substances

All outbound calls include mandatory disclosure at call initiation identifying the caller as a digital assistant acting on behalf of the verified user. If challenged, the system will not misrepresent itself as human or conceal its automated nature

Spool Governance & Automated En...

4. Call Cadence, Rate Limiting, and Time-of-Day Controls

To prevent robocall-like behavior, Spool enforces technical limitations on call volume and frequency, including:

- Rate limiting to prevent high-volume or burst dialing patterns
- Geographic and time-zone–based restrictions to ensure calls are placed only during legally permissible hours
- Monitoring of call cadence to detect and block abnormal usage patterns characteristic of automated robocalling campaigns

These controls are designed to ensure calls remain task-specific, user-initiated, and consistent with legitimate use cases

Spool Governance & Automated En...

5. Recipient Transparency, Opt-Out, and Complaint Handling

Spool maintains mechanisms to protect call recipients and provide meaningful redress, including:

- Immediate compliance with any recipient request to opt out or be placed on a do-not-call list, after which the call is terminated and the opt-out is permanently logged
- A public-facing verification and complaint portal allowing recipients to identify the initiating user based on call metadata
- Manual review of complaints, including review of call transcripts and user authorization

These measures ensure that recipient concerns are addressed promptly and that misuse is identified and corrected

Spool Governance & Automated En...

6. Enforcement, Suspension, and Cooperation with Authorities

Spool enforces a tiered response framework for violations, ranging from warnings and audits to immediate account suspension for serious misconduct. In cases involving harassment, deception, fraud, or criminal activity, accounts are terminated without notice.

Spool commits to responding fully and within 24 hours to traceback requests from the FCC, law enforcement, and the industry traceback consortium. Where legally appropriate, Spool will cooperate with investigations and may provide relevant KYC data and call records in accordance with applicable law

Spool continuously reviews and updates its robocall mitigation controls to reflect evolving regulatory guidance, industry best practices, and observed misuse patterns.