



Carrier Connect RoboCall Mitigation Steps 022224

Carrier Connect Corp (CCC) is an intermediate carrier interconnecting to our customers and vendors via the public internet. CCC does not originate long distance or local traffic with retail customers. Recognizing the responsibility to mitigate robocalling, the company has adopted several methodologies to assist in its efforts to thwart illegal robocalls traversing its network.

1. Know Your Customer:

- A. We require a “know your customer” document to be executed under penalty of perjury on an annual basis by all customers.
- B. All customers are contractually obligated to take their own steps to mitigate robocall traffic by language requiring that CCC will not accept such traffic.
- C. We have a long-standing relationship with all of our customers dating back over a period of a full year and we know the type of traffic they have on their networks. As a result we tailor our mitigation to each customer based on these factors.

2. Measures to stop illegal robocalls:

- A. We analyze our traffic for illegal robocalling patterns on a real time and post mortem basis. We use a proprietary traffic monitoring software that incorporates AI to constantly analyze traffic patterns typical of robocalling.

-
- B. We use both automated and manual blocking to remove and stop any possible illegal robocalls detected from being sent downstream in our network.
 - C. We monitor stir/shaken tokens from upstream calls to block tokens meeting robocalling parameters from traversing our network.
 - D. We return a 603 “denied” reject codes to customers for any suspected robocalls to avoid advancing the call to go to another network.
 - E. We use several lists of bad originating ANIS and block any calls from these ANIS from using our network.
3. Call Analytic systems used:
- A. Proprietary list of suspected ANIS provided by 46Labs, Nexpath, Comcast, Bandwidth
 - B. Real time call analytics for short duration ANIS provided by Nexpath and 46Labs
 - C. DNO lists provided by ATL.