

Robocall Mitigation Plan for Backhaul Network LLC

Backhaul Network has made meaningful investments to implement network upgrades and offer new features to combat illegal robocalls as part of its robocall mitigation program. Backhaul Network utilizes multiple processes to detect potential robocall activity based on statistics such as average call duration, Answer Seize Ratio (“ASR”), and call count carrier/consumer reports. As part of its robocall mitigation program, Backhaul Network provides the following solutions on its network to help minimize the impact of illegal or unwanted robocalls on customers:

Automatic Number Identification (“ANI”) Management: Utilized for customer traffic which is sent to Backhaul Network. ANI Management is used to identify and block originating telephone numbers that are deemed abusive based on repeat attempts to reach the Backhaul Network.

Proactive Blocking: Applied to all traffic. Backhaul Network blocks calls from phone numbers on Do Not Call (DNC) Reported Calls Data lists from FTC. Backhaul Network also blocks calls that originate from invalid, unallocated, or unused numbers.

Through reports generated by Call Detail Record (“CDR”) and pattern trends, fraud information sharing through industry organizations, and third-party notifications and complaints, Backhaul Network can identify potential unlawful robocalling.

Automatic Call Blocking System:

A. Do Not Originate. Backhaul Network, automatically blocks calls on the Do Not Originate (“DNO”) list for calls purporting to originate from a number to be blocked because the number is used for inbound calls only.

B. North American Numbering Plan (“NANP”) Conformance. Backhaul Network, employs a rigorous system to block any numbers that do not conform to the North American Numbering Plan, thereby preventing the use of non-compliant numbers.

C. YouMail Subscription. Backhaul Network utilizes service provider "YouMail" which tracks and analyzes the results of billions of live calls to millions of real consumers. YouMail technology allows Backhaul Network to help identify, intercept, and reject suspicious calls in real time.

III. Know Your Customer Program

Backhaul Network has established and implemented comprehensive Know Your Customer (“KYC”) policies for any new and existing customers. The objective of the KYC policy is to prevent Backhaul Network from being used, intentionally or unintentionally, for spoofed or illegal traffic. KYC procedures enable Backhaul Network to know and understand its customers and their use policy better, which in turn helps Backhaul Network manage unacceptable traffic.

STIR/SHAKEN Implementation:

Backhaul Network, has fully implemented STIR/SHAKEN on its network ensuring the authenticity and integrity of call signatures. All voice traffic that is originated on Backhaul Network, network is signed using the STIR/SHAKEN framework to establish the legitimacy of calls. Backhaul Network, verifies the validity of call signatures for calls received from upstream voice service providers. Each call signature is checked and validated. Invalid signatures are promptly identified and blocked, preventing the propagation of calls with fraudulent intent, incorrect or expired certificates. Backhaul Network, OCN is 752K and Peeringhub, Inc is the Certificate Authority.