

Robocall Mitigation Program Description

Our company has implemented a comprehensive Robocall Mitigation Program designed to prevent unlawful or unwanted robocalls and to ensure compliance with applicable regulations and carrier requirements.

We only allow traffic from verified customers and require all clients to provide accurate business information, intended use case details, and sample message content prior to service activation. High-risk use cases, including prohibited or deceptive messaging, are strictly rejected.

To minimize unwanted traffic, we maintain opt-in and opt-out compliance. End users must provide prior express consent before receiving calls or messages. We honor opt-out requests immediately by adding numbers to suppression lists and blocking further communication. Standard keywords such as STOP, HELP, and INFO are supported and monitored.

We actively monitor traffic patterns for anomalies, including high-volume spikes, excessive complaints, invalid number targeting, or unusual calling behavior. Suspicious activity is flagged and investigated promptly. If potential violations are detected, we may temporarily suspend traffic, request clarification, or terminate the customer account.

We also maintain internal procedures for handling complaints from carriers, regulators, or end users. Upon receiving a complaint, we investigate the source, take corrective action, and implement additional safeguards where necessary.

Additionally, we work with upstream carriers and vendors that support STIR/SHAKEN and other call authentication frameworks where applicable. We cooperate with traceback requests and provide relevant information to authorized entities when required.

Through these measures, we aim to reduce illegal robocalls, protect consumers, and maintain responsible use of telecommunications services.