

Robocall Mitigation Program Description



RFCG COMPUTER S.R.L.

Foreign Voice Service Provider | Dominican Republic

FCC Registration Number (FRN)	0038980777
Business Name	RFCG COMPUTER S.R.L.
Doing Business As (DBA)	GLOWICOM
Business Address	Rafael Augusto Sanchez No. 17, Distrito Nacional 10119, Santo Domingo, Dominican Republic
Provider Filing Type	Voice Service Provider
Foreign Voice Service Provider	Yes - Dominican Republic
STIR/SHAKEN Certification	Option 3 - No STIR/SHAKEN Implementation
Program Version / Date	Version 1.0 - October 6, 2026

Purpose. This document describes the robocall mitigation program that will be maintained by RFCG COMPUTER S.R.L. ("RFCG COMPUTER S.R.L." or "GLOWICOM") for voice services that RFCG intends to provide to its customers, including services that will use North American Numbering Plan (NANP) resources and underlying telecommunications providers for U.S. and Canadian DID services and call termination.

Public filing. This version is intended for submission to the FCC Robocall Mitigation Database and does not contain customer credentials, network passwords, detailed security configurations, or other sensitive operational information.

1. PROVIDER STATUS AND SCOPE

RFCG COMPUTER S.R.L. is organized and operates in the Dominican Republic and intends to provide voice services to business customers, including hotels and other commercial entities. RFCG COMPUTER S.R.L. will use underlying telecommunications providers, including Sangoma, for DID services and for the termination of customer calls to the United States and Canada.

RFCG COMPUTER S.R.L. will identify itself in the RMD as a foreign voice service provider. RFCG COMPUTER S.R.L. has not implemented the STIR/SHAKEN authentication framework on its own network and will file under Option 3 - No STIR/SHAKEN Implementation based on its status as a foreign provider. This mitigation program will apply to all calls originated through RFCG COMPUTER S.R.L. voice services that are within the scope of the RMD filing.

2. PROGRAM OBJECTIVES AND GOVERNANCE

RFCG COMPUTER S.R.L. will maintain this program to take reasonable steps to prevent its services from being used to originate illegal robocall traffic, to identify and address suspicious calling activity, and to cooperate with the FCC, law enforcement, the Industry Traceback Group/Consortium, underlying providers, and other appropriate industry participants.

- Apply customer due diligence before voice service activation and throughout the customer relationship.
- Restrict use of caller identification information to numbers the customer is authorized to use.
- Review reported or anomalous traffic and take proportionate corrective action, including suspension or termination when warranted.
- Respond fully and within 24 hours to traceback requests from the Commission, law enforcement, or the industry traceback consortium, consistent with the certification made in the RMD.
- Maintain records reasonably necessary to investigate complaints, traceback requests, and suspected misuse of the service.

3. KNOW YOUR CUSTOMER (KYC) PROCEDURES

RFCG COMPUTER S.R.L. intends to provide business voice services and will apply customer-identification procedures designed to know its end-user customers and reduce the risk that anonymous or fraudulent actors obtain voice service.

3.1 Onboarding

- Obtain the customer legal/business name, commercial name where applicable, principal business address, primary contact information, and the identity of authorized technical and administrative contacts.
- Validate that the requested service is consistent with the customer business purpose, including the expected use of PBX, SIP trunk, DID, hotel telephony, or other enterprise voice services.
- Maintain a contractual or commercial relationship tying the customer to the service, assigned accounts, SIP trunks, DIDs, and billing records.
- Where risk indicators are present, RFCG COMPUTER S.R.L. may request additional business documentation or clarification before activation or expansion of service.

3.2 Ongoing Customer Review

- Update customer contact and service information when material changes are identified.
- Review complaints, traceback notices, unusual traffic patterns, or unauthorized caller-ID use as potential triggers for enhanced customer review.
- Require customers to cooperate with RFCG COMPUTER S.R.L. investigations relating to suspected unlawful calling activity.

4. CALLER ID, NUMBER USE, AND ANTI-SPOOFING CONTROLS

RFCG COMPUTER S.R.L. will prohibit customers from knowingly transmitting false or misleading caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value, or otherwise using RFCG COMPUTER S.R.L. services for unlawful spoofing or illegal robocalling.

- Customer calling-number presentation is limited to numbers assigned to the customer or numbers for which the customer represents that it has a legitimate right of use.
- RFCG COMPUTER S.R.L. may require supporting information when a customer requests presentation of a number not directly assigned through RFCG COMPUTER S.R.L. or its underlying provider.
- RFCG COMPUTER S.R.L. may block, normalize, remove, or reject caller-ID information that is invalid, malformed, unauthorized, or inconsistent with service configuration.
- Use of emergency-service numbers, unassigned numbers, or numbers associated with another party without authorization is prohibited.

5. TRAFFIC MONITORING AND DATA ANALYTICS

RFCG COMPUTER S.R.L. will not rely on a standalone third-party robocall analytics platform as the sole basis of its mitigation program. RFCG COMPUTER S.R.L. will use operational records available from its voice platform and underlying providers, including call detail records (CDRs), SIP signaling records, customer/account information, complaint information, and provider notices, to investigate suspicious activity. RFCG COMPUTER S.R.L. may also rely on analytics, fraud controls, or network intelligence made available by its underlying provider(s), including Sangoma.

Indicators that may prompt review include unusually high call volume, abrupt changes in traffic profile, repeated short-duration calls, repeated calls to large ranges of destinations, complaints, traceback requests, invalid caller-ID patterns, or other behavior inconsistent with the customer's expected business use.

6. KNOW YOUR UPSTREAM PROVIDER (KYUP) PROCEDURES

RFCG COMPUTER S.R.L. will evaluate and maintain information concerning the providers that will be used to deliver voice services and terminate traffic. RFCG COMPUTER S.R.L. intends to use Sangoma as an underlying provider for U.S. and Canadian DID services and call termination.

- Maintain current commercial and technical contact information for underlying providers.
- Use established provider accounts and contractual/commercial arrangements for voice connectivity and numbering services.
- Maintain information sufficient to identify the upstream route/provider used for affected traffic when investigating complaints or traceback requests, to the extent such information is available to RFCG COMPUTER S.R.L..
- Cooperate with underlying providers on abuse, fraud, traceback, caller-ID, and robocall mitigation matters.

7. TRACEBACK RESPONSE AND COOPERATION

RFCG COMPUTER S.R.L. will respond fully and within 24 hours to traceback requests from the FCC, law enforcement, and the industry traceback consortium/Industry Traceback Group. The response process will be designed to identify the relevant customer, account, calling number, call records, and upstream or downstream routing information available to RFCG COMPUTER S.R.L..

7.1 Traceback Handling Procedure

- Validate and log the request, including the calling number, called number, timestamp, time zone, and requesting entity.
- Search available CDRs, SIP records, customer account information, and provider records for the identified call.
- Identify the customer/account and the relevant underlying provider or route, where available.
- Respond to the requesting entity with responsive information available to RFCG COMPUTER S.R.L. within the required timeframe, subject to applicable law and legitimate confidentiality constraints.
- Escalate suspected unlawful or abusive activity for mitigation action and, when appropriate, coordinate with the underlying provider.

8. COMPLAINT, ABUSE, AND INCIDENT RESPONSE

RFCG COMPUTER S.R.L. will review credible reports of illegal robocalling, spoofing, fraud, and other abuse associated with its services. Reports may originate from customers, called parties, upstream providers, law enforcement, traceback organizations, or other industry participants.

- Preserve relevant records reasonably available for the investigation.
- Contact the customer when clarification or corrective action is required.
- Restrict affected DIDs, caller-ID configurations, trunks, destinations, or account capabilities where necessary to mitigate ongoing risk.
- Suspend or terminate service when the customer fails to cooperate, provides materially false information, or RFCG COMPUTER S.R.L. determines that continued service presents an unacceptable risk of illegal robocalling or spoofing.
- Document material actions taken in response to significant abuse events.

9. CUSTOMER TERMS AND ENFORCEMENT

RFCG COMPUTER S.R.L. voice services will not be permitted to be used for unlawful robocalling, fraudulent calling, illegal spoofing, harassment, or other unlawful activity. RFCG COMPUTER S.R.L. will reserve the right to investigate suspected abuse and to impose restrictions, suspend service, or terminate service when necessary to protect the network, comply with law or regulatory requirements, respond to provider notices, or stop unlawful activity.

RFCG COMPUTER S.R.L. may require a customer to provide additional information concerning traffic origin, business purpose, caller-ID authorization, or calling practices as a condition of continued service.

10. RECORDKEEPING

RFCG COMPUTER S.R.L. will maintain records reasonably necessary to administer its voice services and this mitigation program, including customer/account information, assigned DIDs and service configuration information, billing and commercial records, and available CDR/SIP records. Records relevant to an active abuse investigation or traceback request will be

11. STIR/SHAKEN STATUS AND FOREIGN PROVIDER BASIS

RFCG COMPUTER S.R.L. is a foreign voice service provider organized and operating from the Dominican Republic. RFCG COMPUTER S.R.L. has not implemented STIR/SHAKEN on any portion of its own network and therefore will certify in the RMD under Option 3 - No STIR/SHAKEN Implementation. RFCG COMPUTER S.R.L. understands that its future use of an underlying provider that may implement STIR/SHAKEN will not, by itself, constitute RFCG COMPUTER S.R.L. implementation of STIR/SHAKEN.

RFCG COMPUTER S.R.L. will update its RMD filing and this program description as necessary if its network, regulatory status, STIR/SHAKEN implementation status, or material robocall mitigation practices change.

12. PROGRAM REVIEW AND RESPONSIBLE PERSONNEL

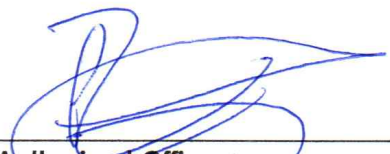
Responsibility for this program will be assigned to RFCG COMPUTER S.R.L. management and operational personnel responsible for voice services. The program will be reviewed periodically and after material changes to the voice service, significant abuse incidents, or changes in applicable FCC requirements.

Principal / Operations	Rusbelt Cuevas - Vice President of Operations
Principal / Executive	Heberto Aquino - Executive Vice President
Robocall Mitigation Contact	RFCG COMPUTER S.R.L. / GLOWICOM - Operations

13. REGULATORY REFERENCES

- 47 CFR § 64.6305 - Robocall Mitigation Database filing and mitigation requirements.
- 47 CFR § 64.1200(n)(4) - Know-your-customer requirements applicable to voice service providers.
- 47 CFR § 64.6300(c) - Definition of foreign voice service provider.
- FCC Robocall Mitigation Database, Frequently Asked Questions for Filers (updated July 9, 2026).
- FCC Robocall Mitigation Database External Filing Instructions (July 2026).

Adoption and accuracy statement. This program description is intended to describe the robocall mitigation policies and procedures that RFCG COMPUTER S.R.L. will implement and maintain for the voice services covered by its RMD filing. RFCG COMPUTER S.R.L. will revise the filing and this program description when required by applicable FCC rules.


Authorized Officer
RFCG COMPUTER S.R.L.
Date: 6-10-2026

