

GTT Robocall Mitigation Program Overview

Updated: July 2025



Table of Contents

1.	Introduction	3
2.	STIR/SHAKEN Status	3
3.	Robocall Mitigation Program.....	4
3.1	Prevention	4
3.2	Detection & Alerting.....	5
3.3	Mitigation	5
4.	Traceback Commitment.....	5

1. Introduction

GTT Communications, Inc. (together with its relevant subsidiaries, “we”) provide voice services to businesses and other voice service providers; we do not provide any voice services to any residential customers. The vast majority of voice communications services that we operate use Voice over IP (VoIP); a small portion is provided via resold TDM facilities. We do not offer voice services via mobile/cellular technology.

We have implemented a Robocall Mitigation Program (“RMP”) for the voice services that we operate; the details of our RMP, the status of our implementation of applicable STIR/SHAKEN requirements and our commitment to responding to Traceback requests are described herein.

The RMP supplements our implementation of STIR/SHAKEN across our voice network in the US.

2. STIR/SHAKEN Status

Where we are a voice service provider utilizing IP networks (i.e., we provide interconnected VoIP services):

- We do not have North American Numbering Plan numbering resources directly allocated to us but obtain numbers via our underlying carriers.
- We are an STI-GA authorized Service Provider registered with the Secure Telephone Identify Policy Administrator (STI-PA) and participate in the Signature-based Handling of Asserted Information Using toKENs (SHAKEN) ecosystem. We authenticate customers following the Robocall Mitigation strategies described herein and based on that authentication, attach the appropriate attestation level to its customers’ outgoing calls.
- Calls originated on our network are compliant with §64.6301(a)(1) and (2), and all calls that originate on our network are subject to our RMP.

3. Robocall Mitigation Program

The reasonable steps that we have taken to avoid originating illegal robocall traffic as part of our RMP are:

3.1 Prevention

- Know Your Customer:
 - We provide services exclusively to non-residential customers. Customers are required to provide identifying information, which typically includes company name, address, website URL, company contact information, President/CEO contact information, Tax ID and/or D&B number, year company was established, and the signature of a company officer on the customer service agreement. We also perform credit checks when applicable.
- We periodically train our sales teams to:
 - Not sell voice services that will be, or are suspected to be, high call volume along with low call revenue, or if it is known that an automated dialing system is in use or planned to be used.
 - Seek in-house support from subject matter experts if the customer or prospective customer inquires about how we handle short duration calls, a high percentage of failed calls, and/or limits of call attempts per second (CAPS).
- We state in our voice service terms and conditions that the customer agrees that:
 - They are not permitted to originate any calls using auto-dialer or other automated call generators and we have the right to suspend our customer's service if we detect such calls originating from the customer.
 - They must present a valid Automatic Number Identification (ANI) when they originate calls.
- We require all end users who request to port numbers to our service to verify their right to use their existing number(s) by providing documentation, such as an invoice from their current service provider. We also require a signed Letter of Agency that identifies the phone numbers to be ported, in compliance with FCC rules.
- We do not currently sell services to international call originators without offices in the FCC regions using North American Numbering Plan Numbers. To the extent we have sold such services in the past, we have applied the processes described above to validate the customer's right to use the telephone number and caller identity.

3.2 Detection & Alerting

Our RMP was developed by us, sources data from Call Detail Records (CDRs), and is automated.

Metadata is extracted from a continuous feed of CDRs and is placed in a database. This data is then periodically queried. The results of queries are used along with logic to determine whether any calling patterns are likely to be robocalls. Performance indicators such as Average Length of Call (ALOC) and Answer Seizure Ratio (ASR) are some of the values used in the determination logic.

Where a calling pattern is likely be robocalls then a “Robocall Alert” is automatically generated and sent to our 24x7 Network Operating Centers (“NOC”) for investigation.

3.3 Mitigation

On receipt of a “Robocall Alert”, the NOC assigns an available voice technician to review. If the voice technician determines that the alert is highly likely to be robocalls, the voice technician follows a documented process to mitigate it and attempts to contact the customer to inform them that they are suspected of originating robocalls.

Various mitigations include, but are not limited to, call blocking based on calling party number(s), source IP address, source trunk group and customer.

The Company blocks inbound calling routed to its voice network from companies not registered in the Robocall Mitigation Database. It relies on its underlying providers to perform this function with respect to resold TDM services, over which GTT has no control.

4. Traceback Commitment

We are committed to responding within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium (currently the ITG), and to cooperate with such entities in investigating and stopping any illegal robocallers that use our service to originate calls. GTT has devoted sufficient resources to provide prompt and complete information to traceback requests. Our points of contact for traceback requests are:

Name	Title	Contact Information
GTT Legal Department		regulation@gtt.net
GTT Voice Engineering Department		voip@gtt.net
GTT Network Operations Center		NOC@gtt.net

The Company investigates traceback requests by analyzing its call detail records. If suspicious calling activity is found, the Company will notify the customer and the customer’s service will be suspended or terminated for violation of the Company’s terms and conditions.