# Robocall Mitigation Program Description

Prepared: 18 November 2026.

## 1. Filing entity and services

Legal entity: Callgear FZCO
FRN: 0039252440
Business address: Unit 1301 Fortune Executive Tower, Plot No: JLT-PH2-T1A, Jumeirah Lake Towers, JLT, 282741, Dubai
Responsible officer: Georgi Valerivich Makarenko, general manager

Robocall mitigation contact: Georgi Valerivich Makarenko, service@callgear.com, +971569924774

Monitored traceback contact and backup: support@callgear.com

The filer serves customers located both in the United States and internationally. Its services include domestic calls within the United States and international calling

## 2. Network role and STIR/SHAKEN status

[The filer provides voice services to end users and routes calls through third-party telecommunications providers. The filer has not implemented STIR/SHAKEN on its own network.

3. Scope and accountability

The program covers all calls handled through the filer's services. The designated officer oversees robocall mitigation, corrective actions, and RMD filing accuracy. Illegal robocalls and unlawful caller ID spoofing are prohibited.

## 4. Customer verification and ongoing review

Before activating service, the filer verifies each customer's identity, business registration, address and contact details, and reviews their business activities and intended use. Service is not activated if material discrepancies remain unresolved.

Existing customers are reviewed when complaints, unusual traffic or material changes arise. Higher-risk customers undergo additional verification.

## 5. Caller ID and acceptable use

Customers may use only telephone numbers assigned to their accounts through CallGear. Suspected unauthorized caller ID use, impersonation or spoofing is investigated, and affected services may be restricted or suspended.
For externally provided numbers, customers must provide proof of ownership or authorization before use.

## 6. Traffic monitoring and analytics

The filer uses Internal systems to manually review CDRs and traffic reports for unusual calling patterns. The responsible team also reviews customer complaints and provider alerts, investigates suspicious activity, and documents corrective actions. No automated robocall analytics or real-time blocking system is used.

## 7. Provider due diligence and routing

The filer verifies directly connected providers' business details, contacts and network roles before routing traffic. For providers subject to RMD requirements, the filer checks their listings and reviews their filings and mitigation plans. Provider status is reviewed by procurement team and following complaints, enforcement notices or material changes. Where required, traffic exchange with unlisted or removed providers is blocked through routing

## 8. Complaints, investigation and enforcement

The filer records complaints and carrier notices and reviews relevant call records, customer details and caller ID authorization. Suspected unlawful activity is investigated, and affected traffic may be restricted or suspended. Confirmed violations may result in account termination. Evidence, corrective actions and conditions for restoring service are documented.

## 9. Traceback cooperation

The filer commits to responding fully within 24 hours to all traceback requests from the FCC, law enforcement and the industry traceback consortium, and to cooperating in investigating and stopping illegal robocalls. A designated contact and backup monitor requests, retrieve relevant customer and call records, and coordinate secure responses.

## 10. Records, training and program review

The filer retains CDRs for 2 years and customer verification documents, number authorizations, customer reviews, complaints, provider checks and traceback responses for 2 years. Records are stored in internal system, with access restricted to authorized staff and protected by 3rd party.

Relevant staff receive training on customer verification, suspicious traffic, complaint handling and traceback requests. The program is reviewed following significant incidents and material regulatory or operational changes. Reviews and corrective actions are documented, and the RMD filing is updated as required.

## 11. Completion and approval

Before filing: complete all bracketed fields; replace proposed controls with verified current procedures; resolve the STIR/SHAKEN status and supporting legal basis; confirm exact entity details and designated contacts; remove drafting notes; and obtain approval from the authorized officer.

Approved legal entity: Callgear FZCO
Authorized officer:  Georgi Valerivich Makarenko, general manager
Approval date: 18.11.2026
Effective date: 18.11.2026