

Full STIR/SHAKEN Implementation

As per the requirements and guidelines set forth by the FCC, Telxio Networks Inc has implemented full STIR/SHAKEN authentication frameworks across its network as required. Telxio Networks, Inc will attest calls across its network as per the criteria set forth by the FCC below:

A-Level Attestation (Full): A trusted customer/subscriber on the Telxio Networks, Inc network that has the right to use this number. All numbers provided by Telxio Networks, Inc to a trusted subscriber will be signed with an A-Level Attestation token. If the trusted customer/subscriber has numbers from other VSP's that will route through the Telxio Networks, Inc network these calls will be signed with a "B" token. If the trusted customer/subscriber provides and signs Telxio Networks, Inc's "Know Your Customer Form" and Telxio Networks, Inc's "STIR/SHAKEN LOA" indicating the customer's intent and certification that they are authorized to certify and attest to these numbers, then Telxio Networks, Inc will sign these calls with an "A" token.

B-Level Attestation (Partial): A trusted customer/subscriber on the Telxio Networks, Inc network using a number not provided by Telxio Networks, Inc or certified by the customer/subscriber.

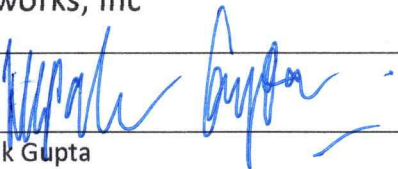
C-Level Attestation (Gateway): In the event that Telxio Networks, Inc establishes an international gateway, or for all other instances when Telxio Networks, Inc can only verify that the call is coming from a known gateway but can't authenticate the call source, Telxio Networks, Inc will sign these calls with a "C" token.

Where Telxio Networks, Inc acts as an intermediate carrier call will be passed with the attestation token as received. Telxio Networks, Inc will not modify the attestation on calls where Telxio Networks, Inc acts as an intermediate carrier.

Telxio Networks Inc complies with efforts to trace back the source of suspected robocalls.

- We actively participate and cooperate with traceback requests received directly from carriers, industry associations, and law enforcement.
- Call detail records (CDRs) are created for all calls and stored in a searchable database, and include all metadata including the ANI, DNIS, originating ip address, timestamps etc. and stored for a minimum of 1 year.
- We have devised analytical tools to capture and analyze call information in real time, including originating number information. The current practice is to immediately warn customers originating suspicious traffic and suspend services to those customers who continue with this.
- Only numbers actually in use by customers are authorized via our switches. Numbers customers use as caller ids are verified by our compliance team, by calling in to these numbers or requesting and collecting number ownership documentation. We ensure that these numbers are actually being used by customers.
- We require signed contracts by authorized representative of the customer. A full-fledged KYC process is in place, that includes Government issued ids for companies and authorised representatives. Service delivery to customers is completed only post KYC verification by the Compliance team.

- We educate customers regarding calling practices and FCC regulations and draw their attention to our Terms of Service. Acceptance of our Terms of Service is mandatory.
- We have a single point of contact for Compliance, the head of this team have over 6 years of experience in managing customers, carrier escalations and compliance.

Telxio Networks, Inc
Signature: 
Name: Deepak Gupta
Designation: President