

ROBOCALL MITIGATION PLAN

Prepared pursuant to 47 C.F.R. § 64.6305

Company: DigiTalker LLC
FCC Registration Number (FRN): 0038436135
Operating Company Number (OCN): 437M
USAC Form 499 Filer ID: 838951
EIN: 36-5178509
Effective Date: August 3, 2026
Plan Version: 3.0
Compliance Officer: Hussain Dawood Chanchwelia, Director

Version 3.0 supersedes Version 2.0 (July 15, 2026). This revision records DigiTalker's implementation of the STIR/SHAKEN caller identification authentication framework on the traffic it originates. Version 2.0 recorded DigiTalker's cessation of gateway and non-gateway intermediate provider activity; DigiTalker continues to operate solely as a voice service provider.

1. Company Identification

DigiTalker LLC ("DigiTalker" or the "Company") is a limited liability company formed under the laws of the State of Delaware on April 28, 2026 (Delaware File Number 10601626). The Company's Employer Identification Number is 36-5178509, and its FCC Registration Number is 0038436135. DigiTalker is registered with the Universal Service Administrative Company as FCC Form 499 Filer ID 838951, and was assigned Operating Company Number 437M on July 2, 2026.

The Company's principal place of business is located at 5904 Jessamine St, STE A15, Houston, TX 77081, United States. DigiTalker operates as a wholesale voice service provider. The Company originates outbound United States-bound voice traffic on behalf of its customers using its own softswitch infrastructure, and uses third-party Direct Inward Dialing numbers ("DIDs") as caller identification on outbound traffic. DigiTalker does not own North American Numbering Plan resources and does not hold a Carrier Identification Code.

Designated Contacts

Compliance Officer / Robocall Mitigation Contact: Hussain Dawood Chanchwelia, Director

- Email: contact@digitaltalker.uk
- Officer email: hussain@digitaltalker.uk
- Telephone: +1 917-730-4364

D.C. Agent for Service of Process: Northwest Registered Agent Service Inc., 1717 N Street NW, STE 1, Washington, DC 20036; telephone 509-768-2249; email support@northwestregisteredagent.com.

2. Provider Role Self-Classification

Consistent with 47 C.F.R. § 64.6300, DigiTalker classifies its provider role as follows:

- Voice Service Provider: DigiTalker originates outbound voice traffic onto the United States public switched telephone network through its own softswitch infrastructure. DigiTalker is the first provider in the call path to place its customers' calls onto the United States network; it originates those calls and does not receive them, already in progress, from another provider.

DigiTalker does not act as a gateway provider and does not act as a non-gateway intermediate provider. It does not receive calls directly from any foreign originating provider or foreign intermediate provider for transmission downstream to a United States provider, and it does not carry or transit calls between two United States-based providers. Because DigiTalker originates the traffic it handles, it does not function as an intermediate provider with

respect to that traffic, and the gateway and non-gateway intermediate provider classifications defined in 47 C.F.R. § 64.6300 do not apply to it. DigiTalker has registered its provider classification in the FCC Robocall Mitigation Database and certifies that it complies with the robocall mitigation obligations applicable to a voice service provider.

3. STIR/SHAKEN Implementation

3.1 Implementation Status

DigiTalker has implemented the STIR/SHAKEN caller identification authentication framework. As of August 3, 2026, DigiTalker authenticates the calls it originates using its own SHAKEN authentication certificate, consistent with 47 C.F.R. § 64.6301(a). Authentication is performed on DigiTalker's ConnexCS softswitch, which applies a SIP Identity header carrying a signed PASSporT to each call DigiTalker places onto the United States public switched telephone network.

DigiTalker continues to maintain the robocall mitigation program described in this Plan, consistent with 47 C.F.R. § 64.6305(a), and applies that program to all traffic it originates.

3.2 Credentialing

DigiTalker holds the credentials required under the Secure Telephone Identity Governance Authority's SPC Token Access Policy and under the SHAKEN certificate governance framework:

- FCC Form 499A: DigiTalker is registered with the Universal Service Administrative Company as FCC Form 499 Filer ID 838951.
- Operating Company Number: DigiTalker was assigned OCN 437M on July 2, 2026.
- Robocall Mitigation Database: DigiTalker is listed in the Robocall Mitigation Database and certifies compliance with the Commission's requirements through this Plan.
- Service Provider Code token: DigiTalker maintains a Service Provider account with the Secure Telephone Identity Policy Administrator (iconectiv). That registration has completed the Policy Administrator's vetting, and DigiTalker obtains its Service Provider Code token through that account.
- Authentication certificate: DigiTalker holds a SHAKEN authentication certificate issued to OCN 437M by Peeringhub, a Certification Authority approved by the Secure Telephone Identity Policy Administrator. The certificate is published at the certificate repository location referenced in the Identity header of DigiTalker's signed calls.

3.3 Attestation

DigiTalker signs every call it originates, and determines the attestation level for each call in accordance with ATIS-1000074:

- Attestation A (Full Attestation): applied where DigiTalker originated the call onto the network, has a direct authenticated relationship with the customer placing the call, and has established that the customer is authorized to use the calling number presented, that number being a DID assigned to that customer by DigiTalker under Section 9 of this Plan.
- Attestation B (Partial Attestation): applied where DigiTalker originated the call and has a direct authenticated relationship with the customer, but has not established the customer's right to use the particular calling number presented.
- Attestation C (Gateway Attestation): applied where DigiTalker cannot establish the customer's right to use the calling number and cannot attest to the source of the call beyond the point at which it entered DigiTalker's network.

The attestation level applied to a call reflects what DigiTalker's records substantiate for that call and calling number. DigiTalker does not apply an attestation level higher than its records support, and the attestation level applied to a customer is reassessed whenever that customer's know-your-customer file or assigned DID inventory changes.

3.4 Certificate and Key Management

- The signing key pair was generated through DigiTalker's Certification Authority service and the private key is installed within DigiTalker's ConnexCS softswitch environment. Access to the private key is restricted to authorized DigiTalker personnel, and the key is not distributed to customers, resellers, or other providers.
- DigiTalker monitors the validity period of its authentication certificate and renews the certificate in advance of expiry so that authentication of originated traffic is not interrupted.
- DigiTalker maintains its Service Provider account with the Policy Administrator and its account with its Certification Authority in good standing, including any subscription renewals necessary to preserve certificate issuance, renewal, and revocation capability.
- In the event of suspected compromise of the signing key, DigiTalker will request revocation of the affected certificate through its Certification Authority and will obtain a replacement certificate and key before resuming authentication.

3.5 Certification and Filing

DigiTalker will file a revised certification in the FCC Robocall Mitigation Database reflecting this implementation within ten (10) business days of the date on which authentication of originated traffic commenced, and will file a further revision upon any material change to its authentication status.

4. Know Your Customer (KYC) Procedures

DigiTalker applies due-diligence procedures before activating any customer and will not transmit traffic for a customer until onboarding verification is complete. The depth of verification reflects the customer type.

4.1 Customer Categories

DigiTalker's customers consist primarily of foreign call centers and foreign businesses that place their own outbound calls to United States numbers using DigiTalker's origination service. These customers are the calling parties: they connect directly to DigiTalker's softswitch as end customers, and DigiTalker, as the originating voice service provider, places their United States-bound calls onto the public switched telephone network. These customers are not themselves voice service providers or intermediate providers, and DigiTalker does not accept call traffic handed off to it by any foreign carrier or foreign provider. DigiTalker's customers may also include United States-registered resellers of its origination service that hold their own FCC Form 499 Filer IDs; in each such case DigiTalker remains the provider that originates the underlying calls onto the network.

4.2 Verification of United States-Registered Carrier / Reseller Customers

For customers that are United States-registered providers, DigiTalker collects and verifies, prior to activation:

- Legal name and FCC Registration Number (FRN).
- FCC Form 499 Filer ID, verified against the public USAC filer database.
- The customer's listing and status in the FCC Robocall Mitigation Database.
- An executed Master Service Agreement containing the provisions described in Section 4.4.

4.3 Verification of Foreign Customers

The foreign call center and foreign business customers described in Section 4.1 are DigiTalker's direct origination customers, being the calling parties whose United States-bound calls DigiTalker originates onto the network. Precisely because DigiTalker originates these calls rather than receiving them from another provider, rigorous identity, address, and use-case verification of these customers is central to its robocall mitigation program. For these customers, DigiTalker collects and verifies, prior to activation:

- The customer's business registration certificate, trade license, or equivalent government-issued evidence of legal incorporation in its country of operation.

- Government-issued identification of the customer's beneficial owner(s) or authorized signatory.
- A verifiable physical business address (not a post-office box, virtual office, or mail-forwarding address).
- A written description of the customer's intended use case, including the nature of the calls, target audience, and projected call volume.
- The IP address(es) from which the customer's traffic will originate, for IP-based authentication.
- An executed Master Service Agreement containing the provisions described in Section 4.4.

DigiTalker verifies the authenticity of submitted documentation through reasonable means, which may include cross-referencing government and corporate registries, conducting a video conference to confirm the customer's premises and personnel, and confirming that the contact details provided are active and consistent with the documentation.

4.4 Master Service Agreement Provisions

Every customer is required to execute a written Master Service Agreement before activation. The agreement includes, at a minimum:

- A prohibition on the origination of illegal robocalls and unlawful spoofed or fraudulent caller identification.
- A representation and certification of compliance with the Telephone Consumer Protection Act and all applicable United States telemarketing and consumer-protection laws.
- A requirement that the customer use only DIDs assigned and authorized by DigiTalker as caller identification, and a prohibition on inserting arbitrary or unauthorized calling numbers.
- The customer's consent to DigiTalker's monitoring of traffic patterns and, where applicable, call recording.
- DigiTalker's right to suspend or terminate service immediately upon credible indicia of illegal traffic.
- Customer indemnification of DigiTalker for liability arising from the customer's unlawful traffic.

4.5 Re-Verification

DigiTalker re-verifies customer information at least annually, and additionally whenever traffic monitoring or a traceback indicates a material change in the customer's calling behavior.

5. Know Your Upstream Provider (KYUP) Procedures

Before purchasing voice termination from, or sending traffic to, any upstream provider, DigiTalker verifies that the provider:

- Holds an active FCC Registration Number and, where applicable, an active FCC Form 499 Filer ID.
- Is currently listed in the FCC Robocall Mitigation Database with a current robocall mitigation certification.
- Holds the FCC authorizations appropriate to the services it provides, including international Section 214 authorization where applicable.
- Is not the subject of any active FCC cease-and-desist order, Notice of Apparent Liability, or removal from the Robocall Mitigation Database.

DigiTalker re-verifies the Robocall Mitigation Database status of its upstream providers on a periodic basis and will not accept traffic from, or send traffic to, any provider that is absent from or has been removed from the Database, consistent with 47 C.F.R. § 64.6305.

6. Call Analytics and Traffic Monitoring

DigiTalker monitors traffic traversing its softswitch through analysis of Call Detail Records (CDRs) and platform analytics. DigiTalker reviews traffic for patterns indicative of illegal robocalling, including but not limited to:

- Abnormally short average call durations (for example, a high proportion of sub-six-second calls), which may indicate automated dialing.

- Low answer-seizure ratios (ASR) inconsistent with legitimate calling.
- Sudden spikes in call volume materially exceeding a customer's established baseline.
- High call-attempt rates per second from a single customer.
- Disproportionate concentration of calls to a single area code, exchange, or destination.
- Calls to numbers on the FCC Do-Not-Originate (DNO) list or to invalid or unallocated numbering ranges.
- Repeated calls to the same destination number consistent with abusive dialing.

Traffic patterns that meet or exceed DigiTalker's internal thresholds generate alerts to the personnel responsible for monitoring, who investigate the flagged traffic and take appropriate action, up to and including suspension of the responsible customer. DigiTalker calibrates and updates its thresholds as operational experience develops.

7. Termination and Suspension Triggers

DigiTalker will suspend or terminate a customer's service upon the occurrence of any of the following:

- Confirmation, through a traceback or other credible evidence, that the customer has originated illegal robocall traffic.
- A pattern of tracebacks attributable to the customer within a short period.
- Traffic-monitoring metrics demonstrating dialer abuse or other behavior consistent with illegal calling.
- Notification from the FCC, the Industry Traceback Group, a state Attorney General, or law enforcement that the customer's traffic is unlawful.
- The customer's failure to complete required know-your-customer re-verification.
- Origination of calls using unauthorized caller identification or calls to numbers on the FCC Do-Not-Originate list.
- Material breach of the Master Service Agreement.

Where circumstances permit and consumer protection is not compromised, DigiTalker may provide the customer with notice and a brief opportunity to cure before suspension; however, DigiTalker reserves the right to suspend service immediately, without prior notice, upon credible indicia of illegal traffic. All suspension and termination decisions are documented with the supporting rationale.

8. Industry Traceback Group (ITG) Response

DigiTalker is committed to responding fully and substantively to all traceback requests received from the registered consortium (the USTelecom Industry Traceback Group, or "ITG") within twenty-four (24) hours of receipt, and to cooperating with the FCC, law enforcement, and other authorities investigating illegal traffic, consistent with 47 C.F.R. § 64.1200(n).

8.1 Designated Traceback Contacts

- Primary: Hussain Dawood Chanchwelia, Director. Email: contact@digitalker.uk; +1 917-730-4364.
- The traceback inbox (contact@digitalker.uk) is monitored on an ongoing basis. DigiTalker maintains personnel coverage sufficient to acknowledge and respond to tracebacks within the required twenty-four-hour window, including across the time zones in which its personnel operate.

8.2 Traceback Investigation Process

Upon receipt of a traceback request, DigiTalker follows this process:

- Acknowledge receipt of the traceback request promptly upon receipt.
- Query the Call Detail Records on the softswitch to locate the identified call by calling and called number, date, and time.

- Identify the customer that originated the call to DigiTalker, and the immediate upstream provider to which DigiTalker delivered the call for termination, as applicable.
- Where the call was signed by DigiTalker, identify the attestation level applied and the basis on which it was applied.
- Investigate the originating customer, including review of the customer's KYC file and recent traffic patterns.
- Provide a substantive response to the ITG identifying the source of the traffic within twenty-four hours.
- Where illegal traffic is confirmed, take enforcement action against the responsible customer in accordance with Section 7, and document the action taken.

9. Caller Identification and DID Authorization

DigiTalker procures DIDs from third-party DID providers for use as caller identification on outbound traffic. DigiTalker controls the assignment of DIDs to customers and does not permit customers to insert arbitrary or unauthorized caller identification. Before any DID is used as caller identification on a customer's outbound traffic:

- DigiTalker assigns the DID to the specific customer account and maintains a record matching each DID to the customer authorized to use it.
- DigiTalker permits customers to transmit only DIDs drawn from the pool authorized to that customer; calls presenting caller identification outside the authorized set are blocked or rejected.
- DigiTalker retains documentation of each customer's authorization to use the assigned DIDs.

DigiTalker maintains these records so that, in response to a traceback or investigation, it can identify the customer associated with any caller identification number used on its network. DigiTalker also honors the FCC Do-Not-Originate list and will block or decline to originate calls it identifies as illegal, or that are identified as illegal by the FCC or the ITG.

The records described in this Section 9 are also the basis on which DigiTalker determines the attestation level applied to a call under Section 3.3. DigiTalker applies Attestation A only where its records establish that the calling number presented is a DID assigned to, and authorized for use by, the customer originating the call. Where that authorization cannot be established for a given call, DigiTalker applies a lower attestation level rather than signing the call at Attestation A.

10. Recordkeeping

DigiTalker maintains the records necessary to support its robocall mitigation program and to respond to tracebacks and investigations, including:

- Call Detail Records for a minimum of twenty-four (24) months.
- Customer know-your-customer documentation for the duration of the customer relationship and for a period of at least twenty-four months thereafter.
- Records matching DIDs to authorized customers.
- Records sufficient to identify the attestation level applied to calls DigiTalker originated and signed.
- Records of tracebacks received, investigations conducted, and responses provided.
- Records of suspension and termination actions and their supporting rationale.

These records are made available to the FCC, the Industry Traceback Group, and law enforcement upon appropriate request.

11. Enforcement History

DigiTalker LLC has no history of FCC enforcement action, Notice of Apparent Liability, or cease-and-desist order. DigiTalker has not been removed from the Robocall Mitigation Database, and is not and has not been the subject of

any state Attorney General investigation, Federal Trade Commission action, or civil action arising from telecommunications fraud or illegal robocalling. To the knowledge of its Compliance Officer, no principal of DigiTalker has been the subject of such an action in connection with any related business.

12. Plan Maintenance and Certification

This Robocall Mitigation Plan is reviewed at least annually and updated as DigiTalker's operations, traffic profile, and regulatory obligations evolve, including upon any material change in the Company's STIR/SHAKEN implementation status or provider classification. The current version of this Plan is filed in the FCC Robocall Mitigation Database and is available upon request to the FCC, the USTelecom Industry Traceback Group, law enforcement, and state regulatory authorities.

DigiTalker certifies that the information contained in this Plan is true and accurate to the best of its knowledge and that the Company has implemented, and will maintain, the caller identification authentication and robocall mitigation practices described herein.

Certified by:

Hussain Dawood Chanchwelia
Director and Compliance Officer, DigiTalker LLC
Date: August 3, 2026