

ROBOCALL MITIGATION PROGRAM DESCRIPTION

ReNu Communication LLC

2709 Horsemint Trl, Garland, Texas 75042

Effective Date: July 31, 2026

This document describes the reasonable steps adopted by ReNu Communication LLC to prevent its services from being used to originate illegal robocalls or unlawful caller-ID spoofing, to investigate suspicious traffic, and to cooperate promptly with the Federal Communications Commission, law enforcement, the Industry Traceback Group, and upstream providers.

1. Company and Service Overview

ReNu Communication LLC is a United States-based provider of hosted PBX, interconnected VoIP, SIP-based telephone, and related communications services to business end users. Customers include hotels, motels, offices, clinics, and other small and medium-sized businesses. Services may be marketed under the ReNuTeck and PBXTOGO names.

ReNu Communication LLC operates and administers its hosted PBX environment and customer accounts. It obtains telephone numbers, public switched telephone network connectivity, call origination and termination, and related carrier functions through approved upstream telecommunications providers.

2. Current STIR/SHAKEN Status

As of the effective date of this program, ReNu Communication LLC has not implemented the STIR/SHAKEN authentication framework using a certificate issued to ReNu Communication LLC. The company relies on approved upstream providers for applicable carrier-network call-authentication functions.

ReNu Communication LLC will update its Robocall Mitigation Database filing and this program description when its STIR/SHAKEN implementation status materially changes. A future implementation may include direct signing or an authorized third-party signing arrangement using credentials assigned to ReNu Communication LLC, as permitted by applicable requirements.

3. Know-Your-Customer Procedures

Before activating service, ReNu Communication LLC uses risk-based procedures designed to understand the prospective customer's identity, business, authorized users, and intended use of the service. The level of review may be increased when the proposed use, expected call volume, payment method, business history, geographic location, or other circumstances present elevated risk.

- Obtain the customer's legal or commonly used business name, service address, billing information, and authorized contact information.
- Confirm that the customer is a legitimate business or organization through reasonably available records, its public website, direct communications, business documentation, or other reliable information.
- Understand the customer's intended use of hosted PBX, SIP trunking, telephone numbers, extensions, and outbound calling.
- Review requests for unusually high call capacity, rapid activation, multiple unrelated caller-ID numbers, or other indicators inconsistent with the stated business purpose.
- Maintain account records sufficient to identify the customer and the services, telephone numbers, PBX accounts, extensions, or SIP credentials assigned to it.
- Decline, delay, restrict, or terminate activation when identity, authority, intended use, or risk cannot be reasonably verified.

4. Caller-ID and Number Authorization Controls

ReNu Communication LLC requires outbound caller-ID information to be associated with the customer, assigned through an approved provider, or otherwise supported by evidence that the customer is authorized to use the number.

- Customer-provided caller-ID numbers may be reviewed before activation or continued use.
- ReNu Communication LLC may request a recent carrier invoice, account record, letter of authorization, porting documentation, or other evidence of control.
- The company may block or remove caller-ID values that are invalid, misleading, unassigned, unauthorized, or associated with complaints or suspicious traffic.
- Customers are prohibited from altering calling-name or caller-ID information for fraudulent, deceptive, or unlawful purposes.

5. Prohibited Uses and Customer Obligations

Customers may not use ReNu Communication LLC services to originate, transmit, or facilitate illegal robocalls, unlawful spoofing, fraud, impersonation, harassment, phishing, traffic pumping, or other deceptive or abusive calling practices.

- Customers must comply with applicable federal and state calling, consent, do-not-call, prerecorded-message, and caller-identification requirements.
- Customers may not resell or provide service to undisclosed third parties without written approval from ReNu Communication LLC.
- Customers must promptly provide information reasonably requested during an abuse, traceback, or regulatory investigation.
- ReNu Communication LLC may impose call limits, destination restrictions, credential changes, caller-ID restrictions, or other controls where reasonably necessary to reduce risk.

6. Traffic Monitoring and Risk Indicators

ReNu Communication LLC uses account information, call-detail records, customer reports, upstream-provider notices, and other reasonably available information to identify traffic that may warrant review. Monitoring may be automated, manual, event-driven, or a combination of these methods.

- Sudden or unexplained increases in outbound call volume or concurrent calls.
- Large numbers of short-duration, unanswered, repetitive, or sequentially dialed calls.
- Traffic patterns inconsistent with the customer's stated business and historical usage.
- Use of multiple or rapidly changing caller-ID numbers without a documented business reason.
- High complaint rates, spam-label reports, traceback requests, fraud alerts, or upstream-provider warnings.
- Repeated calls to high-risk destinations, unusual international destinations, or patterns suggesting artificial traffic generation.
- Compromised credentials, unauthorized account access, or calls originating from unexpected systems or locations.

7. Investigation, Mitigation, Suspension, and Termination

When suspicious or potentially unlawful traffic is identified, ReNu Communication LLC will take reasonable, proportionate, and prompt action based on the available facts and risk.

- Review customer identity, account history, assigned numbers, caller-ID settings, call-detail records, system logs, and relevant communications.
- Contact the customer and require an explanation, supporting records, proof of consent, proof of caller-ID authorization, or other information as appropriate.
- Change credentials; restrict destinations, call rates, concurrent calls, caller-ID values, extensions, PBX accounts, or SIP trunks; or temporarily suspend service while the matter is investigated.
- Permanently terminate service when the company determines that the customer engaged in illegal or abusive activity, materially misrepresented its use, failed to cooperate, or presents an unacceptable risk.
- Preserve relevant records and cooperate with upstream providers, the FCC, law enforcement, and the Industry Traceback Group.

8. Traceback and Government Cooperation

ReNu Communication LLC commits to respond fully and in a timely manner to traceback requests and related inquiries from the Federal Communications Commission, law enforcement, and the Industry Traceback Group. The company intends to provide an initial substantive response within 24 hours of receipt, or sooner when practicable.

- Identify the customer, account, telephone number, PBX, extension, SIP trunk, or credential associated with the traffic when reasonably available.
- Provide relevant routing, origination, call-detail, and account information that the company is legally permitted to disclose.
- Preserve relevant records and take immediate protective action when continued traffic may cause harm.
- Maintain a robocall mitigation contact whose current information is provided in the company's Robocall Mitigation Database filing.

9. Upstream Provider Due Diligence

ReNu Communication LLC currently uses Telnyx as an upstream telecommunications provider for certain PSTN, numbering, origination, termination, and related carrier services. Before activating any additional upstream provider, ReNu Communication LLC performs reasonable due diligence appropriate to the relationship.

- Verify the provider's legal identity, business contact information, and services to be supplied.
- Confirm the provider's current Robocall Mitigation Database status when applicable.
- Review how the provider handles STIR/SHAKEN authentication, traceback requests, illegal traffic, fraud, complaints, and account security.
- Maintain records of provider accounts, contacts, services, and relevant activation or termination dates.
- Avoid or discontinue relationships when a provider cannot be reasonably verified or presents an unacceptable compliance risk.

ReNu Communication LLC may use VoIP.ms or other approved upstream providers in the future. A prospective provider is not treated as active until due diligence is completed and service is actually placed into use.

10. Recordkeeping

ReNu Communication LLC maintains records reasonably necessary to administer customer accounts, investigate suspicious traffic, respond to traceback requests, and demonstrate implementation of this program. Records may include customer identity and contact information, service orders, assigned numbers, caller-ID authorizations, account and credential records, call-detail records, system logs, complaints, provider notices, investigation notes, and enforcement actions.

Records are retained for periods appropriate to operational, contractual, legal, security, and regulatory needs, subject to technical availability and applicable privacy requirements.

11. Training, Responsibility, and Program Review

Company personnel responsible for provisioning, customer support, network administration, billing, and compliance are expected to escalate suspected illegal robocalling, spoofing, fraud, account compromise, or other abusive activity to management and the designated robocall mitigation contact.

ReNu Communication LLC will review this program periodically and after significant changes in its services, upstream providers, network architecture, STIR/SHAKEN implementation, applicable rules, or identified risk. The company will update its RMD filing when required.

12. Program Administration

Legal entity: ReNu Communication LLC

Business address: 2709 Horsemint Trl, Garland, Texas 75042

Robocall mitigation contact: Fenil Mistry, Authorized Representative

Contact telephone and email: As listed in ReNu Communication LLC's current Robocall Mitigation Database filing.

Principal and certifying officer: Nikhil Mistry, Managing Member, or another duly authorized officer.

Adopted by:	ReNu Communication LLC
Authorized Officer:	Nikhil Mistry
Title:	Managing Member
Effective Date:	July 31, 2026

This program is intended to describe ReNu Communication LLC's actual operational controls. The company must implement and follow the procedures stated above and update the document when its practices change.