



Robocall Mitigation Program Description

Company: geoIM

Type of Provider: Voice Service Provider (UCaaS)

Underlying Platform: SkySwitch

1. Overview

geoIM is a voice service provider delivering hosted UCaaS solutions through the SkySwitch platform. geoIM is committed to preventing the origination of illegal robocalls on its network and complies with all FCC requirements under 47 CFR § 64.6300–64.6306. This Robocall Mitigation Program outlines the policies, procedures, and technical safeguards we use to ensure that only legitimate traffic is originated by our customers.

2. STIR/SHAKEN Implementation Status

geoIM relies on SkySwitch's STIR/SHAKEN implementation for calls that traverse IP networks. All eligible SIP traffic is authenticated and signed using STIR/SHAKEN. For traffic that cannot be signed (e.g., TDM interconnects), geoIM applies the mitigation measures described in this document.

3. Know-Your-Customer (KYC) Procedures

geoIM uses strict customer vetting procedures before enabling outbound calling:

- **Business identity verification**
 - EIN verification
 - State business registration
 - Matching service address and billing information
- **Responsible party verification**
 - Government-issued ID
 - Direct contact validation
- **Service use-case review**
 - Expected call volume
 - Nature of business
 - Calling patterns consistent with legitimate operations
- **Prohibited use disclosure**
 - Customers must agree not to use geoIM services for illegal robocalling or TCPA violations.

geoIM reserves the right to deny service to any applicant whose use case appears inconsistent with lawful calling practices.

4. Ongoing Monitoring and Traffic Analysis

geoIM continuously monitors outbound traffic for patterns associated with illegal robocalling, including:

- High-volume short-duration calls
- Repetitive sequential dialing
- Sudden spikes in call attempts
- High answer-seizure ratio anomalies
- Traffic inconsistent with the customer's stated use case

geoIM uses analytics tools provided by SkySwitch and third-party monitoring systems to identify suspicious behavior.

5. Call Blocking and Remediation Procedures

If geoIM detects suspicious or potentially unlawful calling activity:

1. **Immediate investigation**
 - Review call logs, patterns, and customer history
 - Contact customer for explanation or remediation
2. **Mitigation actions** may include:
 - Rate limiting
 - Temporary suspension of outbound calling
 - Blocking specific destinations or call types
 - Permanent termination of service
3. **Escalation**
 - geoIM will promptly notify upstream carriers if traffic appears unlawful
 - geoIM will cooperate with traceback requests from the Industry Traceback Group (ITG)

geoIM responds to traceback requests **within 24 hours**, as required by the FCC.

6. Customer Education and Acceptable Use Policy

All customers must agree to geoIM's Acceptable Use Policy (AUP), which explicitly prohibits:

- Illegal robocalling
- Caller ID spoofing
- Use of auto-dialers without consent
- Any activity violating the TCPA or FCC rules

geoIM provides customers with guidance on compliant calling practices and updates them when regulations change.



7. Recordkeeping

geoIM maintains records of:

- Customer onboarding documentation
- KYC verification
- Traffic monitoring alerts
- Traceback responses
- Mitigation actions taken

Records are retained for a minimum of **two years**, or longer if required by law.

8. Compliance Contact

Name: Carl Powers

Title: President

Email: info@geoim.com

Phone: 910-221-1962

This individual is responsible for responding to traceback requests, FCC inquiries, and compliance matters.

9. Certification

geoIM certifies that it has implemented the above robocall mitigation practices and will continue to monitor and prevent the origination of illegal robocalls on its network.

Authorized Signatory: *Carl Powers*

Title: President

Date: 03-18-2026