

Robocall Mitigation Program - Armored Gate LLC

Robocall Mitigation Program

Armored Gate LLC

FRN: 0038216214

Date: March 26, 2026

Prepared by: Karl Clinger, President

1. Introduction

Armored Gate LLC (“Armored Gate” or “the Company”) is a voice service provider, gateway provider, and non-gateway intermediate provider registered with the Federal Communications Commission (FCC). This document describes the Company’s Robocall Mitigation Program, implemented in compliance with Section 64.6305 of the FCC’s rules (47 C.F.R. § 64.6305).

Armored Gate is committed to preventing the origination, transmission, and termination of illegal robocall traffic on its network and takes reasonable steps to ensure compliance with applicable laws and regulations.

2. Company Overview

Armored Gate LLC provides voice communication services through its partnership with SkySwitch, a leading white-label Unified Communications as a Service (UCaaS) platform. The Company operates as a reseller and provider of voice, gateway, and intermediate provider services.

- **Business Address:** 111 W 4th Street, #23, Okmulgee, OK 74447
- **Phone:** (877) 276-4283
- **Email:** karl.clinger@armoredgate.com

3. STIR/SHAKEN Implementation

Armored Gate relies on its upstream platform provider, SkySwitch (operated by Sangoma Technologies), for STIR/SHAKEN call authentication. SkySwitch implements STIR/SHAKEN across its IP network infrastructure, and all calls originated through the Armored Gate platform are authenticated through SkySwitch's STIR/SHAKEN implementation.

As a reseller operating on the SkySwitch platform, Armored Gate does not independently operate the network infrastructure required for direct STIR/SHAKEN certificate authority participation. Instead, the Company benefits from and relies upon SkySwitch's compliant STIR/SHAKEN deployment for caller ID authentication on all IP-originated calls.

4. Robocall Mitigation Practices

Armored Gate has implemented the following reasonable steps to avoid originating, transmitting, or terminating illegal robocall traffic:

4.1 Customer Vetting and Onboarding

- All new customers undergo identity verification before service activation.
- The Company verifies the legitimacy of businesses requesting voice services.
- Customers must agree to an Acceptable Use Policy (AUP) that explicitly prohibits illegal robocalling, spoofing, and fraudulent call activity.

4.2 Monitoring and Detection

- The Company monitors call traffic patterns for anomalies that may indicate illegal robocall activity, including unusual call volumes, high short-duration call rates, and suspicious calling patterns.
- Traffic from customers exhibiting patterns consistent with illegal robocalling is flagged for review.

4.3 Enforcement and Remediation

- Upon identification of suspected illegal robocall activity, the Company takes prompt action, which may include:
 - Immediate suspension of the offending customer's service.
 - Investigation of the suspected activity.
 - Permanent termination of service for confirmed violators.
 - Cooperation with law enforcement and the FCC as appropriate.

- The Company maintains the right to immediately terminate service to any customer engaged in illegal robocall activity without prior notice.

4.4 Cooperation with Industry and Regulators

- Armored Gate cooperates with traceback requests from the Industry Traceback Group (ITG) and responds promptly to such requests.
- The Company cooperates with FCC enforcement actions and investigations related to illegal robocalls.
- The Company responds to requests from other voice service providers regarding suspected illegal traffic.

4.5 Network-Level Protections

- Through the SkySwitch platform, Armored Gate benefits from network-level call authentication and fraud detection mechanisms.
- The platform implements rate limiting and call volume controls to prevent abuse.
- Known bad actors and numbers associated with illegal robocall campaigns are blocked at the network level.

4.6 Record Keeping

- The Company maintains records of customer information, call detail records, and any enforcement actions taken in connection with suspected illegal robocall activity.
- Records are retained for a period consistent with FCC requirements and are made available to the Commission upon request.

5. Designated Robocall Mitigation Contact

Name: Karl Clinger

Title: President

Phone: (877) 276-4283

Email: karl.clinger@armoredgate.com

6. Commitment

Armored Gate LLC is committed to the ongoing evaluation and improvement of its Robocall Mitigation Program. The Company will update this program as necessary to address evolving threats and to remain

in compliance with FCC rules and regulations.

This Robocall Mitigation Program is filed pursuant to 47 C.F.R. § 64.6305 and is effective as of the date indicated above.