

Summit Telecom, LLC

Summit Telecom is taking the following actions to mitigate its clients with engaging into Robocalls or Spam Text messages.

Step 1: Confirm Summit Telecom clients are registered with the Robo Call Mitigation database and proof of Stir/Shaken Certificates.

Step 2: Confirm and document enterprise practices to combat robocalls (ie. Listening in on outbound calls, verifying Caller ID, Opt-in and Opt-out policies). Document finding in Step 3 below.

Step 3: Enterprise Identity / User Authentication

Require clients to create a digital Identity (via TNID) and build a Chain of Custody via Blockchain. This identity must include the KYC information as well as use case, opt-in/opt-out, Caller ID/CNAM and the telephone numbers associated with each use case for outbound calling.

The chain of custody will be able to easily see the chain of participants from the number administrator down to the enterprise. Carriers and others can dip into TNID via API to verify attestation of end customer and gain a Reputation Score.

The reputation score is based upon several factors (1) customer – carrier relationship, (2) years in business, (3) TCPA violations, (4) Traceback instances, etc.

The digital Identity is attested and vetted by a one-degree relationship up and down, with the option to incorporate an enhanced Identity background check via a 3rd party.

Step 4: Continue to work with interested parties to solve RoboCall and Spam text messages via building a community of interested parties: Fraud organizations (ie CFAC, RAG), USTelecom, AI robocall solutions, carriers, service providers, FTC and FCC. The participants of TNID share data which allows a source of truth that carriers, service providers, enterprises and other interested parties can dip into for free.