

ROBOCALL MITIGATION PROGRAM DESCRIPTION

FCC Robocall Mitigation Database Filing

Date: May 28, 2026

1. Company Information

Field	Information
Legal Name	GIGAKOM
DBA Name	None
Primary Point of Contact	Andrej Komatina (CEO)
Phone	858-769-5408
Email	AK@GIGAKOM.COM

2. Service Provider Classification

GIGAKOM, is filing as a **Voice Service Provider**. GIGAKOM operates as a **reseller** of voice telecommunications services provided by SkySwitch. GIGAKOM does not own or operate its own underlying network infrastructure and relies entirely on SkySwitch for the origination, transport, and termination of voice traffic.

3. STIR/SHAKEN Implementation Status

Certification: Option 3 — No STIR/SHAKEN Implementation

GIGAKOM has not implemented the STIR/SHAKEN authentication framework on any portion of its network. This is because:

- GIGAKOM is a reseller and does not hold, control, or own its own STIR/SHAKEN certificates or SPC tokens
- All calling traffic is originated through Sky Switch's network infrastructure
- Sky Switch, as the upstream service provider, is responsible for STIR/SHAKEN signing and attestation decisions using Sky Switch's own certificates
- GIGAKOM does not have the technical capability to sign or authenticate calls on its own network

This certification is made pursuant to 47 CFR § 64.6305(a) and in accordance with the FCC's guidance that a provider must make all attestation decisions using its own certificate registered with the STIR/SHAKEN Policy Administrator.

4. Robocall Mitigation Program

4.1 Overview

GIGAKOM has implemented a comprehensive robocall mitigation program designed to prevent the origination of illegal robocall traffic on its network. This program satisfies the requirements of 47 CFR § 64.6305(d)(ii)-(iii) and applies to all calls originated, transmitted, or terminated by GIGAKOM

4.2 Know Your Customer (KYC) Procedures

GIGAKOM maintains customer verification procedures including:

- a) **Customer Identification:** All new customers are required to provide valid business registration documents, government-issued identification for principals, and proof of authorized use of calling numbers (ANI).
- b) **Business Purpose Verification:** GIGAKOM verifies the legitimate business purpose of each customer including confirmation that the customer's intended use of voice services is lawful and consistent with FCC regulations.
- c) **Creditworthiness Assessment:** Prior to provisioning service, GIGAKOM conducts a credit review and assesses the customer's history in the industry.
- d) **Customer Acceptance Criteria:** GIGAKOM reserves the right to decline service to any customer whose intended use presents an elevated risk of illegal robocalling including customers with no verifiable physical presence or legitimate business purpose.

4.3 Monitoring and Traffic Analysis

- a) **Traffic Monitoring:** GIGAKOM monitors calling patterns across its customer base to identify anomalies including unusual call volumes, high call abandonment rates, and short duration calls.
- b) **Complaint Tracking:** GIGAKOM maintains a complaint tracking system to receive and investigate reports of illegal robocalling originating from or terminating to its customers.
- c) **Real-Time Mitigation:** Where technically feasible, GIGAKOM implements tools to detect and block suspicious traffic patterns in real-time.
- d) **Periodic Audits:** GIGAKOM conducts periodic audits of customer traffic to ensure compliance with this mitigation program and applicable law.

4.4 Response to Traceback Requests

Pursuant to 47 CFR § 64.6305(a), GIGAKOM commits to fully cooperate with all traceback requests from:

- The Federal Communications Commission (FCC)
- Law enforcement agencies
- The industry traceback consortium (including the Communications Security, Reliability, and Interoperability Council (CSRIC) traceback efforts)

Response Commitment: GIGAKOM will respond to all traceback requests within 24 hours of receipt. GIGAKOM will provide all available information necessary to identify the source of illegal robocall traffic including:

- Customer identification and account information
- Call detail records (CDRs)
- Originating IP addresses (where applicable)
- Date, time, and duration of calls
- Any other relevant information in GIGAKOM's possession

4.5 Cooperation with Law Enforcement and Regulatory Authorities

GIGAKOM commits to fully cooperate with the FCC, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that use GIGAKOM's service to originate or terminate calls. This includes:

- Providing timely responses to subpoenas, cease and desist letters, and other official requests
- Preserving relevant records as required by law
- Taking immediate action to suspend or terminate service to customers found to be engaged in illegal robocalling
- Participating in industry-wide efforts to combat illegal robocalling

4.6 Customer Education and Terms of Service

a) **Acceptable Use Policy:** GIGAKOM's Terms of Service and Acceptable Use Policy explicitly prohibit the use of its services for illegal robocalling, telephone solicitation in violation of the Telephone Consumer Protection Act (TCPA), and other unlawful communications.

b) **Customer Acknowledgment:** All customers are required to acknowledge the Acceptable Use Policy prior to receiving service. c) **Termination for Cause:** GIGAKOM reserves the right to immediately suspend or terminate service to any customer found to be in violation of applicable law or this mitigation program.

4.7 Recordkeeping

GIGAKOM maintains records related to its robocall mitigation efforts including:

- Customer intake documentation
- KYC records
- Traffic monitoring logs
- Complaint records
- Traceback request responses
- Customer termination records

These records will be retained for a minimum of **five (5) years** and made available to the FCC, law enforcement, or the industry traceback consortium upon request.

5. Exemption Claim (If Applicable)

If GIGAKOM claims any exemption from STIR/SHAKEN requirements (e.g., small provider exemption under 47 CFR § 64.6301), the following explanation is provided: GIGAKOM will consult with telecom counsel to determine if any exemption applies. Common exemptions might include: small provider status, service provider for inmate calling services, or other statutory exemptions.

6. Certification

The undersigned hereby certifies that:

1. All calls that GIGAKOM originates on its network are subject to this robocall mitigation program, which includes reasonable steps to avoid originating illegal robocall traffic.
2. GIGAKOM will respond fully within 24 business hours to all traceback requests from the FCC, law enforcement, and the industry traceback consortium.
3. GIGAKOM will cooperate fully with the FCC, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that use GIGAKOM's service.

4. This certification has not been removed by Commission action, and GIGAKOM has not been prohibited from filing in the Robocall Mitigation Database by the Commission.

5. GIGAKOM has not implemented the STIR/SHAKEN authentication framework on any portion of its network (Option 3 certification).

6. The information provided in this filing is true and accurate to the best of the undersigned's knowledge, information, and belief.

Printed Name: Andrej Komatina

Title: CEO

Signature:

A handwritten signature in blue ink, appearing to read "A. Komatina", written over a horizontal line.

Date: ____May 28, 2026____