

Monday, September 27, 2021

Sysnet Communications Robocall Mitigation system and procedures

As part of Sysnet Communications submission to the Robocall Mitigation Database, this document describes the specific reasonable steps Sysnet has taken to avoid originating illegal robocall traffic as part of its robocall mitigation program. Sysnet is committed to respond fully and in timely manner to all traceback request from the commission, law enforcement and industry traceback consortium and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

Entities covered by this certification are:

Sysnet Communications Inc and Ark Telecom Inc.

Below is a list of rules, procedures and system that has put in place in order for Robocall Mitigation according to STIR/SHAKEN implementation requirement:

- 1- All our outbound voice traffic are generated by our customer connected to our network via Virtual Private Network (VPN) tunnels or are identified directly using their public static IP addresses. Assuring all traffic originated from our network are traceable to individual users and user location.
- 2- All customers are SMB users and at the present time we do not have any other service provider transiting traffic via our network. Each call is easily traceable to the originator.
- 3- In our network all users are double authenticated.
 - a. Authentication is done via VPN security key using IPSEC transmission and/or Public static IP assigned to customer
 - b. Additionally each VOIP SIP session are authenticated via SIP user authentication and registration.
- 4- All Call records are stored in secure backend databases in real-time for reporting and traceback should it be necessary and required by law enforcement, the Commission or other legal authorities.
- 5- All our network is protected by state of the art network security products from the network edge.
- 6- Our 24/7 network monitoring system will identity any unusual voice/data traffic pattern for investigation purposes and intruder detection.

These rules and procedures guaranty that our network is fully conforming to robo/call mitigation requirement as required by 47 CFR & 64.6301(a).

Sysnet is committed to responding fully and in a timely manner to all traceback request from the commission, law enforcement, and the industry traceback consortium, and to cooperating with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

Regards

Majid Matinrazm

CEO

Sysnet Communications Inc.