Robocall Mitigation Plan

Introduction

Snapfon LLC (“Snapfon”) is a wireless service provider providing service directly to end users, including the ability to originate and terminate calls over SIP technologies. SNAPFON primarily serves residential users, providing wireless service to it’s customers. In addition to this primary field of operation, SNAPFON does not provide services for dialer applications.

Because SNAPFON primarily serves residential customers with fixed caller-ids and rate limited connections, it considers itself a low-medium risk of robocall abuse.

Technical Safeguards

SNAPFON implements a number of technical safeguards against abuse of it’s services by robocallers and other illegitimate traffic sources.

STIR/SHAKEN

SNAPFON’s network has fully implemented the STIR/SHAKEN caller-id authentication framework, and provides proper attestation across all of it’s outbound calls.

Caller-ID

Generally, SNAPFON provides DIDs to customers, and therefore, SNAPFON’s network does not allow user-supplied caller id data unless a specific agreement is in place with a customer governing caller id. In the event that such an agreement is executed, it will detail the all caller id values that the customer plans to use, which will be validated before they are allowed on the network. In the event that sent caller-id data does not match the permissible values for the customer's account, the call will be rejected, and the customer will be contacted to determine the source of the configuration issue.

Rate Limiting

SNAPFON customers are rate limited to a maximum of two concurrent calls, unless a written agreement is in place. Such an agreement will stipulate the maximum number of concurrent calls as a function of the number of active DIDs the customer has purchased, and the

expected conversational calling profile of an organization of a given size. Sudden, continuous saturation of outbound trunks will result in automatic suspension of the customer's outbound dialing priviliges until contact is made to ensure that the customer's systems haven't been compromised, and that the profile of their operations hasn't changed.

CDR Monitoring

SNAPFON will analyze the the CDRs of all customers on a weekly basis, and will analyzie several metric to ensure that their calling data matched the profile of operations that they indicated on their KYC forms, or that would be expected from a residential customer. SNAPFON will analyze the customer's number of caller attempts, ASR, ACD, call duration, and fraction of calls shorter than 60 seconds. Any customers found to have signs of automated dialing, significant deviations from past months, or high rates of unanswered calls will be immediately contacted for an explanation of their changed behavior. Any users who do not have an explanation for their changed behaviors within 72 hours will have their accounts suspended.

Additionally, SNAPFON monitors CDR data across accounts to detect sim boxing and account aggregation. If multiple accounts are being used from the same IP address or location and are placing a large number of calls, or have a calling pattern indicative of robocalling, they will be contacted for an explanation, and all affected accounts will suspended if an explanation is not received.

Policy Safeguards

SNAPFON conforms to a number of industry best practices and policies designed to mitigate the ability for robocallers to utilize it's network, and ensure their swift removal if they do gain access.

Contractual limitations

SNAPFON's customers contractually agree to not use the service for any high-volume outbound applications, as part of a dialer system, for telemarketing purposes, or to originate any type of robocall, legal or otherwise. Any customer found to be engaging in any of these activities will have their account terminated immediately.

Know your Customer policies

Every SNAPFON customer must provide a real physical address, full name, email address, and existing phone number before service will be provided. Business customers must additionally provide a business registration number, and must use an email domain

associated with their business. In all cases, SNAPFON will only accept payments using credit cards or bank transfers.

Know you Upstream Provider

SNAPFON only accepts calls from upstream providers which are regulated carriers, and will ensure that all upstream providers are listed in the FCC's Robocall Mitigation Database. In the event that any provider is removed, SNAPFON will immediately cease accepting calls from them.

Additionally, before entering into an agreement with any new carrier, SNAPFON will take steps to ensure that that carrier is legitimate, and is taking appropriate measures to protect their network against abuse.

Traceback

SNAPFON commits to promptly handling all traceback requests within 12 hours of when they are received. Any traceback results in an immediate detailed analysis of the initiating customer's CDRs for the past 30 days, followed by engagement with the customer to explain anomalies in the CDRs as well as the specific traceback example. If we do not receive satisfactory explanation within 72 hours, the customer is suspended. A customer that is the subject of three tracebacks in 90 days is permanently banned from our platform, unless the traceback examples are shown with certainty to be legal and compliant.