

Robocall Mitigation Program Description

Company Name: Kishek, Inc

Program Purpose:

Kishek Inc maintains a Robocall Mitigation Program designed to prevent the origination, transmission, and termination of illegal or unwanted robocalls on its network. This program aligns with FCC requirements, including the TRACED Act, and follows industry best practices to protect consumers from fraudulent, abusive, or unauthorized voice traffic.

Call Monitoring and Analytics:

We actively monitor voice traffic using automated and manual review processes to detect abnormal calling patterns, high-volume short-duration calls, invalid caller ID usage, and other indicators commonly associated with illegal robocalling activities.

STIR/SHAKEN Compliance:

Where technically feasible, Kishek Inc supports STIR/SHAKEN authentication to verify caller ID information and reduce caller ID spoofing. Calls that fail authentication or exhibit suspicious characteristics are subject to increased scrutiny or blocking.

Traffic Screening and Blocking:

We employ call screening tools and vendor-supported analytics to identify and block known illegal robocall sources, including calls associated with spoofed numbers, invalid numbering resources, or previously identified bad actors.

Customer Vetting and Acceptable Use:

All customers are required to comply with our Acceptable Use Policy, which strictly prohibits illegal robocalling, unsolicited automated calls, and any activity that violates federal or state regulations. We conduct reasonable due diligence during onboarding and reserve the right to suspend or terminate service for violations.

Complaint Handling and Enforcement:

We promptly investigate consumer complaints, traceback requests, and notices from regulatory authorities or industry partners. If illegal activity is confirmed, Kishek Inc takes immediate corrective action, which may include call blocking, service suspension, or termination.

Ongoing Review and Updates:

Our Robocall Mitigation Program is reviewed and updated regularly to address evolving threats, regulatory changes, and improvements in industry standards and technology.