



GeoNet Telecom Limited

Robocall Mitigation Plan

Updated – July 9, 2025



The following is GeoNet Telecom Limited (“GEONET”) submission to the Robocall Mitigation Database, pursuant to the FCC’s directives outlined in the Report and Order(s) DA 24-73 (<https://docs.fcc.gov/public/attachments/DA-24-73A1.pdf>) (RMD Public Notice)

Indicated below are the robocall mitigation measures employed by GEONET switching platform. GEONET implements the features on their network and traffic. GEONET certifies that its switching platform follows required traceback standards. GEONET will continue to implement new robocall mitigation measures as they become available.

24 Hour Response

GEONET certifies that it will respond to all Traceback Requests from the Industry Traceback group (ITG) within 24 hours and civil and criminal law enforcement agencies, cooperating fully in efforts to investigate and eliminate illegal robocalls, while following CPNI requirements.

Partial STIR/SHAKEN implementation

GEONET has Partially implemented STIR/SHAKEN attestation. GEONET has an address of 12 London Road, Morden, Surrey, SM4 5BQ, United Kingdom. All compliance or questions with the RMD and/or STIR/SHAKEN should be reported to compliance@geonettelecom.com.

GEONET RMD Verification

GEONET policies require refusing traffic from any provider not registered in the Robocall Mitigation Database (RMD).

GEONET KYC Verification

GEONET performs Customer Due Diligence and KYC, mandating that all potential customers complete a Know Your Customer (KYC) form and undergo a due diligence process.

GEONET DNO Compliance

GEONET is utilizing Do Not Originate (“DNO”) lists, primarily leveraging the ITG list via Peeredge, as well as adding additional numbers reported outside the ITG list manually.

GEONET Mitigation Certification

GEONET certifies that all calls originating on our network are subjected to a robocall mitigation program that meets the specified requirements. We affirm that we are not barred from participation in the Robocall Mitigation Database, nor has GEONET been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description. GEONET has Partially implemented STIR/SHAKEN across our network, and is in process of completing Stir/Shaken certification for full compliance.



Analytics

GEONET relies in part on third-party analytics. GEONET relies upon ITG Communications for Do Not Originate lists via Peeredge, and GEONET relies upon Peeredge Telecom for spam filter services to block and label calls as SPAM.

The following plan shall outline specific “commercially reasonable efforts/steps” GEONET has undertaken to prevent origination and transmission illegal robocall traffic.

Regulatory Compliance

GEONET is not currently, nor has it ever been, subject to any Commission, law enforcement, or regulatory agency action or investigation related to suspected unlawful robocalling or spoofing activities.

Traceback CPNI

For handling sensitive customer information (CPNI), GEONET adheres to strict protocols, ensuring that such information is exclusively shared through the official ITG portal. It is important to note that CPNI is only disclosed within the secure transmission such as ITG portal.

To facilitate the traceback process, the official channels through which Traceback Requests can be initiated:

Email: Requests can be directed to compliance@geonettelecom.com Upon receipt, GEONET personnel will verify the request before proceeding.

Direct Contact: Kwesi Victor Adade (CEO), is the designated contact in the Robocall Mitigation Database, reachable at (44) 7961386350 or via email at victor.adade@geonettelecom.com.

NOC: Available around the clock, our support center can be reached at support@geonettelecom.com. Upon receipt a ticket is assigned, and tracked to completion.

Methods and Efforts Employed to Avoid Carrying or Processing Illegal Robocalls

- Do Not Originate “DNO” queries (ITG Database) are utilized to confirm compliance with proper DNO requirements.
- Know Your Customer “KYC” measures have been implemented, and are reviewed yearly for customers, to ensure compliance.
- ANIs and DNISs are tracked and documented from customer through vendor delivery, including all voice “hops” and stored for 90-days.
- Originating and termination numbers are profiled by traffic analytics engine for irregular behavior including, but not limited to:
 - High Volume / Short Duration Traffic
 - Calls to Unallocated Numbers
 - Calls with excessive cancels
 - Calls from numbers that exist on a known robodialer list.
- Automated filtering for both inbound and outbound traffic to our voice network.
- GEONET commits to respond within the 24 hour requirement to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.
- GEONET shall take action when notified by the FCC of potentially illegal calls utilizing its network and will promptly inform the Commission that it is not the originating or gateway provider for the identified traffic, specify which upstream VSP with direct access to the U.S. public switched telephone network it received the traffic from, and, if possible, take lawful steps to mitigate this traffic.
- We conduct a review of our measures in an effort to combat new techniques that scammers use to compromise the PSTN in the US.
- GEONET maintains an Acceptable Use Policy (AUP) that subscribers may sign before being permitted to use GEONET’s network. GEONET’s contractual terms with subscribers specify that GEONET may take action up to suspension or termination of service for violation of the AUP. Among other things, the AUP prohibits:
 - providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call;
 - violating any applicable law;
 - violating applicable industry accepted guidelines; and
 - using GEONET’s service to engage in or in connection with fraudulent activities.
- GEONET works with its upstream carriers to detect a calling pattern consistent with illegal robocalls. If such a call is detected, GEONET will identify the party that is using our network to originate those calls and will take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating subscriber owns or is authorized to use the Caller ID number, and suspending or terminating the party’s ability to originate calls on our network.

- When traffic analysis indicates the presence of likely illegal robocalling, GEONET may follow certain procedures on investigating such subscribers.
The procedures established may include but are not limited to:
 - checking recent and past call detail records and benchmark against expected trends;
 - checking recent and past account activity and purchases;
 - investigating if any system issue generates the strange behavior;
 - verifying that the call originating path is valid; and
 - contacting the subscriber to understand his or her particular use case and validate that the activity belongs to that subscriber.
- New customers requesting an excessive number of calls per second “CPS” will be screened for legitimate call usage needs.
- New and existing customers with an excessive number of call paths may receive Robocall outreach.
- GEONET utilizes KYC measures to eliminate illegal robocalling customers from terminating to GEONET’s network.

Traceback Requests.

GEONET certifies that its software follows required traceback standards. GEONET commits to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, regulators, and the industry traceback consortium.

Kwesi Victor Adade
CEO



Updated 7/9/2025