

Robocall Mitigation Plan for Relay Innovations, Inc. DBA AgentPhone

April 14, 2026

Relay Innovations, Inc. DBA AgentPhone (“AgentPhone”) provides a communications platform that enables business customers to interact with end users through voice and messaging channels. AgentPhone’s platform is designed to support legitimate business communications, including customer support, appointment reminders, follow-ups, and other user-authorized interactions. AgentPhone does not operate as a facilities-based carrier and does not independently implement STIR/SHAKEN authentication on its own network. Instead, AgentPhone relies on upstream voice providers for call authentication while maintaining a robocall mitigation program at the application and customer-management layers.

Purpose of This Plan

This Robocall Mitigation Plan describes the steps AgentPhone takes to reduce the risk of illegal robocalls, spoofing, and abusive calling practices on its platform. AgentPhone is committed to preventing misuse of its services, ensuring that customers use the platform lawfully, and cooperating with lawful traceback, enforcement, and compliance processes as required.

Overview of AgentPhone’s Service

AgentPhone provides software and communications tooling that allows customers to provision and use phone numbers for business communications. These capabilities may include outbound and inbound voice calling, as well as messaging features. AgentPhone’s customers are businesses using the platform to communicate with their own users, leads, patients, customers, or other authorized recipients.

AgentPhone does not market its services for unsolicited bulk calling. Outbound communications initiated through AgentPhone are expected to be tied to legitimate business workflows and lawful end-user interactions.

Robocall Mitigation Framework

AgentPhone’s robocall mitigation program is built around three core components:

1. Prevention
2. Monitoring and Detection
3. Mitigation and Enforcement

1. Prevention

AgentPhone takes reasonable steps to reduce the likelihood that bad actors gain access to the platform or use it for unlawful calling activity.

- a) **Customer Review and Onboarding.** AgentPhone reviews prospective customers and their proposed use cases before enabling calling capabilities. As part of this process, AgentPhone may collect identifying information about the customer, business details, website and domain information, intended use case descriptions, and other relevant onboarding materials.
- b) **Know Your Customer Practices.** AgentPhone maintains risk-based Know Your Customer (KYC) practices designed to verify that customers are legitimate businesses and to assess whether their intended use of the platform presents elevated robocall, fraud, or abuse risk.
- c) **Use Case Review.** AgentPhone reviews whether proposed calling use cases appear consistent with lawful and expected business communications. Use cases associated with spam, deceptive calling, spoofing, lead-generation abuse, or other high-risk behavior may be restricted, rejected, or subjected to enhanced review.
- d) **Customer Representations and Contractual Restrictions.** AgentPhone requires customers to agree to applicable terms of service and acceptable use restrictions. These restrictions prohibit unlawful robocalling, spoofing, fraudulent conduct, and communications made without any required consent under applicable law.
- e) **Consent Expectations.** AgentPhone requires customers to obtain any legally required consent before placing calls or sending messages to end users. Customers are responsible for ensuring that their calling campaigns, workflows, and contact lists comply with applicable laws and regulations, including consumer protection requirements.

2. Monitoring and Detection

AgentPhone uses operational and technical safeguards to identify unusual, suspicious, or abusive use of its services.

- a) **Traffic Monitoring.** AgentPhone monitors platform activity for unusual traffic patterns, including abnormal call volumes, irregular call timing, suspicious dialing behavior, elevated failure rates, and other signs of misuse.
- b) **Rate Limits and Volume Controls.** AgentPhone may apply rate limits, account-level controls, or other operational restrictions to reduce abuse risk and to prevent sudden high-volume traffic spikes associated with unlawful robocalling.
- c) **Anomaly Detection and Manual Review.** AgentPhone reviews flagged activity through a combination of automated systems and manual investigation. Accounts or workflows that appear inconsistent with stated use cases may be investigated further.
- d) **Complaint and Feedback Review.** AgentPhone reviews complaints, provider notices, and other feedback signals that may indicate improper use of its services. These signals may be incorporated into account monitoring and enforcement decisions.
- e) **Upstream Provider Coordination.** Where relevant, AgentPhone works with upstream providers to review problematic traffic, investigate suspicious activity, and support compliance with applicable voice ecosystem requirements.

3. Mitigation and Enforcement

If AgentPhone identifies suspected abuse or unlawful calling activity, it takes corrective action designed to stop the activity and reduce further risk.

- a) **Account Investigation.** AgentPhone investigates accounts that generate suspicious traffic patterns, complaints, or provider escalations.
- b) **Restrictions and Suspensions.** AgentPhone may restrict, suspend, or terminate accounts, numbers, or calling capabilities where misuse is suspected or confirmed.
- c) **Customer Outreach and Remediation.** In appropriate cases, AgentPhone may contact customers to request clarification, documentation, or remediation steps before restoring or expanding service.
- d) **Traceback and Lawful Cooperation.** AgentPhone will cooperate with lawful traceback requests, upstream provider inquiries, and valid requests from regulatory or law enforcement authorities as required by law.

- e) **Ongoing Risk Reduction.** AgentPhone updates its controls, onboarding processes, and monitoring practices as needed in response to evolving fraud patterns, platform usage, and compliance requirements.

STIR/SHAKEN Status

AgentPhone does not directly implement STIR/SHAKEN authentication on its own network and does not claim an exemption from compliance requirements. AgentPhone relies on upstream voice providers for call authentication and related network-level obligations, while maintaining robocall mitigation controls at the application and customer-management layers.

Customer Responsibilities

Customers using AgentPhone are responsible for:

- obtaining any legally required consent before placing calls;
- ensuring that calling practices comply with applicable laws and regulations;
- using accurate caller identification information;
- avoiding deceptive, abusive, or unsolicited calling practices; and
- responding promptly to AgentPhone inquiries relating to compliance or suspected abuse.

Affiliated Entities

This Robocall Mitigation Plan applies to:

- Relay Innovations, Inc. DBA AgentPhone

AgentPhone has no parent company, subsidiaries, or affiliated operating entities covered by this plan unless and until such entities are later identified in an updated filing.

Principal Contact

Name: Meet Modi

Title: Co-founder

Company: Relay Innovations, Inc. DBA AgentPhone

Email: meet@agentphone.to

Certification

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge and belief.

Executed on: April 14, 2026

e-Signature: Meet Modi