

Robocall Mitigation Plan

The following policies apply to all customers and/or prospective customers of Diamond Voice LLC and comprise our Robocall Mitigation Plan to avoid originating illegal robocall traffic from our network:

CONTRACT REQUIREMENT:

Our agreements clearly prohibit passing illegal robocalls through any of our switches or networks and define precise requirements for ASR, LCD and other traffic statistics. Customers who violate these rules are subject to immediate termination without notification. If COMPUTER TECHNOLOGY SOLUTIONS, INC. believes illegal traffic has been passed through its network, the customer sending such traffic forfeits confidentiality and all data will be shared with industry partners and law enforcement as required by regulatory bodies.

Know Your Customer

We follow 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>)

All customers are required to disclose certain information about their business such as physical location, contact personnel, state/country of incorporation or business formation, federal tax I.D. or non-USA government I.D. They must also disclose the practices and nature of their business. We endeavor to know the precise type of traffic which originates from each customer's switch including the type of customers they acquire and exact type of services they provide. COMPUTER TECHNOLOGY SERVICES, INC. investigates each Customer's claims to verify accuracy before accepting them as a customer.

Traceback

COMPUTER TECHNOLOGY SOLUTIONS, INC. monitors its system diligently and will investigate any suspicious traffic. We act promptly when we detect traffic which appears to be robocall activity to ensure it has been pre-authorized as "legal" (i.e. authorized political, non-profit, reverse 911 or fully-opted-in traffic). In the event COMPUTER TECHNOLOGY SOLUTIONS, INC. receives a Traceback request for an illegal robocall, we act on it immediately, request a specific and detailed explanation from our customer(s) and insist on immediate corrective action. We timely respond to all Traceback request from authorities. If corrective action is not timely provided by our customer, COMPUTER TECHNOLOGY SOLUTIONS, INC. takes whatever action is necessary to prevent recurrence of the event(s).

PUBLICATION AND NOTIFICATION:

COMPUTER TECHNOLOGY SOLUTIONS, INC. publishes in the public section of its website this Robocall Mitigation Plan and further pro-actively notifies all customers of such policy along with keeping a record of such notifications.

STIR/SHAKEN Extensions

COMPUTER TECHNOLOGY SOLUTIONS, INC. has implemented STIR/SHAKEN on our network with a trusted provider on our network.

All the voice traffic that originates on our network is subject to the robocall mitigation program described below.

Robocall Mitigation Program

We use software provided by TransNexus to monitor our outbound voice traffic in real time to prevent the origination of illegal robocalls. The software provides detailed reporting identifying suspected illegal robocalls and alerts us if we originate any calls where the calling number is invalid, unallocated, on a Do Not Originate list, in the FCC consumer complaint database or has a poor reputation. We immediately investigate any identified calls to determine if the caller was attempting to originate unlawful robocalls. If we determine that the caller was attempting to originate unlawful robocalls, then we either warn them to stop or terminate their service as appropriate.