TELGO | Robocall Mitigation Program Description

Vonoip Systems LLC, doing business as TELGO | October 20, 2026

1. Business and service overview

TELGO provides business communications services, including VoIP and AI-assisted call handling. This program describes TELGO's approach to preventing the use of its customer-facing services for illegal robocalls, caller-ID misuse, and related calling abuse.

2. Customer identification and authorized use

TELGO uses account-level authentication and security controls to limit access to its services. Its mitigation process includes reviewing customer identity and account activity when abuse indicators or complaints arise. TELGO seeks to ensure that calls and calling numbers are used only with appropriate customer authorization; suspected misuse is subject to review and service restriction.

3. Layered technical safeguards and automatic IP blocking

TELGO employs network firewalls, application-level security code, and AI-enabled platform capabilities to help protect its voice environment against unauthorized access and misuse. When an unauthorized request is detected, the originating source IP address is blocked to prevent continued access attempts. These security controls complement, but do not replace, review of potentially illegal calling traffic and abuse complaints.

4. Traffic assessment and upstream-provider oversight

TELGO assesses reports of anomalous or potentially unlawful traffic using available account information, call records, security events, and information from its connectivity provider, Bandwidth. Where traffic analytics or third-party blocking tools are used, their results inform further investigation; TELGO does not claim that any particular analytics vendor or automated call-blocking system is deployed unless separately documented. TELGO coordinates with Bandwidth when network-originating information or traffic restrictions are needed.

5. Mitigation actions and complaints

When illegal calling, unauthorized caller-ID use, a compromised account, or other abuse is suspected, TELGO investigates and may limit calling privileges, block affected traffic, disable access credentials, or suspend or terminate the customer account, as appropriate. TELGO reviews abuse complaints and takes measures reasonably designed to prevent recurrence.

6. Traceback cooperation and program administration

TELGO will cooperate with the FCC, law enforcement, and the registered industry traceback consortium to identify the source of suspected illegal calls, including responding to applicable traceback requests within 24 hours. TELGO will designate a responsible compliance contact, preserve and review relevant records consistent with law and its retention practices, and update this program as its service and mitigation controls evolve.

This description addresses robocall mitigation practices only. Technical call-authentication certifications are made separately in the FCC filing.