

Robocall Mitigation Statement

TNS-TransLine, LLC is committed to detecting, avoiding, and blocking illegal robocall traffic. We follow industry best practices to enable our efforts. TNS-TransLine is a non-gateway intermediate provider and hence our customers do not originate traffic on the TNS-TransLine network. All of TNS-TransLine's traffic is originated on other networks and is transited to TNS-TransLine already signed and "Attested". TNS-TransLine passes the Attestation level and any authenticated caller identification information that is sent by the originating carrier.

TNS-TransLine uses a multi-faceted approach in our mitigation strategy. This includes:

1. We know our upstream customers' businesses and monitor them closely:
 - a. Sanctions Screening: We screen all customers against lists of sanctioned parties issued by governments and international organizations. This ensures TNS-TransLine does not engage in business with prohibited or high-risk entities.
 - b. Know Your Customer (KYC) Data Collection: We collect each customer's legal name, address, and contact information to verify that the corporate entity and business purpose is legitimate and verify that the customer has reasonable safeguards in place to prevent illegal robocall and fraud traffic.
 - c. Contractual Provisions: TNS-TransLine's contracts include language requiring upstream customers to commit to not using TNS-TransLine's services for any improper or unlawful purpose and to being in full compliance with all regulations and laws set forth by the FCC. These contracts also reserve the right for TNS-TransLine to block routes and suspend service when it detects illegal, fraudulent, or abusive use of its services.
2. STIR/SHAKEN
 - a. Our voice solution allows STIR/SHAKEN signed messages and authenticated caller identification information to be passed from traffic originators to traffic termination companies. We have completed the STIR/SHAKEN testing process and validated that all information is being passed correctly.
 - b. We partner with vendors that have implemented STIR/SHAKEN in their networks.
3. Traceback/USTelecom
 - a. We commit to participate in the Traceback community and will respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium. We will cooperate with such entities in investigating and stopping any illegal robocallers that use our service.
4. Audit and monitoring
 - a. We apply Do-Not-Originate (DNO) blocking on all originated and terminated calls. We use the Transaction Network Services, Inc. (TNS) DNO list and certify that it is compliant with the FCC requirements for DNO blocking.
 - b. We have implemented analytics across multiple platforms and monitor traffic statistics and metrics to detect and block unlawful call activity. TNS-TransLine uses TNS' analytics solution.
 - c. We are committed to investigating any notifications of illegal robocall activity and will diligently work directly with customers to improve their behavior or remove them from our network if their call patterns do not improve.

At TNS-TransLine, we take robocall mitigation seriously. We believe our current practices are consistent with best in class practices; however, we continuously look for new approaches to detect and eliminate illegal robocalls.

Sincerely,

Joe Dechant

Joe Dechant
Vice President, Network Transformation
TNS-TransLine, LLC