

	ROBOCALL MITIGATION POLICY				
	Issued on	Revised	Version	Document ID	Confidentiality
	7/7/2024	12/10/2024	2.0	GTS-IDSMP-002	PUBLIC

This document and all its contents have been approved to be shared publicly among the business stakeholders.

PUBLIC

ROBOCALL MITIGATION POLICY

	ROBOCALL MITIGATION POLICY				
	Issued on	Revised	Version	Document ID	Confidentiality
	7/7/2024	12/10/2024	2.0	GTS-IDSMP-002	PUBLIC

Properties

Properties	Value
Customer name	Internal
Contract	Internal
Document title	CALL IDENTIFICATION AND ROBOCALL MITIGATION POLICY
Version	2.0
Filename	GTS-IDSMP-002
Status	For immediate release

Table of Contents

COMPANY STATEMENT 3

1. OBJECTIVE 3

2. SCOPE 4

3. GLOSSARY 4

4. GTS INTERNAL STAKEHOLDERS 5

5. ROBOCALL PREVENTION POLICY 5

6. TECHNICAL DESIGN 6

7. KYC 7

8. TRACEBACK 8

9. GTS ROBOCALL MITIGATION AND STIR/SHAKEN ESCALATION LIST 9

	ROBOCALL MITIGATION POLICY				
	Issued on	Revised	Version	Document ID	Confidentiality
	7/7/2024	12/10/2024	2.0	GTS-IDSMP-002	PUBLIC

COMPANY STATEMENT

GLOBAL TELECOM SOLUTIONS is a Unified Communications as a Service Provider. GLOBAL TELECOM SOLUTIONS only accepts originating calls from customers that have completed our KYC (“Know your customers company authentication process”) to guarantee that traffic corresponds strictly to enterprise regular traffic and not to telemarketing campaigns, alerting, solicitation of services or any other unsolicited voice traffic.

GTS HEREBY CERTIFIES THAT ALL CALLS ORIGINATED ON ITS NETWORK ARE SUBJECT TO A COMPREHENSIVE ROBOCALL MITIGATION PROGRAM. THIS PROGRAM ADHERES TO ALL APPLICABLE REGULATORY REQUIREMENTS AND INCORPORATES ROBUST MEASURES TO DETECT, MITIGATE, AND PREVENT ILLEGAL OR UNAUTHORIZED CALL ACTIVITY.

FURTHERMORE, GTS CONFIRMS THAT NO PRIOR CERTIFICATION HAS BEEN REMOVED BY FCC ACTION, NOR HAS GTS BEEN PROHIBITED FROM FILING IN THE ROBOCALL MITIGATION DATABASE (RMD).

1. OBJECTIVE

The objective of this policy is to establish a comprehensive framework for ensuring the integrity, reliability, and security of telecommunications by implementing robust measures to authenticate caller identities, mitigate spam and fraudulent calls, and comply with industry standards and regulatory requirements.

This policy aims to:

1. **Protect End-Users:** Safeguard customers and stakeholders from the risks of fraudulent, unsolicited, and malicious calls.
2. **Enhance Trust:** Promote trust in telecommunication services by ensuring the authenticity of caller identities and reducing the prevalence of spam and spoofed calls.
3. **Regulatory Compliance:** Adhere to national and international standards, including FCC regulations to prevent illegal robocalls.
4. **Operational Excellence:** Support providers, intermediaries, and users with clear guidelines and procedures for traceback capabilities and anti-spam enforcement.

This policy serves as a cornerstone for maintaining a secure and trusted communication environment, balancing technological innovation with privacy and security best practices.

	ROBOCALL MITIGATION POLICY				
	Issued on	Revised	Version	Document ID	Confidentiality
	7/7/2024	12/10/2024	2.0	GTS-IDSMP-002	PUBLIC

2. SCOPE

This policy applies to all stakeholders involved in the origination and termination of calls within **GTS's** network. It encompasses the following:

1. Voice Service Providers
2. Enterprise Customers
3. Regulatory and Compliance Authorities
4. Internal Teams Responsible for Call Management and Compliance

3. GLOSSARY

- **Authentication:** The process of verifying the identity of the caller to ensure the validity of the call's source.
- **Caller ID:** Information transmitted with a call that displays the caller's identity.
- **Call Blocking:** A mechanism to prevent calls from reaching the recipient based on specific criteria.
- **Call Origination:** The initiation of a call by a provider or end-user.
- **Call Termination:** The completion of a call when it reaches its intended recipient.
- **Fraudulent Call:** A call made with malicious intent, such as phishing or spoofing.
- **Spoofing:** Falsifying caller ID information to mislead the recipient about the origin of the call.
- **Traceback:** The process of identifying the source of a call through its path in the call chain.
- **Voice Service Provider (VSP):** An entity that facilitates the origination, transmission, and termination of calls.
- **Gateway Provider:** A provider that routes calls between networks or systems.
- **Spam Call:** An unsolicited call, often for advertising or fraudulent purposes.
- **Illegal Call:** Any call that violates legal or regulatory standards.
- **Call Analytics:** Tools or systems used to analyze call data.
- **Robocall Mitigation:** Measures to prevent or reduce automated calls.
- **Regulatory Compliance:** Adherence to laws and standards governing telecommunication practices.
- **Fraud Prevention:** Strategies and systems implemented to detect and deter fraudulent activity.
- **Call Verification:** The process of confirming the authenticity of call details, such as caller ID.
- **Network Monitoring:** Continuous observation of network activity to detect anomalies in call behavior.

Other documents for reference:

- Sixth Caller ID Authentication Order (2023)
- Seventh Call Blocking Order (2023)
- Second Caller ID Authentication Order (2020)
- 47 CFR § 64.6305
- RMD Public Notice (2024)
- FCC Robocall Mitigation Database Filing Deadlines and Instructions
- FCC Declaratory Rulings and Orders on STIR/SHAKEN

	ROBOCALL MITIGATION POLICY				
	Issued on	Revised	Version	Document ID	Confidentiality
	7/7/2024	12/10/2024	2.0	GTS-IDSMP-002	PUBLIC

4. GTS INTERNAL STAKEHOLDERS

POSITION	RESPONSIBILITY
CEO	Approve the policy, oversee compliance and apply sanctions.
VOICE ENGINEERING	Configure and implement required mechanisms and protocols in the voice network.
TECHNICAL SUPPORT	Attend and process new provisioning orders as well as traceback requests.

5. ROBOCALL PREVENTION POLICY

GTS ensures the prevention of robocalls at origination by implementing measures as follows:

1. Blocking calls from invalid, high-risk and *Do-Not-Originate* numbers using trusted third-party information sources.
2. Monitoring real-time traffic to detect suspicious calling patterns from our enterprise customers.

Detection Mechanisms

The following detection methods are in place to mitigate robocalls at origination:

- **Blacklist Filtering:** Calls are screened against predefined blacklists, including Invalid or unauthorized calling numbers and specific IP geographical regions flagged for suspicious activity.
- **Traffic Analysis:** Real-time SIP Analytics monitors to detect threshold breaches.
- **Reputation Lookup:** Phone numbers are evaluated for reputation scores, flagging numbers with poor reputations for further investigation.
- **Call Detail Record (CDR) Analysis:** Patterns such as high call volumes, short durations, and frequent hang-ups are analyzed to identify anomalies indicative of robocalls.

Response Protocols

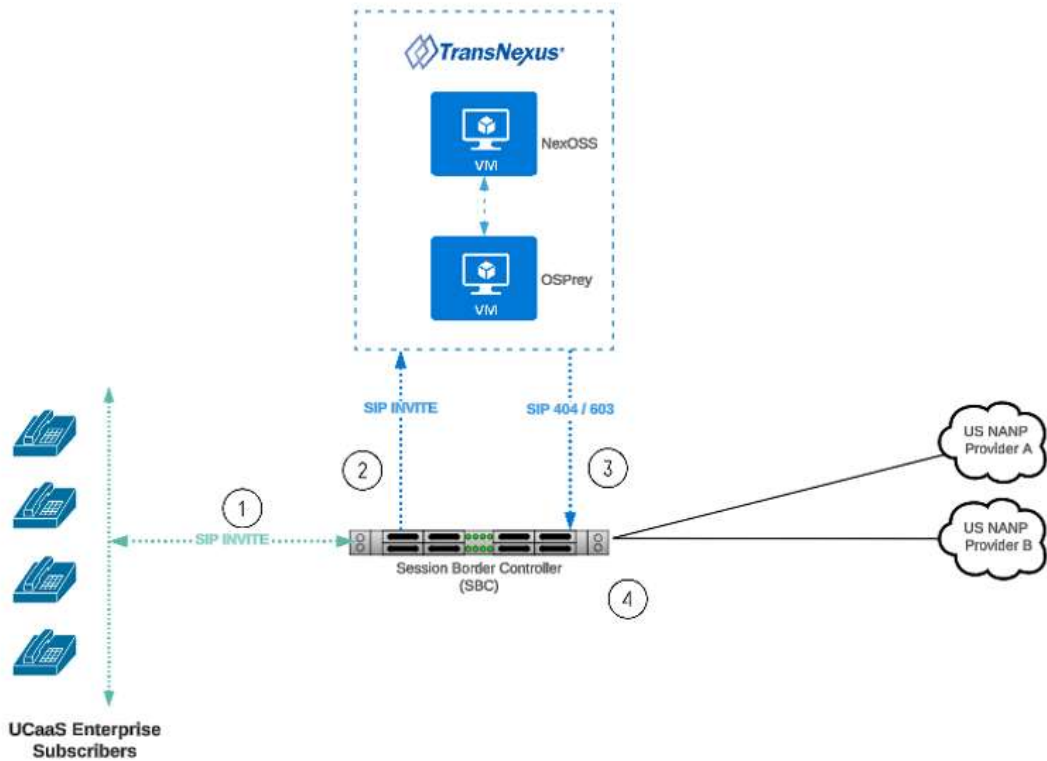
Upon detection of a robocall threat, the following actions are enforced:

1. Notify enterprise customers that suspicious traffic is blocked in real-time.
2. Block calls originating from identified customer enterprise location.
3. Generate automated alerts for further investigation by the compliance team.

	ROBOCALL MITIGATION POLICY				
	Issued on	Revised	Version	Document ID	Confidentiality
	7/7/2024	12/10/2024	2.0	GTS-IDSMP-002	PUBLIC

6. TECHNICAL DESIGN

GTS has adopted the TRANSNEXUS NEXOSS/OSPREY solution to implement its robocall mitigation controls.



The diagram above depicts the signaling real-time flow for mitigating robocalls.

	ROBOCALL MITIGATION POLICY				
	Issued on	Revised	Version	Document ID	Confidentiality
	7/7/2024	12/10/2024	2.0	GTS-IDSMP-002	PUBLIC

7. KYC

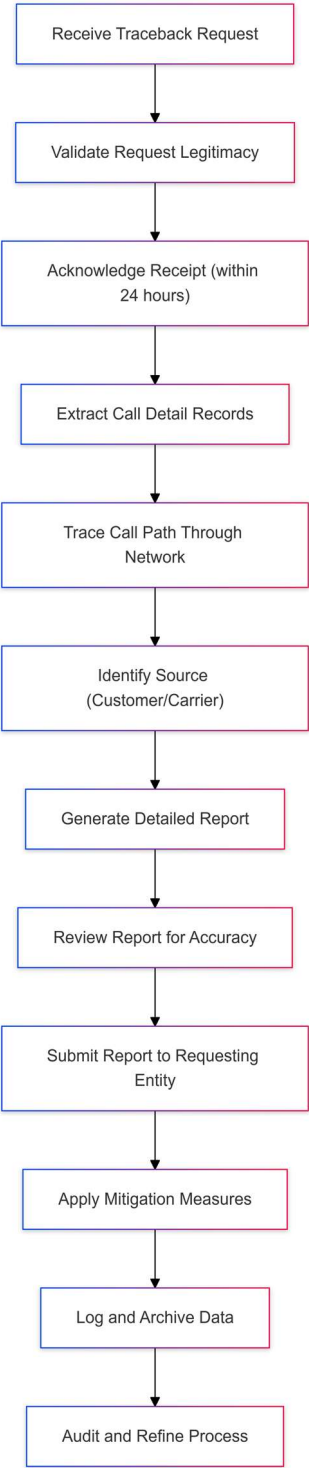
GTS's Know Your Customer (KYC) process is designed to ensure compliance with FCC regulations and to safeguard the integrity of our services by thoroughly understanding and verifying the businesses we work with.

This process begins by collecting detailed information about the customer's legal identity, including their entity type, incorporation details, and operational history, to confirm that they are a legitimate and traceable organization. Additionally, we require key contact information for individuals responsible for compliance and billing to ensure clear communication and accountability. We also assess the customer's geographical and operational scope, such as whether they operate internationally or manage servers outside the U.S., as this helps us evaluate their alignment with U.S. regulatory standards.

As part of ensuring adherence to FCC requirements, we ask customers to confirm their implementation of robocall mitigation measures, their willingness and commitment for their participation in traceback processes, and their registration in the Robocall Mitigation Database (RMD). Understanding their call management practices, including their use of telemarketing, automated dialing, and caller ID protocols, is essential to verify that their operations fall within legal parameters and avoid misuse of GTS's services.

Furthermore, we include provisions to protect GTS from liabilities, requiring customers to notify us of any material changes to their operations and to indemnify us in cases of misuse or noncompliance. By verifying all this information and requiring a certification of its authenticity, we not only ensure compliance with regulatory mandates but also build a foundation of trust and accountability with our customers, reducing risks associated with fraudulent or illegal activities and maintaining the integrity of the services we provide. This comprehensive approach allows GTS to fulfill its obligations.

8. TRACEBACK



GTS maintains a stringent traceback process to ensure immediate and thorough attention to traceback requests. The process is executed as follows:

Upon receipt of a traceback request from an authorized entity, such as the Industry Traceback Group (ITG) or the FCC, the designated Coordinator within GTS initiates the process by validating the request's legitimacy. This includes verifying the origin of the request, the associated call identifiers (ANI, timestamps, and other data), and the timeframe provided. Once confirmed, the coordinator acknowledges the request within 24 hours, formally confirming receipt and initiating internal investigation procedures.

The investigation begins with an immediate extraction of Call Detail Records (CDRs) from our Session Border Controllers as well as from our billing systems. Using timestamped call metadata, SIP logs, and routing information, the originating source of the call is traced across any possible network nodes or enterprise customer SIP Trunk. This includes identifying the upstream or downstream locations involved in the call's transit through the GTS network. The analysis is conducted within the defined 24-hour window to meet regulatory timelines. Simultaneously, the responsible customer or internal system associated with the flagged activity is identified and flagged for compliance verification.

Once the source is determined, the coordinator generates a detailed report containing the call's origin, path through the GTS network, and any anomalies or non-compliance detected. This report includes specific evidence from SIP logs, CDRs, and any real-time monitoring systems that may have flagged the call. The report is then reviewed by senior voice engineers to ensure accuracy and completeness before submission.

The completed report is submitted to the requesting entity, providing all required information and any supplementary documentation. If the traceback identifies a customer in violation of GTS's policies, immediate mitigation measures are enforced. These measures include call blocking, service suspension, or permanent termination of services. The responsible party is also notified of the violation and provided with a formal explanation of actions taken.

All traceback activities are logged and stored within GTS's repository for a minimum of two years. Logs include request details, investigation findings, communication records, and corrective actions taken. Regular audits of the traceback process are conducted to ensure adherence to standards and for continuous improvement. Network monitoring thresholds and mitigation protocols are dynamically adjusted based on findings to prevent similar incidents.

	ROBOCALL MITIGATION POLICY				
	Issued on	Revised	Version	Document ID	Confidentiality
	7/7/2024	12/10/2024	2.0	GTS-IDSMP-002	PUBLIC

9. GTS ROBOCALL MITIGATION AND STIR/SHAKEN ESCALATION LIST

LEVEL 1

compliance@teamgts.com
 Phone

LEVEL 2

Sadir Hamad
 Email: sadirh@teamgts.com
 Phone: 888-832-6487

*** END OF DOCUMENT ***