

Robocall Mitigation Program Description

RevelAI operates as an application-layer platform that facilitates voice communications on behalf of its customers using third-party telecommunications providers (e.g., Twilio). RevelAI does not operate its own telecommunications network or originate calls directly to the public switched telephone network (PSTN).

Although STIR/SHAKEN implementation is performed by our underlying voice service providers, RevelAI maintains a robocall mitigation program appropriate to its role to prevent the origination of illegal or unwanted robocall traffic.

Customer Vetting and Permitted Use:

RevelAI verifies customer organizations during onboarding and restricts platform use to legitimate healthcare communication workflows (e.g., care coordination, reminders, and clinical follow-up). Customers are contractually required to comply with applicable laws and regulations, including TCPA and HIPAA.

Consent and Patient-Level Controls:

All outbound communications are tied to a specific patient and active care episode. The platform enforces explicit patient consent prior to outreach, and messages or calls are not sent unless valid consent is recorded. Patients may opt out at any time via standard mechanisms (e.g., STOP/UNSUBSCRIBE), which are enforced immediately and prevent further outreach. Carrier-level unsubscribe signals are also honored automatically.

Use Restrictions and Safeguards:

The platform does not support bulk or broadcast dialing. All communications are initiated on a per-patient basis, preventing large-scale unsolicited calling campaigns. Outbound calling functionality is configurable at the customer level and can be disabled at any time.

Rate Limiting and Volumetric Controls:

RevelAI enforces rate limits and volumetric controls, including per-customer concurrency limits, daily call and message caps, and application-level throttling. These controls are designed to prevent excessive or anomalous calling behavior.

Monitoring and Detection:

Platform activity is continuously monitored for suspicious or anomalous patterns, including unusual call volumes or behavior inconsistent with expected healthcare workflows. Logging and monitoring systems support real-time visibility and alerting.

Enforcement and Response:

RevelAI maintains the ability to suspend or terminate accounts that violate acceptable use policies or present a risk of illegal robocalling. We cooperate with our telecommunications providers and will respond promptly to traceback requests from regulators, law enforcement, and industry partners, as applicable to our role.

Coordination with Upstream Providers:

RevelAI relies on its telecommunications providers (e.g., Twilio) for call authentication, attestation, and network-level mitigation measures, including STIR/SHAKEN compliance.

Through these combined controls, RevelAI takes reasonable steps to prevent the use of its platform for illegal robocalls and to support broader industry efforts to mitigate unwanted and fraudulent calling activity.