

Grace Communications LC

Robocall Mitigation Plan

Document Owner	Grace Communications LC
Authorized Company Representative	Darla Cokeley, Owner
Operational Contact	Al Speelman, MOV Technologies
Effective Date	8/1/2026
Annual Review Date	July 1 of each year

1. Purpose and Scope

This plan describes the procedures Grace Communications LC ("GC") uses to prevent, identify, investigate, and stop illegal robocalling, unlawful caller-ID spoofing, fraud, and other abusive calling activity originating through GC-provided services.

This plan applies to all GC customers, telephone numbers, extensions, administrators, contractors, credentials, and outbound calling activity.

GC provides retail voice services to end-user customers. GC does not knowingly accept wholesale, gateway, or intermediate-provider traffic from unaffiliated third-party carriers.

2. Network and STIR/SHAKEN Structure

GC obtains telephone numbers and public switched telephone network connectivity through Telnyx LLC. Outbound calls placed through GC service are routed through Telnyx for termination and applicable STIR/SHAKEN authentication.

GC does not currently maintain its own Operating Company Number, Service Provider Code token, STIR/SHAKEN certificate, or hosted-signing service. GC relies on Telnyx to perform applicable call authentication based on the originating customer account, assigned telephone number, and information available to Telnyx.

GC maintains records associating each customer with the telephone numbers, extensions, devices, and credentials authorized for that customer's use.

GC does not permit customers to independently alter call-routing or authentication arrangements in a manner that bypasses GC or Telnyx controls.

3. Customer Verification and Due Diligence

Before commercially activating a new customer, renewing service, or approving a material expansion or change in service, GC takes affirmative and effective measures to identify the customer and evaluate the intended use of the service.

GC ordinarily collects and records:

- The customer's legal name or legal business name.
- The customer's service and billing addresses.
- The name and contact information of a responsible individual.
- A working telephone number and email address.
- Payment and billing information.
- The nature of the customer's business or intended use of the service.
- The telephone numbers, extensions, devices, and credentials assigned to the customer.
- The outbound caller-ID numbers the customer is authorized to present.

GC verifies that each customer is authorized to use each presented outbound caller-ID number. GC-provided accounts are ordinarily configured so customers cannot freely present unapproved outbound caller-ID numbers.

GC may request additional documentation when verification cannot be completed through ordinary business records or when elevated risk indicators are present. Additional documentation may include:

- Government-issued identification.
- Business-registration records.
- Proof of service or billing address.
- Proof of telephone-number ownership or authorization.
- Information establishing a legitimate business or personal use for the service.
- Other supporting records reasonably necessary to verify the customer or intended service use.

Additional review may be performed when a customer:

- Requests high-volume or automated calling capability.
- Provides inconsistent, incomplete, or unverifiable information.
- Cannot demonstrate a legitimate purpose for the requested service.
- Requests authorization to present a caller-ID number not supplied by GC.
- Experiences a sudden or unexplained change in calling volume or traffic pattern.
- Presents another indicator of potential fraud, abuse, or illegal calling activity.

Accounts may remain restricted, may be denied activation, or may be suspended until verification is complete.

GC may periodically reverify customer information and may require reverification when customer ownership, responsible contacts, payment information, service use, calling volume, caller-ID authorization, or other material account information changes.

4. Prohibited Conduct

Customers and other users of GC services may not engage in any of the following conduct:

- Presenting a caller-ID number that the customer does not own or is not authorized to use.
- Making illegal prerecorded, artificial-voice, or automatically dialed calls.
- Making fraudulent, deceptive, harassing, threatening, or impersonation calls.
- Making calls intended to defraud, mislead, or unlawfully obtain money, property, credentials, or personal information.
- Conducting high-volume dialing, lead generation, political calling, debt-collection calling, telemarketing, prerecorded calling, or automated dialing without GC's prior written approval and documentation demonstrating compliance with applicable law.

- Sharing account credentials with unauthorized parties.
- Reselling GC service without written authorization.
- Laundering or disguising traffic for another person or provider.
- Attempting to bypass caller-ID, call-routing, authentication, volume, destination, or fraud controls.
- Using GC service in violation of federal, state, or local law.
- Using GC service in violation of applicable Telnyx acceptable-use requirements.

GC customer terms prohibit illegal and abusive traffic, unauthorized caller-ID presentation, unauthorized credential sharing, unapproved service resale, traffic laundering, and circumvention of calling restrictions.

GC reserves the right to investigate, restrict, suspend, or terminate service when prohibited conduct, illegal traffic, or a material risk of abuse is identified.

5. Monitoring and Detection

GC monitors available information for indicators of illegal or abusive calling activity.

Information reviewed may include:

- Call-detail records.
- Telnyx alerts and notices.
- Customer and third-party complaints.
- Traceback requests.
- Unusual or unexplained calling volume.
- Sudden traffic spikes.
- Repeated short-duration calls.
- High concentrations of calls to sequential or similar destinations.
- Invalid, unusual, or high-risk destinations.
- Failed registration or authentication attempts.
- Unauthorized caller-ID presentation.
- Repeated use of newly created or changed credentials.
- Calling activity inconsistent with the customer's stated purpose.
- Other indicators of fraud, abuse, or unlawful activity.

GC does not rely upon a single volume, duration, destination, or numerical threshold to determine whether traffic is unlawful. Activity is evaluated in context based on the customer, account history, stated use, traffic pattern, complaints, carrier information, and other available evidence.

New accounts, recently changed accounts, accounts using new credentials, and accounts approved for unusual or elevated calling volume may receive additional review.

6. Complaint, Traceback and Investigation Procedures

GC documents and investigates complaints, traceback requests, Telnyx notices, and other credible reports of potentially illegal or abusive traffic.

6.1 Complaint and Investigation Process

Stage	Required Action
Log	Record the date, reporting party, affected number, calling number, time of calls, complaint details, and available evidence.
Preserve	Retain relevant call-detail records, Telnyx notices, account data, and customer communications.
Contain	Restrict outbound calling, disable affected credentials, or suspend service when immediate risk exists.
Investigate	Review traffic patterns, verify caller-ID authorization, contact the customer when appropriate, request supporting documentation, and coordinate with Telnyx or other appropriate parties.
Resolve	Restore service, impose continued restrictions, require corrective action, terminate the account, or refer the matter to an appropriate authority based on the findings.
Document	Record the investigation, supporting evidence, actions taken, final disposition, and any continuing restrictions or monitoring requirements.

GC may restrict or suspend service before completing an investigation when immediate action is reasonably necessary to protect consumers, the public telephone network, GC, Telnyx, or another provider.

6.2 Traceback and Government Requests

GC commits to responding fully within 24 hours of receipt of traceback requests from:

- The Federal Communications Commission.
- Federal, state, local, or other authorized law-enforcement authorities.
- The Commission-designated industry traceback consortium.

GC will cooperate with these entities in investigating and stopping illegal robocallers that originate calls through or otherwise use GC services.

GC will preserve and provide available customer, account, telephone-number, credential, routing, and call-detail information as permitted or required by law.

The Robocall Mitigation and Technical Contact is responsible for receiving, investigating, and preparing operational responses to traceback requests. The Authorized Company Representative retains authority to certify company responses and take actions requiring authorization on behalf of GC.

7. Enforcement

GC may warn, restrict, suspend, or terminate an account without delay when calling activity presents a legal, fraud, network, reputational, or public-safety risk.

Available enforcement actions include:

- Warning the customer and requiring corrective action.
- Requiring additional customer or caller-ID verification.
- Restricting calling destinations or calling volume.
- Disabling outbound calling.
- Disabling affected extensions, devices, or credentials.
- Removing authorization to present a caller-ID number.
- Temporarily suspending the affected service.
- Permanently terminating the customer account.
- Referring relevant information to Telnyx, law enforcement, regulators, or other appropriate entities.

GC may decline to reactivate service until the customer provides adequate documentation, explains the questioned activity, corrects identified deficiencies, and demonstrates that future use will comply with applicable requirements.

GC may permanently refuse service when the customer has engaged in deliberate fraud, illegal calling, traffic laundering, unauthorized service resale, repeated violations, or attempts to circumvent GC controls.

8. Upstream and Industry Coordination

GC will promptly respond to Telnyx requests concerning suspected illegal, fraudulent, or abusive traffic.

GC will provide available customer, account, telephone-number, credential, and traffic information to Telnyx as permitted or required by law and applicable contractual obligations.

GC will cooperate with Telnyx and follow reasonable and lawful instructions necessary to:

- Investigate suspicious traffic.
- Identify affected customers, numbers, credentials, or devices.
- Restrict or block harmful traffic.
- Suspend affected services.
- Preserve relevant records.
- Stop confirmed illegal or abusive calling activity.
- Prevent recurrence of identified activity.

GC may immediately suspend affected credentials, extensions, telephone numbers, or customer accounts while an investigation is pending.

GC will also cooperate, as appropriate, with the Federal Communications Commission, law-enforcement authorities, the Commission-designated industry traceback consortium, and other voice service providers involved in investigating or stopping illegal traffic.

9. Record Retention, Filing Updates, and Plan Review

GC retains customer-verification records, telephone-number assignments, caller-ID authorizations, complaints, traceback requests, investigation notes, enforcement actions, relevant customer communications, carrier notices, and available call-detail evidence in its compliance records.

Records associated with an active complaint, traceback request, investigation, suspension, enforcement action, regulatory inquiry, or legal matter will not be routinely destroyed while the matter remains open or while preservation is reasonably necessary.

Access to retained records is limited to authorized persons with a legitimate business, technical, compliance, regulatory, or legal need.

This plan will be reviewed at least annually. GC's scheduled annual review begins July 1 of each year so that any necessary revisions may be completed before the August 1 anniversary of the plan's effective date.

This plan will also be reviewed when GC materially changes:

- Its upstream carrier relationship.
- Its STIR/SHAKEN or call-signing arrangements.
- Its role in the call path.
- Its customer-verification procedures.
- Its service offerings.
- Its calling controls.
- Its robocall-mitigation procedures.
- Its responsible company or operational contacts.

GC will update its Robocall Mitigation Database filing within 10 business days when information required in the filing changes.

GC will submit any required annual Robocall Mitigation Database recertification by the applicable FCC deadline.

Proposed FCC rules or guidance will not be treated as binding requirements unless and until they are adopted, become effective, and apply to GC. GC may revise this plan sooner when a final rule, order, or other binding requirement necessitates a change.

10. Approval

Approved by:

Printed Name:

Darla J CoKeley

Date:

July 28, 2026

Title/Capacity:

Owner

Authorized Signature:

dj coKeley