



Clarity Technologies Group, LLC

ROBOCALL MITIGATION PROGRAM

Revised: 08-28-2025

Below is the Robocall Mitigation Plan filing for **Clarity Technologies Group, LLC**

This plan is being submitted to the FCC's Robocall Mitigation Database and adapted to the latest laws, regulations, and industry best practices.

Company

Business Information

- **Legal name:** Clarity Technologies Group, LLC
- **Business name (DBA):** ClarityVoip™
- **Address:** 1347 US Highway 46, Ledgewood, NJ 07852

Contact Information for Robocall Mitigation-related Issues

- **Full Name:** Bruce G. Kreeger
- **Title:** Chief Executive Officer
- **Department:** Management
- **Business Address:** 1347 US Highway 46, Ledgewood, NJ 07852
- **Telephone Number:** 973-440-5811
- **Email Address:** bkreeger@clarityscg.com / accounting@clarityscg.com - for any law enforcement requests.

Monitoring

Clarity Technologies Group, LLC has monitoring and reporting systems to analyze high-volume voice network traffic to identify and monitor patterns consistent with robocalls. Our monitoring systems provide alerts on calling patterns with unusual spikes, traffic patterns, or attempted use of non-validated Telephone Numbers (TN) to detect patterns consistent with illegal robocalls.

Suppose Clarity Technologies Group, LLC detects a pattern consistent with illegal robocalls or has reason to suspect illegal robocalling or spoofing is taking place over our network. In that case, we will seek to identify the party using our network to originate, route, or terminate these calls and take appropriate action.



Appropriate action may include:

- Validating that the originating party is authorized to use the TN.
- Suspending the calling party's ability to originate, route, or terminate calls on the **Clarity Technologies Group, LLC** network.

Traceback Cooperation

Clarity Technologies Group, LLC commits to responding promptly and supporting all traceback requests from the FCC, law enforcement, and the [Industry Traceback Group \(ITG\)](#).

Bulk Solutions Robocall Mitigation Solution Overview

- General information
 - o Robocall scoring is based on the annual +100B carrier calls that Bulk Solutions processes as part of the Caller Name service.
 - o STIR/SHAKEN Transaction Detail Records (TDRs) are now being added as an additional data source.
 - o Each call is assessed through the Bulk Solutions model, leading to a constantly refreshed view of call behavior and the probability of a given number currently being used for robocalling.
 - o Active numbers are assessed by the model for behavioral attributes typically associated with robocalling, including:
 - Neighbor spoofing events
 - Sudden spikes in volume, such as those driven by call spoofing
 - o Do-Not-Originate (DNO) numbers are also considered robocalls if they are the calling party number. This is sourced from industry (e.g., US Telecom) and directly from enterprises.
 - o The service covers both US domestic and international TNs.
- Calls originating from your network (i.e., Robocall Protection)



- o Provides detailed reporting identifying suspected illegal robocalls and alerts if calls originate where the call number is invalid or unallocated on a Do-Not-Originate list.
 - o If the platform detects suspected robocalling patterns, Clarity Technologies Group, LLC will take appropriate action, including suspending or terminating the subscriber.
 - o It supports a real-time query to the service to determine if a number originating on your network could be a robocall. Such calls can be blocked, or the terminating party can be notified via CNAM.
 - o For each new instance of robocalling using the Operating Service Provider (OSP)TNs, an alert is sent to the OSP in near real-time. This alert will result in the OSP (manually) blocking the TN and all TSPs being alerted via CNAM through an overlay such as “ROBOCALLER”. The CNAM alerting helps address instances of spoofing of TNs not going through the OSP that owns the number.
- Termination (i.e., Robocall Mitigation)
 - o Supports a real-time query to the service to determine if a number terminating on your network could be a robocall. This protects subscribers from calls that come from networks that cannot authoritatively attest to the end user caller (i.e., all Communications Service Providers (CSPs)that do not have STIR/SHAKEN and all CSPs *with* STIR/SHAKEN but who do not have a direct and vetted end-user relationship).
 - o Such calls can be blocked, or the called party can be notified via CNAM.

Modus operandi in case of illegal traffic

A real-time block system is in place as soon as abnormal activities are detected (including but not limited to abnormal spikes of calls, abnormal trends, low call completion statistics, systematic calling, unusual amounts of calls, etc.). The ClarityVoip™ system blocks suspicious traffic and automatically reaches out to



customers to understand the highlighted behaviour. A dedicated team is always on the trigger to follow up with the customer. ClarityVoip™ has a zero-tolerance policy regarding potential fraud, scam, and robocall activities. ClarityVoip™ also reviews outbound call logs and analytics regularly to monitor for possible abuse. Finally, ClarityVoip™ also works with its upstream providers to identify behaviors that indicate illegal call activity.

Commitment

To the extent that ClarityVoip™ receives information from law enforcement, traceback entities, or other sources that a customer is engaged in illegal robocalling, our policy is to cooperate fully, including providing the identity of any suspected illegal robocaller, pursuant to legal service or process. Our internal policy is to reply to those requests within 24 hours.

ClarityVoip™ also follows the Industry Traceback Group recommended best industry practices and cooperates in traceback and trace-forward investigations.

As a matter of fact, ClarityVoip™ offers a single point of contact for any law enforcement requests: lawenforcement@clarityscg.com. Law enforcement agencies can provide the following information, and the request will be treated on a highly accelerated basis:

- Full name, Authorized Agency / Department,
- Phone Number,
- Nature of Request (Subscriber info, Call detail records, Billing info, etc.),
- Target Telephone Number(s),
- Request Start Date and End Date,
- Copy of the Subpoena, Court Order, Search Warrant, or Other Formal Legal Process, and
- Additional Notes (incl. specific circumstances and/or deadlines).

If there are multiple requests, please submit only one legal process per email to ensure proper treatment.

While ClarityVoip™ already had everything in place to fight illegitimate traffic (including but not limited to robocalls), it also fully commits to ensuring and enhancing compliance with this program. ClarityVoip™ also fully complies with STIR-SHAKEN. If any material change to this plan, ClarityVoip™ will republish it to employees, consultants, and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.