

Robocall Mitigation Program Description

PatientGrid, Inc.

1. Company Overview

PatientGrid, Inc. ("the Company") is a Voice over Internet Protocol (VoIP) service provider serving end users. The Company specializes in providing VoIP and unified communications services exclusively to healthcare providers, including medical and dental practices, located in the State of Florida.

The Company does not provide wholesale voice services and does not offer services to the general public. All services are provided directly to verified healthcare entities for legitimate business communications related to patient care, scheduling, and administrative operations.

The Company relies on a hosted VoIP platform provided by Ooma, Inc., utilizing its 2600Hz-based infrastructure. The Company resells access to the hosted platform's user interface (MonsterUI) and performs configuration, provisioning, and customer management within the hosted environment. The Company does not operate its own switching, signaling, or STIR/SHAKEN signing infrastructure.

2. STIR/SHAKEN Implementation

The Company has a STIR/SHAKEN implementation obligation and complies with that obligation through partial implementation, as permitted under applicable FCC rules.

STIR/SHAKEN authentication and attestation are implemented on portions of the call path through the Company's hosted VoIP platform and upstream service providers. Calls originated by the Company's end users are authenticated and signed by upstream providers where technically feasible.

The Company does not operate its own STIR/SHAKEN authentication services or signing infrastructure and therefore relies on its hosted platform and upstream carriers to perform STIR/SHAKEN signing and verification functions.

The Company's approach is consistent with and compliant with the requirements of 47 CFR § 64.6301 and 47 CFR § 64.6305, and all calls originated by the Company are subject to the Company's robocall mitigation program.

3. Customer Vetting and Onboarding

The Company maintains strict customer vetting and onboarding procedures designed to prevent illegal robocall activity.

Customer vetting includes identity verification through in-person visits for all new customers, business purpose validation limited exclusively to healthcare providers, review of intended call use, and acceptance of the Company's acceptable use and anti-robocall policies.

4. Traffic Monitoring and Mitigation

The Company monitors call traffic patterns on an ongoing basis to identify potentially illegal or suspicious calling behavior. Triggers for investigation include unusual call volumes or patterns inconsistent with healthcare use cases. Mitigation actions may include customer outreach, rate limiting, suspension, or termination of service.

5. Response to Traceback Requests

The Company commits to respond fully and within 24 hours to traceback requests from the Federal Communications Commission (FCC), law enforcement agencies, and the industry traceback consortium, and to cooperate in investigating and stopping illegal robocalls.

6. Enforcement and Escalation

When violations are identified, the Company documents findings, requires customer remediation when appropriate, and escalates to suspension or termination of service for confirmed violations. The Company cooperates with law enforcement and regulatory authorities as required.

7. Program Maintenance

The Company periodically reviews and updates this robocall mitigation program to ensure continued compliance with FCC rules and guidance. Internal responsibility for compliance oversight is assigned to management.

8. Contact Information

Compliance Contact: Andres Recarey, Vice President of Operations

Email: andres@patientgrid.io

Business Hours: Monday through Friday, 9:00 AM – 5:00 PM Eastern Time

Escalation procedures are in place to ensure timely responses to regulatory inquiries.