

ROBOCALL MITIGATION PLAN

Filer: GigaParts, Inc.

Covered Entities: GigaParts, Inc. (and all subsidiaries)

Filing Date: June 2026

Regulatory Authority: FCC 47 CFR § 64.6305

1. Introduction & Company Overview

GigaParts, Inc. operates primarily as a downstream Voice Service Provider (Originating Provider). The company resells Voice over Internet Protocol (VoIP) services to commercial end-users, integrating these services into custom hardware, software, and network solutions.

GigaParts, Inc. does not maintain legacy TDM/non-IP infrastructure and does not operate as an intermediate or gateway carrier for third-party transit traffic. This Robocall Mitigation Plan (RMP) covers GigaParts, Inc. and all of its corporate subsidiaries.

2. STIR/SHAKEN Implementation Status

As a reseller of VoIP services, GigaParts, Inc. implements its offerings via an underlying upstream wholesale platform. GigaParts, Inc. does not directly issue or generate cryptographic STIR/SHAKEN certificates on its own network core; instead, caller ID authentication capabilities under the STIR/SHAKEN framework are fully provisioned, executed, and passed through via GigaParts, Inc.'s wholesale upstream provider, SkySwitch.

To ensure complete regulatory coverage and network compliance, GigaParts, Inc. executes this Robocall Mitigation Plan to actively prevent the origination of illegal or unverified robocall traffic on behalf of its direct end-users.

3. "Know Your Customer" (KYC) Protocols

GigaParts, Inc. enforces strict "Know Your Customer" (KYC) procedures during the onboarding and renewal processes to guarantee that malicious or illegal actors are denied network access.

In-Person & Direct Verification: Company representatives meet with all prospective commercial customers in person or via verified direct consultations.

Business Credentialing: GigaParts, Inc. collects and authenticates corporate documentation, verifying the legal business entity type, checking active business licenses, and confirming tax registration details against state databases before provisioning any services.

Use Case & Volume Assessment: During onboarding, GigaParts, Inc. reviews the client's intended business use case and anticipated call volumes to ensure their traffic profile aligns with standard, lawful

business practices.

Contractual Safeguards: Customer Service Agreements include explicit, legally binding clauses that strictly prohibit the transmission of illegal robocalls, telemarketing violations, or predatory autodialed traffic, with immediate termination penalties for non-compliance.

4. Call Analytics, Monitoring, and Suspicious Traffic Detection

GigaParts, Inc. continuously monitors call traffic generated across its solutions utilizing advanced cloud-native analytical tools and reporting software integrated via its underlying platform partner, SkySwitch.

Behavioral Detection: The network analytics systems actively monitor for known signatures of illegal robocalling, including sudden, anomalous traffic spikes, high ratios of short-duration calls (less than 6 seconds), and abnormally high error rates or unanswered/busy signals.

Real-Time Guardrails: Specialized Session Border Controller (SBC) capabilities and automated security logic provided through the SkySwitch ecosystem continuously evaluate outbound traffic streams to isolate and flag structural irregularities.

5. Network-Based Blocking, Spoofing Prevention & Enforcement

When suspicious or illicit traffic profiles are detected, GigaParts, Inc. employs a swift, definitive response mechanism to protect the Public Switched Telephone Network (PSTN):

Automated Trunk Suspension: If an active, unauthorized robocalling campaign or a massive surge of unverified traffic triggers system thresholds, an automated network alert is generated, and outbound traffic on the offending SIP trunk is immediately and automatically halted.

Manual Review and Intervention: Following an automated lockout, technical analysts at GigaParts, Inc. intervene to perform a manual review of the subscriber's account, request immediate justification for the traffic spike, and perform traceback investigations before service can be considered for restoration.

Caller ID Verification & Spoofing Prevention: GigaParts, Inc. prohibits unverified caller ID manipulation. Outbound Caller ID fields must strictly match the verified legal business name and authorized telephone numbers established via the customer's business license and onboarding documentation.

6. Strict 24-Hour Traceback Commitment

GigaParts, Inc. is fully committed to the rapid mitigation of illegal traffic and complies entirely with the FCC's mandatory traceback enforcement standards.

GigaParts, Inc. officially pledges to fully cooperate with and respond to all traceback requests from the Industry Traceback Group (ITG), the Federal Communications Commission (FCC), federal civil authorities, and state law enforcement agencies within 24 hours of receipt.

Designated Traceback Point of Contact:

Dedicated Email Address: techdesk@gigaparts.com

Process: Incoming traceback requests sent to this address automatically generate a high-priority ticket in the GigaParts, Inc. queue, notifying a dedicated system analyst to investigate, isolate the call path source, and deliver a comprehensive response within the mandatory 24-hour window.