

UT TELECOM, LLC
ROBOCALL MITIGATION PLAN

2026

1. Executive Overview

UT Telecom, LLC ("UT Telecom") is committed to protecting the U.S. communications ecosystem from unlawful robocalls. As a registered Non-Gateway intermediate provider, UT Telecom is in the process to comply fully with the Federal Communications Commission's ("FCC" or "Commission") rules under 47 C.F.R. § 64.6305, the TRACED Act, and related Commission orders.

This Robocall Mitigation Program (RMP) outlines the reasonable and effective measures UT Telecom is in the process to implement to mitigate the origination, carriage, or processing of illegal robocalls. These measures will include robust STIR/SHAKEN authentication, proactive traffic monitoring and analytics, strict Know Your Customer (KYC) and Know Your Upstream Provider (KYUP) controls, and full cooperation with traceback investigations and law enforcement requests.

The Commission has explained that an RMP is sufficient if it includes detailed practices that can reasonably be expected to significantly reduce illegal robocalls and if the provider complies with those practices. Consistent with this guidance and industry best practices, UT Telecom's mitigation efforts focus on identifying and addressing potentially unlawful calls that may violate Section 227(b) of the Communications Act or the Truth in Caller ID Act, Section 227(e).

UT Telecom affirms that no prior certification has been removed by Commission action and that it is not prohibited from filing in the Robocall Mitigation Database (RMD).

2. Company Profile

- Legal Name: UT Telecom, LLC
- Principals: Ingrid Demelendez
- Primary Role: Intermediate Provider and U.S.-Based Voice Service Provider
- Focus: Wholesale carrier services and enterprise-level voice solutions
- Parent Company: None (Independent Entity)
- Subsidiaries: None

UT Telecom operates as a non-gateway intermediate provider that focuses its business and operations on the wholesale segment of the voice services communications market. The company provides international and domestic long distance voice termination through interconnections with telecommunications carriers, mobile operators, and other service providers.

3. Call Authentication (STIR/SHAKEN)

UT Telecom is in the process to fully implement STIR/SHAKEN (Secure Telephone Identity Revisited/Signature-based Handling of Asserted Information Using Tokens) protocols across its IP voice network.

- All SIP calls carrying U.S. North American Numbering Plan (NANP) numbers that are eligible for authentication are authenticated and transmitted with their identity tokens.

- Calls originating from UT Telecom's network will be signed with valid STIR/SHAKEN tokens, attesting to the verifiable nature of the caller ID information.
- Calls received from upstream providers that carry valid STIR/SHAKEN signatures are passed unaltered.
- Calls without valid authentication, or those exhibiting suspicious characteristics, are subjected to enhanced scrutiny, additional analysis, or blocking as described in Section 7 of this plan.

4. Know Your Customer (KYC) Protocol

UT Telecom implements strict Know Your Customer (KYC) protocols for all customers, regardless of UT Telecom's role in the call chain. These protocols are designed to support compliance with applicable regulatory requirements and to mitigate the risk of illegal robocalls and other unlawful or abusive traffic.

4.1 Customer Vetting and Onboarding

As part of its onboarding process, UT Telecom conducts a comprehensive review of each prospective customer prior to entering into a formal service agreement. This review includes the collection and verification of identity, business operations, regulatory status, and intended use of services. UT Telecom evaluates this information to reasonably assess whether the customer's activities appear to be legitimate and consistent with applicable federal and state telecommunications laws and regulations.

UT Telecom reserves the right to request additional information, documentation, or certifications at any time when necessary to satisfy regulatory, compliance, or risk management requirements. Customer onboarding and the continuation of any business relationship with UT Telecom are conditioned on the customer's timely, complete, and ongoing cooperation with these KYC requirements.

4.2 KYC Information Collected

Customers are required to provide the following information. Failure to comply with KYC requirements may result in delays, rejection, or discontinuation of service:

- Business registration and incorporation verification
- FCC Registration Number (FRN) and FCC Form 499 Filer ID
- Robocall Mitigation Database (RMD) filing status and certification
- Confirmation of company ownership, physical office address, and corporate website
- Contact information: main telephone number, official business email, and key personnel
- Bank and trade references for financial due diligence
- Type of voice services provided and description of business activities
- Confirmation of STIR/SHAKEN implementation status (where applicable)

4.3 Validation and Record Keeping

Upon receipt of the required information, UT Telecom conducts a validation process to ensure accuracy, which includes:

- Reviewing the customer's website, social media profiles, and LinkedIn presence
- Confirming the authenticity of FCC 499 filings and FCC registration numbers
- Verifying active registration in the Robocall Mitigation Database (RMD)
- Cross-checking provided information for consistency with RMD data

The Company maintains records of all KYC documentation, validation processes, and ongoing compliance reviews for auditing and regulatory purposes. KYC information is reviewed and updated on a recurring basis for all active customers.

5. Upstream Provider Controls (KYUP)

UT Telecom only accepts traffic from carriers and upstream providers that meet the following criteria:

- The provider is listed and active in the FCC's Robocall Mitigation Database (RMD)
- The provider's filing has not been subject to suspension or delisting due to enforcement actions by the Commission
- For domestic voice service providers, UT Telecom solely accepts calls if the provider's filing is listed in the RMD and compliant with 47 C.F.R. § 64.6305(e)(1)
- For foreign voice service providers and foreign intermediate providers utilizing the North American Numbering Plan, UT Telecom only accepts calls upon the provider's inclusion in the RMD and absence of delisting due to enforcement actions.

UT Telecom conducts periodic reviews of upstream provider status to ensure continued compliance with these requirements.

6. Acceptable Use Policy (AUP) and Contractual Provisions

UT Telecom requires all customers to execute a Master Service Agreement (MSA) that incorporates by reference the company's Acceptable Use Policy (AUP). These contractual provisions explicitly:

- Prohibit the use of UT Telecom services for unlawful, fraudulent, or deceptive purposes, including but not limited to: o Illegal robocalls and unsolicited telemarketing activities that violate the Telephone Consumer Protection Act (TCPA), Telemarketing Sales Rule (TSR), or state-level Do Not Call laws o Caller ID spoofing or other violations of the Truth in Caller ID Act, Section 227(e) o Transmission of traffic that violates federal, state, or international law
- Require customers to comply with all applicable federal, state, and international telecommunications laws and regulations
- Obligate customers to fully cooperate with UT Telecom in responding to traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG) within 24 hours, including disclosure of upstream provider information when necessary
- Require customers to maintain accurate and updated KYC information

Violation of these provisions, or reasonable suspicion of transmitting illegal robocalls, results in immediate suspension or termination of service without prior notice, at UT Telecom's sole discretion.

7. Network Monitoring, Analytics and Call Filtering

UT Telecom utilizes 46Labs Peeredge as its core session management and traffic monitoring platform. Through Peeredge and supplemental analytics tools, UT Telecom maintains continuous, 24/7 supervision of traffic across its network to identify suspicious patterns associated with illegal robocalls.

The Network Operations Center (NOC) team, supported by the Peeredge analytics platform, proactively monitors and enforces controls in alignment with FCC robocall mitigation requirements and industry best practices.

Key monitoring and filtering capabilities include:

- Traffic Analysis: Identifying abnormal traffic patterns through configurable calls-per-second (CPS) and session limits, with real-time anomaly detection
- Call Quality Metrics: Analyzing Answer Seizure Ratio (ASR), Average Call Duration (ACD), short-duration calls, and other key performance indicators to flag suspicious activity
- ANI Validation: Detecting and blocking calls with invalid, unassigned, or mismatched Automatic Number Identification (ANI) information
- IP Reputation Management: Blocking traffic from media IP addresses associated with known suspicious or unlawful robocall campaigns
- DNO Integration: Utilizing Somos Do-Not-Originate (DNO) lists to filter calls from numbers that should not originate calls, such as unassigned or government-exclusive numbers
- SIP Error Monitoring: Investigating unusual patterns of SIP error codes (404, 603, 607, etc.) that may indicate suspicious calling activity

When illegal robocalling or spoofing is suspected, UT Telecom promptly identifies the responsible party and takes appropriate action, including traffic filtering, blocking, or account suspension, in a timely manner.

UT Telecom affirms that, consistent with FCC rules, it will not block any emergency calls placed to 911 under any circumstances and will make all reasonable efforts to ensure that calls originating from Public Safety Answering Points (PSAPs) and other government emergency numbers are not blocked. These safeguards are integrated into UT Telecom's call blocking policies and monitoring systems to ensure uninterrupted access to emergency services, in full compliance with 47 C.F.R. §§ 64.1200(k)(9) and related Commission guidance.

8. Traceback Process and Enforcement Cooperation

UT Telecom diligently follows established protocols to address and respond to traceback requests in full compliance with 47 C.F.R. § 64.6305(a)(2), which requires providers to respond within 24 hours to traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG).

To meet these obligations, UT Telecom:

- 24-Hour Response: Commits to respond fully, within 24 hours, to all traceback requests from the Commission, law enforcement, and ITG, and to cooperate with such entities in investigating and stopping illegal robocallers that use its service to originate, carry, or process illegal robocalls
- Secure Portal Access: Utilizes the ITG's secure traceback portal to review and confirm traffic records, ensuring consistency and cooperation with investigations

- Ongoing Coordination: Exchanges information regarding suspicious traffic patterns with other voice service providers through established industry channels, including email and direct coordination
- Evidence Preservation: Maintains records of traceback requests, responses, and actions taken for audit and regulatory review

9. Mandatory Blocking and Commission Notifications

In accordance with the FCC's Gateway Provider Order and related rules, UT Telecom will:

- Promptly investigate any notification of suspected illegal traffic received from the Commission's Enforcement Bureau
- Block confirmed unlawful calls from traversing its network upon verification of illegal activity
- Document all actions taken, including investigations, findings, and blocking measures, for compliance and audit purposes
- Cooperate fully with the Commission and law enforcement in resolving identified issues UT Telecom adheres to the specified Process for Issuing a Notification of Suspected Illegal Traffic outlined in the Gateway Provider Report and Order to ensure effective resolution of such matters.

10. Updates to RMD Submission and RMP

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(c)(5) & (d)(5), UT Telecom will update its submission in the Robocall Mitigation Database (RMD) within 10 business days of any change to the applicable information, including material changes to this Robocall Mitigation Program.

11. Training and Awareness

UT Telecom provides ongoing training to its sales, commercial, and Network Operations Center (NOC) teams on robocall mitigation policies and procedures.

Training covers:

- FCC regulatory requirements and compliance obligations
- Identification of suspicious traffic patterns and red flags associated with illegal robocalls
- KYC and KYUP protocols and customer vetting procedures
- Traceback response obligations and escalation procedures • Documentation and record-keeping requirements

By ensuring that both commercial and technical staff are properly trained, UT Telecom reinforces compliance across all levels of the organization and strengthens its ability to prevent, detect, and respond to illegal robocall activity

12. Compliance Record and Audit Trail

UT Telecom maintains comprehensive records of all compliance-related activities, including:

- KYC documentation and validation records for all customers
- Traffic analysis data, monitoring logs, and filtering actions
- Traceback correspondence, responses, and investigation records
- Enforcement notifications and blocking actions

- Training records and policy acknowledgments

All records are preserved for a minimum period as required by applicable regulations and are available for audit and regulatory inspection upon request.

13. Commitment Statement

UT Telecom, LLC affirms its unwavering commitment to:

- Work towards full Stimulus/Shaken compliance with FCC regulations, including 47 C.F.R. § 64.6305, the TRACED Act, and all related Commission orders.
- Enforcing industry best practices and continuously improving mitigation measures to reduce unlawful robocalls.
- Cooperating fully with the Commission, law enforcement agencies, and industry partners in ongoing enforcement and traceback efforts.
- Protecting U.S. consumers from harmful and illegal robocall activity through proactive monitoring, strict vetting, and robust authentication.

By implementing these comprehensive measures, UT Telecom ensures the integrity of its voice services and remains a responsible participant in the fight against illegal robocalls.