

Geo Teleco LLC RMP

This Robocall Mitigation Plan (“Plan”) is submitted by **Geo Teleco LLC** (“Provider”), pursuant to the provisions of **47 C.F.R. § 64.6305**, adopted by the Federal Communications Commission (“FCC”), which require all “voice service providers” to establish and implement a robocall mitigation plan.

This Plan sets forth the Provider’s current policies and procedures designed to reduce or eliminate the origination of illegal outbound robocalls on its network. The Provider views these policies and procedures as constituting “reasonable steps” to avoid the origination of illegal robocalls. In addition, the Provider commits to responding to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (“ITG”), and to fully cooperate with such entities in investigating and stopping any illegal robocallers that may use its service to originate calls.

I. STIR/SHAKEN IMPLEMENTATION STATUS

As reflected in the FCC’s Robocall Mitigation Database, **Geo Teleco LLC has fully implemented the STIR/SHAKEN caller ID authentication framework** in accordance with FCC rules.

- The Provider **authenticates and signs all outbound SIP traffic** originating on its network using the STIR/SHAKEN framework.
- Appropriate attestation levels (A, B, or C) are assigned based on the Provider’s relationship with the originating customer and verification of the customer’s right to use the calling telephone number.
- Geo Teleco LLC maintains internal policies, technical controls, and monitoring processes to ensure accurate attestation, prevent caller ID spoofing, and support traceback and enforcement efforts.

For any traffic that may traverse non-IP or interworking segments outside of the Provider’s direct control, Geo Teleco LLC applies the robocall mitigation measures described in this Plan to ensure continued compliance and prevent the origination of illegal robocalls.

Any calls that cannot be authenticated using STIR/SHAKEN will be blocked

II. TRACEBACK REQUESTS

The Provider will cooperate with the FCC, law enforcement agencies, and the ITG on all traceback requests and investigations.

To ensure timely and effective enforcement efforts against illegal robocallers, the Provider:

- Commits to **fully responding to all traceback requests within twenty-four (24) hours** of receipt
- Dedicates sufficient internal resources to promptly investigate and respond to all traceback inquiries
- Maintains a **single point of contact** for traceback requests, identified in **Appendix A**

The Provider will also include, where applicable, traceback cooperation requirements within its carrier interconnection and service agreements. These provisions require parties to promptly identify the upstream provider or originating customer responsible for suspected illegal robocall traffic.

III. CUSTOMER VETTING PRACTICES

The Provider employs best practices to vet the identity of all voice service subscribers, including residential, business, and reseller customers, to prevent the origination of illegal robocalls.

Customer vetting measures include, as applicable:

- Verification of customer identity and contact information
- Collection of physical address and billing details
- Confirmation of business purpose and nature of operations
- Review of incorporation or registration information (where applicable)
- Evaluation of requested service capacity relative to stated use case

Commercial and high-volume customers may be subject to enhanced vetting procedures, which may include additional background review and/or site validation.

Additionally, the Provider:

- Uses service agreements and Acceptable Use Policies prohibiting illegal robocalls and fraudulent activity
- Reserves the right to suspend or terminate service for violations of applicable laws or service terms
- Reviews call detail records (CDRs) on a recurring basis to identify suspicious traffic patterns
- Contacts customers within **24 hours** if activity indicative of illegal robocalling is detected

IV. TELEPHONE NUMBER VALIDATION PRACTICES

The Provider maintains procedures to validate a customer's right to use telephone numbers presented as caller ID.

- Subscribers may only use telephone numbers assigned by the Provider or obtained through authorized upstream partners
- Switching and screening systems restrict originating calls to numbers assigned to the subscriber
- Multi-line and PBX customers are screened to ensure originating numbers match assigned inventories

These controls provide automated and secure validation of originating telephone numbers.

V. INTERNATIONAL CALL ORIGINATORS

The Provider is **not currently an international voice service provider**.

If the Provider begins offering services to international call originators using North American Numbering Plan resources, it will implement enhanced vetting, monitoring, and number validation practices consistent with FCC requirements and industry best practices.

VI. KNOW YOUR UPSTREAM PROVIDER PROCEDURES

The Provider maintains relationships with a limited number of upstream providers and monitors their compliance posture and operational legitimacy.

The Provider is committed to ensuring that all upstream providers:

- Actively monitor their networks for illegal robocall traffic
- Cooperate with traceback investigations
- Include robocall mitigation and compliance language in applicable agreements

A list of the Provider's immediate upstream providers is included in **Appendix A**.

VII. ONGOING ROBOCALL MITIGATION PRACTICES

The Provider continuously monitors network usage and reviews CDRs to identify potential illegal robocalling activity.

Indicators reviewed include, but are not limited to:

1. Abnormally high call volumes or traffic spikes
2. Short call durations and low completion rates
3. Sequential or predictive dialing patterns
4. Calls to invalid or Do-Not-Call numbers
5. Calls to unassigned or invalid NPA-NXXs

When suspicious activity is detected, the Provider may take actions including:

- Initiating traceback investigations
- Verifying caller ID ownership and authorization
- Suspending or terminating service
- Notifying law enforcement or regulatory authorities

VIII. THIRD-PARTY ANALYTICS

The Provider utilizes third-party call analytics solutions to enhance detection and prevention of illegal robocalls.

Details regarding the analytics vendor(s) and systems used are provided in **Appendix A**.

Appendix A | Traceback Request Single Point of Contact

Name: *AJ*

Title: *CEO*

Phone: *727-755-6620*

Email: *aj@geoteleco.com*

Call Analytics Vendor

Vendor Name: *Veriswitch*

Description:

Geo Teleco LLC utilizes third-party analytics platforms to monitor call patterns, analyze CDRs, detect anomalous traffic, and prevent illegal robocalls. These tools may include real-time SIP analytics, reputation databases, Do-Not-Originate screening, blacklisting/whitelisting, and automated mitigation controls.