



1095 Broken Sound Pkwy, Ste 201
Boca Raton FL 33487
888.864.2317
www.4voice.net

4Voice Robocall Mitigation Program

As part of the FCC's Robocall mitigation efforts, this document describes specific steps 4Voice takes to detect and prevent Robocall traffic sent via 4Voice systems.

1) Customer Due Diligence

4Voice's new customer activation process includes a detailed discovery step to ensure 4Voice understands the customer's business, their expected traffic volume and the type of voice traffic expected (volume, inbound/outbound mix, use of software tools for calling etc.).

4Voice specifically excludes all types of robocall traffic in service agreements for both existing and new customers.

4Voice places parallel call limits, maximum call limits and other thresholds to ensure that even compromised endpoints are not able to abuse the system to engage in any type of robocall behavior.

4Voice monitors customer traffic for unusual patterns and activity to detect potential compromise of their systems as a vector for unauthorized or malicious traffic.

2) Traffic Control

4Voice does not accept 'transit' traffic from other carriers – all traffic is originated by end-users, which are individuals or small/medium sized businesses based in the United States.

4Voice does not accept traffic from International carriers for transit.

4Voice ensures all termination traffic travels via carriers that provide STIR/SHAKEN attestation for calls originating on the 4Voice network.

3) Traffic Tracing

4Voice is committed to assisting the FCC, our up-stream carriers and other authorities with all traceback requests for potential robocall traffic.

4Voice maintains call-records and connection logs for all traffic passing through the network to facilitate timely responses.

4Voice also assists it's own customers in tracing third-party entities who may be spoofing numbers, by contacting relevant carriers with call information when such activity occurs.