

Robocall Mitigation Plan

Revised 12/26/2024

Client-Server Technology Group, Inc (hereinafter "CSTG"), a provider of voice services as defined in 47 CFR 64.1600(r), certifies that all of the calls that originate on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(a).

The specific reasonable steps CSTG has taken to avoid originating, carrying, or processing illegal robocall traffic as part of its robocall mitigation program are:

1. Providing voice services to only small business retail end-users
2. Restricting connections to the voice network to authenticated users or devices
3. Restricting Caller ID to properly ported-in numbers
4. Connecting calls only to an upstream provider, Bandwidth Inc., that uses call traffic pattern detection – including voice network traffic anomalies, cost anomalies, and geographic traffic abnormalities – and proactive restriction for fraudulent activity. The upstream provider also uses detection and blocking of the following ANIs: unallocated numbers, invalid numbers, invalid digits, and invalid alpha-numerics. CSTG uses no other third-party analytics vendors.

CSTG complies with its obligation to know its customers pursuant to 47 CFR 64.1200(n)(4) by following the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group. (<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>)

CSTG uses only one upstream provider, Bandwidth Inc., a pioneer in stopping telecommunications fraud that “actively participates in industry organizations and industry efforts to stop illegal robocalling.” Bandwidth Inc. is a member of NANC, STIR/SHAKEN working groups, and the Communications Fraud Control Association.

CSTG commits to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.