

ROBOCALL MITIGATION DATABASE PLAN

Submitted Pursuant to:

47 C.F.R. § 64.6305 · FCC Report & Order, FCC 20-42
TRACED Act (Pub. L. No. 116-105) · Second Report and Order, FCC 21-60
Third Report and Order, FCC 22-7 · Fourth Report and Order, FCC 23-37

FILING ENTITY

Auralink Global Telecom

1221 Brickell Ave, Suite 900
Miami, FL 33131
Tel: 1-800-694-2158
support@auralinkglobaltelecom.com
Contact: Michael Alvarez

PLAN DETAILS

Document Type
Robocall Mitigation Database Plan

Provider Classification
Non-Gateway Provider & Voice Service Provider

STIR/SHAKEN Status
Full Implementation — Subject to Obligation

Version / Date
Version 1.0 · 2025

1. PROVIDER IDENTIFICATION AND CONTACT INFORMATION

Auralink Global Telecom (hereinafter "Auralink" or the "Company") submits this Robocall Mitigation Database Plan ("Plan") in accordance with 47 C.F.R. § 64.6305, the FCC's Report and Order in the Matter of Call Authentication Trust Anchor (FCC 20-42), the Second Report and Order (FCC 21-60), the Third Report and Order (FCC 22-7), the Fourth Report and Order (FCC 23-37), and the requirements of the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, Pub. L. No. 116-105. Auralink operates exclusively as a domestic voice service provider — all calls on its network originate and terminate within the United States — and is therefore not subject to the gateway provider obligations set forth in 47 C.F.R. § 64.6305(b). This Plan addresses Auralink's obligations as a non-gateway voice service provider with full STIR/SHAKEN implementation.

Legal Entity Name	Auralink Global Telecom
Trade Name (if any)	Auralink Global Telecom
Business Address	1221 Brickell Ave, Suite 900, Miami, FL 33131
Telephone Number	1-800-694-2158
Primary Contact	Michael Alvarez
Contact Email	michael@auralinkglobaltelecom.com
General Support Email	support@auralinkglobaltelecom.com
Plan Effective Date	2025
Plan Review Cycle	Annual (or upon material operational change)

This Plan is filed and maintained in the FCC's Robocall Mitigation Database (RMD) as required by 47 C.F.R. § 64.6305(a). Auralink will update this filing within thirty (30) days of any material change in its robocall mitigation practices, STIR/SHAKEN implementation status, provider classification, or contact information.

2. PROVIDER CLASSIFICATION AND REGULATORY FRAMEWORK

◆ 2.1 Provider Classification

Auralink Global Telecom is classified as a non-gateway voice service provider under the FCC's robocall mitigation framework. All calls handled by Auralink originate and terminate within the United States; Auralink does not receive or transmit calls entering the U.S. telecommunications network from foreign originating carriers or foreign-originated call paths. Accordingly, Auralink is not a "gateway provider" as defined under 47 C.F.R. § 64.1, and the gateway-specific obligations in 47 C.F.R. § 64.6305(b) do not apply. This Plan addresses Auralink's robocall mitigation obligations in its capacities as described below:

Classification	Description and Regulatory Obligations
Non-Gateway Provider	Auralink does not function as a gateway provider. It does not accept calls from foreign originating networks, does not serve as a point of entry for international traffic into the U.S. public switched telephone network, and has no foreign carrier interconnection arrangements. The gateway-specific obligations under 47 C.F.R. § 64.6305(b) — including mandatory blocking of international traffic and foreign carrier due diligence — are not applicable to Auralink's operations.
Voice Service Provider	Auralink provides originating and terminating voice communications services to business and residential end users in the United States. As a voice service provider, Auralink is subject to STIR/SHAKEN authentication obligations under 47 C.F.R. § 64.6301, robocall mitigation obligations under § 64.6305(a), call blocking requirements, upstream provider certification obligations, and all other rules applicable to voice service providers under the FCC's anti-robocall framework.

◆ 2.2 Applicable Regulatory Authority

Auralink's compliance obligations derive from the following primary regulatory sources:

- Telephone Consumer Protection Act (TCPA), 47 U.S.C. § 227
- TRACED Act, Pub. L. No. 116-105 (Dec. 30, 2019)
- Communications Act of 1934, as amended, 47 U.S.C. §§ 151 et seq.
- 47 C.F.R. Part 64, Subpart Z — Caller ID Authentication
- FCC Report & Order, FCC 20-42 (Mar. 31, 2020) — STIR/SHAKEN mandate for voice service providers
- FCC Second Report & Order, FCC 21-60 (Jun. 17, 2021) — Robocall mitigation requirements
- FCC Third Report & Order, FCC 22-7 (Feb. 4, 2022) — Additional blocking requirements and RMD obligations
- FCC Fourth Report & Order, FCC 23-37 — Upstream provider certification and RMD filing requirements
- FCC Declaratory Ruling and Order, FCC 22-38 — Call blocking safe harbor for voice service providers
- Industry Technical Standards: ATIS-1000074 (SHAKEN), RFC 8224, RFC 8225, RFC 8226

◆ 2.3 Summary of Applicable Obligations

The following table identifies the FCC robocall mitigation obligations applicable to Auralink as a non-gateway voice service provider and confirms Auralink's compliance status with respect to each:

Obligation	Applicable to Auralink	Auralink Status
------------	------------------------	-----------------

STIR/SHAKEN Implementation (47 C.F.R. § 64.6301)	Yes — Required	Fully Implemented
RMD Filing (47 C.F.R. § 64.6305(a))	Yes — Required	Filed
Upstream Provider Certification (47 C.F.R. § 64.6305(a))	Yes — Required	Compliant
Illegal Traffic Blocking (47 C.F.R. § 64.1200(k))	Yes — Required	Active
Do-Not-Originate (DNO) List Compliance	Yes — Required	Active
Traceback Cooperation (USTelecom ITG)	Yes — Required	Active
Analytics-Based Call Blocking	Yes — Required	Active
Erroneous Blocking Dispute Process	Yes — Required	Active
Reassigned Numbers Database (RND) Compliance	Yes — Required	Active
Annual Robocall Mitigation Reporting	Yes — Required	Compliant
Enforcement Cooperation (FCC/DOJ/FTC/State AG)	Yes — Required	Compliant
Gateway Provider Obligations (47 C.F.R. § 64.6305(b))	Not Applicable	N/A — Non-Gateway

3. STIR/SHAKEN IMPLEMENTATION

◆ 3.1 Implementation Status

Auralink Global Telecom has fully implemented the STIR/SHAKEN caller ID authentication framework on its IP network in accordance with 47 C.F.R. § 64.6301 and the standards established by ATIS (ATIS-1000074) and the Internet Engineering Task Force (RFC 8224, RFC 8225, RFC 8226). Auralink is not claiming any exemption or extension with respect to STIR/SHAKEN implementation.

◆ 3.2 Certificate Authority and Token Issuance

Auralink has obtained and maintains valid Service Provider Codes (SPC) and digital certificates issued by an authorized Certificate Authority (CA) accredited by the STI-PA (Secure Telephone Identity Policy Administrator), currently managed by iconectiv as the FCC-designated STI-PA.

STI-PA: iconectiv (FCC-designated Secure Telephone Identity Policy Administrator)

Certificate Type: Service Provider Code (SPC) Token

Certificate Renewal Cycle: Annual, or upon expiration per STI-PA requirements

Token Issuance Authority: Authorized STI-CA (Secure Telephone Identity Certification Authority)

◆ 3.3 Attestation Levels

Auralink applies attestation levels to outbound calls based on the level of verification achievable for the calling party, consistent with the framework established under ATIS-1000074 and the FCC's orders:

Level	Attestation Type	Application Criteria
A	Full Attestation	Applied when Auralink is the originating carrier, has a direct customer relationship with the subscriber, and has verified that the subscriber is authorized to use the calling number in full compliance with Auralink's Know Your Customer (KYC) and number management processes.
B	Partial Attestation	Applied when Auralink has authenticated the originating call source and verified that the call was originated from a known customer or entity, but cannot verify that the customer is authorized to use the specific calling number (e.g., calls from a PBX or multi-line business where full number authorization is not confirmed).
C	Transit / Pass-Through Attestation	Applied when Auralink is transiting a call received from a domestic upstream carrier and cannot independently verify that the originating party is authorized to use the calling number. Auralink attests only that it received the call from a known domestic carrier but cannot confirm subscriber identity or number authorization. This level is used sparingly and only for domestically originated transiting traffic.

◆ 3.4 STIR/SHAKEN Signing and Verification

Auralink signs outbound calls using a SIP Identity header in accordance with RFC 8224 and ATIS-1000074. For inbound calls, Auralink verifies the PASSporT (Personal Assertion Token) in the SIP Identity header where technically feasible, including checking certificate validity, signature integrity, and attestation level.

◆ 3.5 Non-IP Networks and Interoperability

For calls that traverse non-IP (TDM) network segments where STIR/SHAKEN signing is not technically feasible, Auralink implements Out-of-Band (OOB) STIR/SHAKEN or passes available authentication information to downstream providers to the maximum extent technically feasible, consistent with FCC guidance. Auralink is actively working to convert legacy TDM interconnections to IP-based interconnections to maximize STIR/SHAKEN coverage.

◆ 3.6 Number Authorization and KYC Procedures

Auralink maintains a formal Know Your Customer (KYC) program to ensure that STIR/SHAKEN Full Attestation (Level A) is applied only to customers who have been verified as authorized users of their assigned numbers. Key elements of the KYC program include:

- Identity verification of all business and enterprise customers prior to service activation, including collection of legal entity documentation, beneficial ownership information, and number assignment records;
- Verification that customer-assigned telephone numbers are duly allocated from the North American Numbering Plan Administrator (NANPA) or ported numbers for which ownership has been confirmed;
- Ongoing monitoring of customer calling patterns to detect anomalies inconsistent with authorized number use;
- Prompt investigation and remediation of any identified unauthorized number use, including suspension of STIR/SHAKEN signing authority pending investigation;
- Annual review and re-verification of all active enterprise and wholesale customers.

◆ 3.7 STIR/SHAKEN Records

Auralink maintains records of STIR/SHAKEN signing and verification activities, including logs of attestation levels applied, certificate usage, and any anomalies identified during verification, for a minimum period of two (2) years. These records are available to the FCC and law enforcement upon lawful request.

4. NON-GATEWAY PROVIDER ROBOCALL MITIGATION OBLIGATIONS

◆ 4.1 Scope and Non-Gateway Confirmation

Auralink Global Telecom confirms that it does not operate as a gateway provider as defined under 47 C.F.R. § 64.1. All traffic handled by Auralink's network originates and terminates within the United States. Auralink does not receive calls entering the U.S. network from foreign originating carriers, does not maintain international gateway facilities, and does not have interconnection arrangements with foreign telecommunications carriers. The obligations described in this Section reflect Auralink's robocall mitigation responsibilities as a domestic non-gateway voice service provider under 47 C.F.R. § 64.6305(a).

◆ 4.2 Domestic Upstream Provider Due Diligence

Although Auralink is not subject to the foreign carrier due diligence requirements applicable to gateway providers, Auralink conducts rigorous due diligence on all domestic upstream carriers and originating providers from which it accepts traffic. This program includes:

- Pre-activation verification that each upstream domestic carrier is a licensed U.S. telecommunications provider in good standing, with an active FCC Registration Number (FRN) and a current RMD filing where required;
- Confirmation that each upstream provider has filed a Robocall Mitigation Plan with the FCC's Robocall Mitigation Database, or is otherwise exempt from that requirement, prior to accepting traffic from that provider;
- Collection of contractual anti-robocall representations from all upstream carriers, including representations that the carrier will not knowingly route illegal robocall traffic to Auralink and will cooperate with traceback investigations;
- Ongoing monitoring of traffic patterns from each upstream carrier for indicators of illegal robocall activity, including abnormal ANI distributions, high call failure rates, and calling number clustering inconsistent with legitimate calling patterns;
- Suspension or termination of traffic acceptance from any upstream carrier that fails to cooperate with traceback investigations, repeatedly routes confirmed illegal traffic, or whose RMD filing lapses or is removed from the database;
- Annual re-evaluation of all active upstream carrier relationships for continued compliance.

◆ 4.3 Mandatory Blocking of Illegal Domestic Traffic

Auralink implements mandatory blocking of calls exhibiting characteristics of illegal robocall activity on its domestic network, consistent with 47 C.F.R. § 64.1200(k) and applicable FCC orders. Blocking criteria include:

- Calls from telephone numbers on the FCC's Do-Not-Originate (DNO) list, including numbers designated as subject to illegal spoofing (e.g., 911, 211, 511, N11 codes, unallocated NANP numbers, and government agency numbers identified by the FCC as spoofed);
- Calls carrying malformed, invalid, or non-conforming calling party numbers that do not comply with NANP E.164 formatting standards;
- Calls from number ranges identified by the FCC, USTelecom's Industry Traceback Group (ITG), or Auralink's internal analytics as associated with confirmed illegal robocall campaigns;
- Calls for which Auralink has received a lawful direction from the FCC, a court order, or a verified law enforcement request to block;
- Calls identified through Auralink's analytics platform as exhibiting high-confidence robocall signatures, consistent with Auralink's call blocking safe harbor practices under 47 C.F.R. § 64.1200(k).

◆ 4.4 Do-Not-Originate (DNO) List Compliance

Auralink subscribes to and actively applies the FCC's DNO list and supplementary DNO resources for domestic traffic. Auralink's DNO list management practices include:

- Daily automated synchronization with the FCC's published DNO list;
- Integration of DNO list checks into call routing logic at the network ingress point for all inbound traffic from upstream carriers;
- Maintenance of Auralink's proprietary internal DNO additions based on traceback findings, consumer complaints, and law enforcement input;
- Quarterly review of Auralink's proprietary DNO additions for ongoing accuracy and validity;
- Logging of all calls matched against the DNO list, retained for a minimum of two (2) years.

◆ 4.5 Upstream Provider RMD Verification

Consistent with 47 C.F.R. § 64.6305(a) and FCC Fourth Report and Order (FCC 23-37), Auralink verifies the RMD filing status of all domestic upstream providers from which it accepts voice traffic. Auralink will not accept traffic from any provider that:

- Is required to file an RMD plan but has not done so, or whose RMD filing has been removed by the FCC;
- Has been identified by the FCC as a provider that has failed to implement STIR/SHAKEN or an approved robocall mitigation program, and has not remedied that failure within the FCC's prescribed timeframe;
- Has been subject to a cease-and-desist or similar order from the FCC related to illegal robocall traffic.

Auralink performs RMD verification checks upon onboarding each new upstream carrier and re-verifies RMD status quarterly for all active upstream providers. Records of these checks are maintained for a minimum of two (2) years.

◆ 4.6 Traceback Cooperation

Auralink cooperates fully with USTelecom's Industry Traceback Group (ITG) and complies with the traceback framework recognized by the FCC. Auralink's traceback obligations and practices include:

- Responding to traceback requests from the ITG within forty-eight (48) hours of receipt, and within twenty-four (24) hours for requests designated as urgent by the ITG or the FCC;
- Providing upstream provider information, call detail records (CDRs), and other information necessary to trace illegal call campaigns to their domestic source;
- Designating a Traceback Point of Contact (PoC) — currently Michael Alvarez — who is available during normal business hours and reachable by emergency contact outside business hours;
- Maintaining CDRs with sufficient detail (ANI, DNIS, timestamp, trunk group identifier, upstream provider identifier) to support traceback investigations, retained for a minimum of two (2) years;
- Participating in ITG working groups and cooperative investigations as requested.

Traceback Contact: Michael Alvarez | michael@auralinkglobaltelecom.com | 1-800-694-2158

5. VOICE SERVICE PROVIDER ROBOCALL MITIGATION OBLIGATIONS

◆ 5.1 Scope of Voice Service Operations

In its capacity as a voice service provider, Auralink provides originating and terminating voice communications services to business and residential customers. Auralink's voice service operations are subject to the robocall mitigation requirements described in this Section.

◆ 5.2 Call Analytics and Blocking

Auralink implements an analytics-based call blocking program to identify and block calls exhibiting characteristics of illegal robocall campaigns before they are delivered to end users or downstream carriers. The program includes:

- Deployment of a real-time call analytics platform that scores inbound and transiting calls based on risk indicators including calling number reputation, calling pattern anomalies, traffic volume spikes, and STIR/SHAKEN attestation levels;
- Automatic blocking of calls receiving a high-risk score exceeding Auralink's established blocking threshold, with manual review of calls in the moderate-risk range;
- Blocking of calls from numbers appearing on the Reassigned Numbers Database (RND) where the calling party has not demonstrated current assignment;
- Implementation of the FCC's call blocking safe harbor (47 C.F.R. § 64.1200(k)) for calls blocked based on reasonable analytics;
- Retention of blocking logs for a minimum of two (2) years;
- Provision of a customer-accessible mechanism for reporting erroneously blocked calls, as described in Section 5.4.

◆ 5.3 Customer Onboarding and Calling Campaign Review

Auralink maintains a customer onboarding and ongoing monitoring process specifically designed to prevent customers from using Auralink's network to conduct illegal robocall campaigns:

- All prospective business and wholesale customers are subject to a pre-activation review that includes identity verification, business purpose assessment, and evaluation of intended calling use cases;
- Customers intending to conduct high-volume outbound calling campaigns must disclose the nature of their campaign and provide confirmation of compliance with the TCPA, including consent documentation practices and opt-out mechanisms;
- Auralink reserves the right to require pre-approval of calling campaigns that meet defined volume or pattern thresholds;
- Auralink's acceptable use policy (AUP) explicitly prohibits use of Auralink's network to place illegal robocalls, spoof caller ID, or engage in any calling practice that violates the TCPA, FCC rules, or state laws;
- Violation of the AUP is grounds for immediate service suspension and termination, and referral to law enforcement authorities.

◆ 5.4 Erroneous Blocking Dispute Resolution

Auralink provides a documented process for callers whose legitimate calls have been erroneously blocked to seek reinstatement of their number from any internal block list or block recommendation:

- Callers may submit erroneous blocking complaints to support@auralinkglobaltelecom.com or by calling 1-800-694-2158;
- Auralink will acknowledge receipt of all erroneous blocking complaints within one (1) Business Day;

- Auralink will investigate and provide a substantive response within five (5) Business Days;
- Where an erroneous block is confirmed, Auralink will reinstate the number within twenty-four (24) hours of the determination and implement measures to prevent recurrence;
- Auralink will maintain records of all erroneous blocking complaints and resolutions for a minimum of two (2) years.

◆ 5.5 Reassigned Numbers Database (RND) Compliance

Auralink queries the FCC's Reassigned Numbers Database (RND) as required to identify calls directed to numbers that may have been reassigned, consistent with 47 C.F.R. § 64.1200(n). Auralink's automated systems are configured to flag calls to numbers that appear in the RND as recently reassigned, enabling appropriate routing or blocking decisions.

◆ 5.6 National Do Not Call Registry

To the extent Auralink's customers place outbound telemarketing calls, Auralink's AUP requires those customers to maintain compliance with the National Do Not Call (DNC) Registry administered by the FTC (16 C.F.R. Part 310) and applicable state DNC registries. Auralink does not facilitate telemarketing calling campaigns without confirming that the responsible customer has represented compliance with DNC Registry requirements.

6. TRAFFIC MONITORING, ANALYTICS, AND ANOMALY DETECTION

◆ 6.1 Real-Time Monitoring

Auralink operates a 24x7 network monitoring capability focused on detecting calling patterns that may indicate illegal robocall activity. Monitored metrics include:

- Calls per second (CPS) and calls per minute (CPM) per originating source, trunk group, and customer;
- Answer-to-seizure ratios and call completion rates, with alerting on deviations from established baselines;
- Calling number concentration — the ratio of unique calling numbers to total call volume, used to detect artificial number cycling;
- Geographic dispersion of called numbers, with alerting on unusual geographic concentration patterns;
- STIR/SHAKEN attestation level distribution across trunk groups, with alerting on unusual shifts toward lower attestation levels;
- Calls from numbers appearing on DNO lists, FCC-published illegal number lists, or Auralink's internal block lists.

◆ 6.2 Automated Alerting and Response

Auralink's monitoring platform is configured to generate automated alerts and, where appropriate, automated responses for the following triggering conditions:

Triggering Condition	Automated Response	Human Review Timeframe
CPS spike > 200% of 30-day baseline	Rate limiting applied	Within 30 minutes
DNO list match	Automatic block	Daily audit review
Calling number cycling (>500 ANIs/hour per source)	Traffic hold, alert generated	Within 1 hour
STIR/SHAKEN failure rate > 15% on a trunk group	Alert generated	Within 2 hours
Traceback request received (ITG)	Ticket opened, PoC notified	Within 24 hours (urgent: 6 hrs)
Upstream carrier anomaly or RMD status lapse detected	Rate limiting, investigation opened	Within 4 hours
FCC enforcement notification received	Escalation to senior management	Immediate

◆ 6.3 Call Detail Record Retention

Auralink retains Call Detail Records (CDRs) that include, at minimum, the following data elements: originating ANI, terminating DNIS, call timestamp (date, time, time zone), call duration, trunk group identifier, upstream domestic provider identifier, STIR/SHAKEN attestation level (where applicable), and disposition (completed, blocked, failed). CDRs are retained for a minimum of twenty-four (24) months and are available for production to the FCC, law enforcement agencies, and the ITG in response to lawful requests.

7. ENFORCEMENT COOPERATION AND COMPLAINT RESPONSE

◆ 7.1 FCC Enforcement Cooperation

Auralink is committed to full cooperation with the FCC's enforcement efforts against illegal robocalls, including those initiated by the FCC Enforcement Bureau. Upon receipt of a notice of apparent liability, a citation, an informal investigation letter, or any other enforcement communication from the FCC, Auralink will:

- Acknowledge receipt within one (1) Business Day;
- Assign a designated internal compliance officer to coordinate the response;
- Provide all requested records, CDRs, and documentation within the timeframe specified by the FCC, and in no event later than ten (10) Business Days unless an extension is granted;
- Implement any directed interim blocking or mitigation measures within twenty-four (24) hours of the FCC's direction;
- Provide written confirmation of compliance measures taken.

◆ 7.2 Law Enforcement Cooperation

Auralink cooperates with federal and state law enforcement agencies, including the Department of Justice (DOJ), Federal Trade Commission (FTC), state attorneys general, and other agencies investigating illegal robocall activity. Cooperation includes provision of CDRs, network logs, and customer records pursuant to lawful legal process (subpoenas, court orders, national security letters). Auralink maintains an internal law enforcement response protocol and designates a law enforcement liaison.

◆ 7.3 Consumer Complaint Handling

Auralink maintains a consumer complaint intake and response process for complaints related to robocalls, illegal spoofing, and unwanted calls:

- Complaints may be submitted via email to support@auralinkglobaltelecom.com or by telephone at 1-800-694-2158;
- Auralink will acknowledge receipt of all complaints within two (2) Business Days;
- Complaints will be investigated and a substantive response provided within ten (10) Business Days;
- Complaints determined to involve a potential TCPA or FCC rules violation will be escalated to the compliance team for immediate action and, where appropriate, referral to the ITG or law enforcement;
- Complaint records are retained for a minimum of two (2) years.

◆ 7.4 Immediate Action Protocol

Upon receiving credible evidence of an active illegal robocall campaign routing through Auralink's network — whether from consumer complaints, traceback requests, law enforcement direction, or internal monitoring — Auralink will initiate its Immediate Action Protocol:

- Step 1: Quarantine — Traffic from the identified source is placed in a temporary hold within four (4) hours;
- Step 2: Investigate — Compliance team reviews CDRs and upstream provider information within twenty-four (24) hours;
- Step 3: Block or Suspend — If the investigation confirms illegal robocall activity, the source is blocked and the responsible customer or upstream provider is suspended within twenty-four (24) hours of confirmation;
- Step 4: Report — Auralink notifies the ITG and, as appropriate, the FCC and relevant law enforcement within forty-eight (48) hours of taking blocking action;

- Step 5: Document — All actions are documented in Auralink's compliance incident log, retained for a minimum of two (2) years.

8. INTERNAL COMPLIANCE PROGRAM

◆ 8.1 Compliance Governance

Auralink has established an internal compliance program dedicated to robocall mitigation and caller ID authentication. The program is overseen by the designated Robocall Mitigation Compliance Officer (currently Michael Alvarez) and includes the following organizational elements:

- Robocall Mitigation Compliance Officer: Responsible for maintaining this Plan, overseeing STIR/SHAKEN compliance, managing traceback responses, and coordinating with the FCC and ITG;
- Network Operations Center (NOC): Responsible for 24x7 traffic monitoring, automated alerting, and first-level response to anomalies;
- Legal and Regulatory Affairs: Responsible for monitoring FCC rulemaking developments, updating the compliance program, and managing enforcement responses;
- Customer Operations: Responsible for AUP enforcement, customer onboarding screening, and complaint intake.

◆ 8.2 Training

Auralink provides mandatory robocall mitigation training to all employees with responsibilities relevant to the implementation of this Plan, including customer-facing staff, network operations personnel, and management. Training covers:

- Overview of FCC robocall mitigation rules and STIR/SHAKEN obligations;
- Identification of red flags for illegal robocall activity in customer calling patterns;
- Traceback cooperation procedures and escalation protocols;
- STIR/SHAKEN attestation level determination criteria;
- Complaint handling and immediate action protocols.

Training is conducted upon hire and at least annually thereafter. Training completion records are maintained for a minimum of three (3) years.

◆ 8.3 Policy Reviews and Updates

Auralink reviews this Robocall Mitigation Database Plan and its associated internal policies at least annually, or promptly following any material change in:

- Auralink's network architecture, services, or provider classification;
- FCC rules, orders, or guidance affecting robocall mitigation or STIR/SHAKEN obligations;
- Industry standards (ATIS, IETF) affecting caller ID authentication;
- Auralink's STIR/SHAKEN implementation status or STI-PA/STI-CA relationships;
- Material changes in Auralink's upstream carrier relationships or network architecture.

Updates to this Plan will be reflected in a revised RMD filing within thirty (30) days of the triggering change.

◆ 8.4 Record Retention Summary

Record Type	Retention Period	Responsible Party
Call Detail Records (CDRs)	24 months	Network Operations
STIR/SHAKEN signing/verification logs	24 months	Network / Compliance
DNO list match logs	24 months	Network Operations

Traceback request records and responses	24 months	Compliance Officer
Upstream provider certifications	Duration of relationship + 2 years	Compliance / Legal
Consumer complaint records	24 months	Customer Operations
Blocking decision logs	24 months	Network Operations
Training completion records	36 months	HR / Compliance
Compliance incident logs	24 months	Compliance Officer
FCC/Law enforcement correspondence	5 years	Legal Affairs

9. REGULATORY CONTACT DIRECTORY

The following contacts are designated for purposes of this Plan and the FCC's Robocall Mitigation Database filing:

Robocall Mitigation Compliance Officer	Michael Alvarez
Compliance Officer Email	michael@auralinkglobaltelecom.com
Compliance Officer Phone	1-800-694-2158
General Support / Complaints	support@auralinkglobaltelecom.com
General Support Phone	1-800-694-2158
Traceback PoC (ITG)	Michael Alvarez — michael@auralinkglobaltelecom.com
Law Enforcement Liaison	Michael Alvarez — michael@auralinkglobaltelecom.com
FCC Enforcement PoC	Michael Alvarez — michael@auralinkglobaltelecom.com
Erroneous Blocking Disputes	support@auralinkglobaltelecom.com 1-800-694-2158
Mailing Address	1221 Brickell Ave, Suite 900, Miami, FL 33131
Business Hours	Monday–Friday, 9:00 AM – 6:00 PM Eastern Time
After-Hours Emergencies	1-800-694-2158 (on-call rotation)

10. CERTIFICATIONS AND ATTESTATIONS

◆ 10.1 STIR/SHAKEN Implementation Certification

Pursuant to 47 C.F.R. § 64.6305(a)(1)(i), Auralink Global Telecom hereby certifies that it has fully implemented the STIR/SHAKEN caller ID authentication framework on its IP network in accordance with the standards and requirements established by the FCC's Report and Order (FCC 20-42), Second Report and Order (FCC 21-60), Third Report and Order (FCC 22-7), Fourth Report and Order (FCC 23-37), and applicable ATIS and IETF standards. Auralink is not claiming any exemption or extension from the STIR/SHAKEN implementation requirement.

◆ 10.2 Robocall Mitigation Program Certification

Pursuant to 47 C.F.R. § 64.6305(a)(1)(ii), Auralink Global Telecom hereby certifies that it has implemented a robocall mitigation program that includes the practices described in this Plan. Auralink certifies that it takes affirmative steps to avoid being a source of illegal robocall traffic, will fully cooperate with traceback requests from the Industry Traceback Group (ITG) and other authorized parties, and will not allow customers to use Auralink's network as a conduit for illegal robocall campaigns. Auralink further certifies that it will respond to all traceback requests from the ITG within the timeframes specified in Section 4.6 of this Plan. Auralink confirms that it operates exclusively as a non-gateway voice service provider and that all traffic on its network originates and terminates within the United States.

◆ 10.3 Upstream Provider Certification Compliance

Pursuant to 47 C.F.R. § 64.6305(a) and the FCC's Fourth Report and Order (FCC 23-37), Auralink Global Telecom certifies that it has obtained, or is in the process of obtaining, certifications from all domestic upstream providers as required under applicable FCC rules, and that Auralink will not accept traffic from any provider that has been removed from the FCC's Robocall Mitigation Database or that has failed to file a required RMD certification. Auralink certifies that it maintains a process to verify the RMD filing status of all domestic upstream providers from which it accepts traffic, and that no traffic is accepted from providers subject to active FCC cease-and-desist or equivalent enforcement action related to illegal robocall traffic. Auralink further confirms that the gateway provider upstream certification requirements under 47 C.F.R. § 64.6305(b)(4) do not apply to Auralink's operations, as Auralink is not a gateway provider.

◆ 10.4 Accuracy of Filing

The undersigned authorized representative of Auralink Global Telecom hereby certifies that the information contained in this Robocall Mitigation Database Plan is true, complete, and accurate to the best of the

undersigned's knowledge and belief, and that Auralink Global Telecom has implemented, or will implement within the timeframes specified herein, all robocall mitigation measures described in this Plan. The undersigned understands that the submission of false or misleading information to the FCC may subject Auralink Global Telecom and its officers to civil and criminal penalties under 47 U.S.C. § 220 and other applicable statutes.

— END OF ROBOCALL MITIGATION DATABASE PLAN —

Auralink Global Telecom · support@auralinkglobaltelecom.com · 1-800-694-2158