
Know Your Customer (KYC) and Robocall Mitigation Plan

VoIP Cloud Services – SIP Trunking and Managed PBX

Company Information

Provider: GRNLK Corp dba GreenLink Networks
Filing Entity: VOIP Provider
FCC Registration: 0025402306
RMD File Number: 0006638

Email: mayronh@greenlinknetworks.com

Purpose

GreenLink Networks has implemented this Know Your Customer (KYC) and Robocall Mitigation Plan to establish reasonable, risk-based procedures to prevent, detect, and mitigate illegal, unwanted, or fraudulent robocall traffic originating from or transiting its VoIP network, in compliance with FCC rules and Robocall Mitigation Database (RMD) requirements * under 47 CFR § 64.6305.

Customer Identification – New Customers

Prior to activating SIP Trunk or managed cloud phone services, GreenLink Networks collects and reviews customer information appropriate to the customer's risk profile, which may include:

- Legal business name or individual name
- Physical service address and country of operation
- Valid contact information
- Government-issued identification or business registration documentation, as applicable
- Description of intended use of VoIP services
- Expected call volumes, destinations, and traffic characteristics

Customers with elevated risk indicators (such as high-volume outbound calling or campaign-based traffic) may be subject to additional review prior to service activation.

Application of KYC to Existing Customers

GreenLink Networks applies its KYC procedures to **existing customers on an ongoing basis** through:

- Continuous monitoring of originating and terminating traffic
- Review of abnormal call volumes, call rates, or destination patterns
- Investigation triggered by consumer complaints, traceback requests, upstream carrier notifications, or internal alerts
- Re-verification of customer information when risk indicators are identified

Existing customers are subject to the same enforcement and mitigation measures as new customers.

Traffic Monitoring and Analytics

GreenLink Networks monitors VoIP traffic using internal systems and operational controls, including:

- Call Detail Record (CDR) analysis
- Call volume, rate, and destination threshold monitoring
- Detection of anomalous traffic behavior
- Manual review of flagged traffic by technical staff

Third-Party Analytics:

GreenLink Networks does not currently utilize a third-party analytics vendor for robocall detection and performs traffic monitoring internally.

Number Authentication and Origination Controls

GreenLink Networks enforces strict origination controls within its multi-tenant PBX environment, including:

- Calls may only originate using telephone numbers that are **registered and assigned within the Company's system**
- Call origination from unregistered, spoofed, or unauthorized numbers is not permitted
- SIP authentication and tenant-level controls are enforced for all originating traffic

These controls significantly reduce the risk of caller ID spoofing and unauthorized call origination.

Interconnection with Upstream Carriers and STIR/SHAKEN

GreenLink Networks interconnects with upstream voice service providers for call origination and termination.

GreenLink Networks primary upstream carrier is **Bandwidth**, which performs STIR/SHAKEN signing and applies appropriate attestation levels for calls originating from the Company's network.

- GreenLink Networks provides Bandwidth with accurate customer and number assignment information necessary for proper attestation
- STIR/SHAKEN certificates are managed and applied by the upstream carrier
- Calls that cannot be properly authenticated or that present elevated risk indicators are subject to increased scrutiny and mitigation

GreenLink Networks monitors traffic behavior and cooperates with upstream carrier notifications related to suspected illegal or unwanted traffic.

Reasonable Steps to Mitigate Illegal or Unwanted Traffic

When potentially illegal or unwanted robocall traffic is identified, GreenLink Networks may take reasonable and proportionate mitigation steps, including:

- Contacting the customer to request clarification or corrective action
- Blocking or rate-limiting specific traffic sources, destinations, numbers, or tenants
- Temporarily suspending service pending investigation
- Permanently terminating service for repeat or severe violations
- Cooperating with industry traceback groups, upstream carriers, and law enforcement inquiries

Mitigation actions are based on the severity, scale, and persistence of the identified traffic.

Record keeping

GreenLink Networks maintains records related to customer onboarding, traffic monitoring, investigations, mitigation actions, and upstream carrier communications for a reasonable period to demonstrate compliance with FCC robocall mitigation requirements.

Ongoing Review

The KYC and Robocall Mitigation Plan is reviewed periodically and updated as necessary to reflect changes in FCC rules, upstream carrier requirements, industry best practices, and the Company's operational environment.

We hereby certify that GreenLink has implemented the above robocall mitigation measures and will continue to enforce them to prevent illegal robocall traffic.