

ROBOCALL MITIGATION PLAN

Beacon Telecom, Inc. (“Beacon Telecom” or the “Company”), with its principal place of business being located at 80 Cedar Street, Canton, Massachusetts 02021, has adopted this Robocall Mitigation Plan (“RMP”) to outline the affirmative steps the Company has taken in preventing and mitigating the origination, carrying or the processing of illegal robocall traffic.

Know Your Customer

Beacon Telecom has policy and procedure in place to prevent new and renewing customers from using the network to originate, carry or process illegal robocalls including the following measures:

- a. Vetting of new customers must include a credit application and undergo an approval process. Information collected in this initial application must include the end customer physical address, contact person(s) information, relevant trusted industry references, federal tax ID, state of incorporation, and nature of the customers business.*
- b. Renewing customers must have (a) an account in good standing, (b) verify that all information in their profile is up to date and accurate.*
- c. Both New and Renewing customers are assigned a dedicated and trained Account Manager to process and verify customer information is complete and accurate (LOA, Form-A, CSR, contact information, etc.), document business requirements, including service areas, consumer trends, seasonality, and growth forecast.*

Through the above stated measures of getting to Know-the-Customer, we are able to accurately limit trunks based on customer’s required call capacity, and review usage patterns and consumption to identify potentially illegal calling activity.

Regular Monitoring and Audits

As a reseller, Beacon Telecom leverages various monitoring mechanisms from its provider to identify suspicious use of calling numbers and suspicious traffic.

All voice traffic consumed by our clients is routinely monitored and analyzed via CDR records with originating and terminating TN information to ensure and verify legitimate call usage.

Beacon Telecom additionally leverages a Management and Monitoring Solution (EdgeView Service Control Center) to capture and analyze customer communication data in real-time, providing notifications of suspected fraudulent activity.

Traceback Requests

Beacon Telecom, Inc. commits to respond fully, within twenty-four (24) hours, to all traceback requests from the FCC, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers that use its service to originate, carry, or process illegal robocalls.

In the past twenty-four (24) months, Beacon Telecom has not received any traceback requests for any traffic originating from our network or customers.

STIR/SHAKEN

Beacon Telecom is a reseller of Intelpeer Cloud Communications (RMD0004630). As a reseller, Beacon Telecom is not required to implement STIR/SHAKEN because it lacks control over the network infrastructure necessary to implement STIR/SHAKEN, as described in the following provision: *Call Authentication Trust Anchor, WC Docket No. 17-97, REPORT AND ORDER AND FURTHER NOTICE OF PROPOSED RULEMAKING, paragraph 40, March 2020.*

Call Blocking and Filtering

Beacon Telecom, Inc. reserves the right to refuse traffic from any party at any time where robocalling or use of originating numbers that are not valid or they are not authorized to use has occurred or is suspected. Beacon Telecom, Inc. is able to block the originating number(s), terminating number(s), trunk(s) or customer, including termination of customer relationship to prevent robocalling, invalid originating number or spoofed origination number transitioning the Company's networks.