

CDE LIGHTBAND ROBOCALL MITIGATION PROGRAM

CDE LIGHTBAND (CDE) does not have an obligation to implement STIR/SHAKEN because it lacks the facilities necessary to implement STIR/SHAKEN and does not meet the qualifications to obtain a SPC token. The reasons listed are consistent with 47 CFR § 64.6304. CDE does not have an OCN assigned and does not have numbering assigned nor a network for routing traffic.

CDE has contracted with Momentum Telecom to provide numbering for assignment to CDE customers and to provide all call routing and caller identification authentication for CDE customers.

Momentum Telecom has registered with the Policy Administrator and is an authorized service provider in the STIR|SHAKEN ecosystem. Momentum Telecom has fully implemented STIR/SHAKEN within its network and signs the originating calls on behalf of CDE customers routing on Momentum's IP network.

Robocall Mitigation Program

All voice traffic that CDE customers originate on Momentum Telecom's network is subject to the following Robocall Mitigation Program.

Call Analytics

Momentum Telecom provides call analytics for CDE. Momentum has implemented its own call analytics to identify unlawful traffic originated by the end users of its wholesale customers' services. Momentum's call analytics can detect call patterns that indicate robocall activity, including, but not necessarily limited to, an unusually large number of calls from the same number, an excessive number of short duration calls, and calls that stop attempting to connect after a single ring. Momentum's call analytics also can detect where the calling number is invalid, unallocated, or on ITG's Do Not Originate ("DNO") list. If Momentum's call analytics detect any of the above-described issues, an internal report is generated that summarizes the issues presented and the applicable wholesale customer that is responsible for the underlying calls.

In the event Momentum's analytics report indicates potential illegal robocall activity by a CDE end user customer, Momentum alerts CDE and asks CDE to investigate the issue and inform Momentum: (i) when the issue is resolved and (ii) what actions the wholesale customer took in resolving the issue.

CDE will work internally to identify the party that is potentially originating illegal robocalls and take appropriate action.

If it is determined a CDE customer is originating illegal robocalls, CDE will either warn the customer to stop such practices or terminate their service.

Know your Customer

CDE has procedures in place to prevent new & renewing customers from using our network to originate illegal robocalls. CDE thoroughly vets new residential and business customers by asking personally identifiable questions for additional security on each account before activating new service or making changes to existing services.

Residential customers are asked to provide their full name, address (physical and mailing, if different), phone number, email, and establish a security question, and a password.

Business customers are asked to provide their full name, address (physical and mailing, if different), tax identification number, phone number, email, and establish a security question, and a password.

CDE also requires a photo ID for all new customers requesting voice service.

Upstream Provider Knowledge

CDE knows all the carriers from which it receives traffic and has confirmed that the carriers are listed in the Robocall Mitigation Database. CDE has reviewed the providers' robocall mitigation policies and procedures related to identifying and blocking unlawful robocall traffic.

Traceback

CDE commits to cooperating with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that we learn are using our service to originate calls. CDE commits to responding to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, within twenty-four (24) hours.