

Robocall Mitigation Plan

FRACTALVISION TECHNOLOGY SERVICES dba NEIGHBORNET is a small internet and voice service provider (VSP) dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network. The FCC requires that, by June 30, 2021, all VSPs certify in the Robocall Mitigation Database that they have (1) fully implemented STIR/SHAKEN across their entire network, (2) implemented STIR/SHAKEN on a portion of their network and that the remained of the calls are subject to a Robocall Mitigation Plan (RMP), or (3) have not implemented STIR/SHAKEN but subject all calls to an RMP to ensure that the network is not originating illegal robocalls.

The FCC requires that VSPs develop an RMP that:

- Lists the specific, reasonable steps the VSP has taken to avoid originating illegal robocall traffic

- States a commitment to respond fully and promptly to all traceback requests from the FCC, law enforcement, and the industry traceback consortium

- To cooperate with entities investigating and stopping any illegal robocallers that use its services to originate calls

FRACTALVISION TECHNOLOGY SERVICES dba NEIGHBORNET purchases origination, termination, and hosted-switch access from Atheral LLC (FRN 0028070290), which provides crucial elements of our RMP as part of their interconnected white-label VoIP wholesale services to FRACTALVISION TECHNOLOGY SERVICES.

Know Your Customer

We follow the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group.

International Subscribers

FRACTALVISION TECHNOLOGY SERVICES dba NEIGHBORNET does not sell origination or termination services to subscribers outside the United States.

Acceptable Use Policy

FRACTALVISION TECHNOLOGY SERVICES dba NEIGHBORNET maintains an Acceptable Use Policy ("AUP") that subscribers must sign before being permitted to use FRACTALVISION TECHNOLOGY SERVICES 's broadband or voice services. Among other things, this AUP prohibits:

Illegal use. Using the Services to transmit any material (by e-mail, uploading, posting, or otherwise) that, intentionally or unintentionally, violates any applicable local, state, national or international law, or any rules or regulations promulgated thereunder.

Harm to minors. Using the Services to harm, or attempt to harm, minors in any way.

Threats. Using the Services to transmit any material (by e-mail, uploading, posting, or otherwise) that threatens or encourages bodily harm or damage to or destruction of property.

Harassment. Using the Services to transmit any material (by e-mail, uploading, posting, or otherwise) that harasses another person or entity.

Fraudulent activity. Using the Services to make fraudulent offers to sell or buy products, items, or services or to advance any type of financial scam such as pyramid schemes, Ponzi schemes, and chain letters.

Forgery or impersonation. Adding, removing, or modifying identifying network header information in an effort to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or forging other identifying information is prohibited. The use of anonymous remailers or nicknames does not constitute impersonation. Using deliberately misleading headers ("munging" headers) in news postings in order to avoid spam e-mail address collectors is allowed.

Unsolicited e-mail. Using the Services to transmit any unsolicited commercial e-mail or unsolicited bulk e-mail. Activities that have the effect of facilitating unsolicited commercial e-mail or unsolicited bulk e-mail whether or not that e-mail is commercial in nature.

Unauthorized access. Using the Services to access, or to attempt to access, the accounts of others, or to penetrate, or attempt to penetrate, security measures of NEIGHBORNET's or another entity's computer software or hardware, electronic communications system, or telecommunications system, whether or not the intrusion results in the corruption, theft, or loss of data.

Copyright or trademark infringement. Using the Services to transmit any material (by e-mail, uploading, posting, or otherwise) that infringes any copyright, trademark, patent, trade secret, or other proprietary right of any third party, including, but not limited to, the unauthorized copying of copyrighted material, the digitization and distribution of photographs from magazines, books, or other copyrighted sources, and the unauthorized transmittal of copyrighted software. NEIGHBORNET is registered under the Digital Millennium Copyright Act of 1998.

Collection of personal data. Using the Services to collect, or attempt to collect, personal information about third parties without their knowledge or consent.

Sharing or Reselling the services. Sharing or reselling the Services without NEIGHBORNET's authorization.

Network disruptions and unfriendly activity. Using the Services for any activity which adversely affects the ability of other people or systems to use NEIGHBORNET Services or the Internet. This includes "denial of service" (DoS) attacks against another network host or individual user. Interference with or disruption of other network users, network services or network equipment is prohibited. It is the User's responsibility to ensure that their network is configured in a secure manner. A User may not, through action or inaction, allow others to use their network for illegal or inappropriate actions. A User may not permit their network, through action or inaction, to be configured in such a way that gives a third party the capability to use their network in an illegal or inappropriate manner.

Online community. Users should use their best judgment when posting to any online community. Many groups have charters, published guidelines, FAQs, or "community standards" describing what is and is not considered appropriate. The continued posting of off-topic articles is usually prohibited. Commercial advertisements are off-topic in most online communities, especially regional groups not specifically named for such. The presence of such articles in a group is not indicative of the group's "intended" use. Please familiarize yourself with the community's etiquette before posting to that online community. Posting the same or similar message to one or more online communities (excessive cross-posting or multiple-posting, also known as spam) is explicitly prohibited. Users may not cancel messages other than their own messages. A User may cancel posts forged in that User's name.

Peer-to-Peer and file sharing. Users must not engage in the unauthorized copying, distributing, altering, maintaining or transmitting of copyrighted materials, information, software, music or other media.

Traceback Requests

FRACTALVISION TECHNOLOGY SERVICES is committed to responding promptly to all traceback requests from the Federal Communications Commission, law enforcement, state attorneys general, Atheral LLC, and the industry traceback consortium. Furthermore, FRACTALVISION TECHNOLOGY SERVICES is committed to cooperating with such entities in investigating and stopping any illegal robocallers that use FRACTALVISION TECHNOLOGY SERVICES service to originate calls. Subscribers are required to comply with traceback requests via our AUP. Traceback requests can be sent billing@neighbornet.co for immediate processing by FRACTALVISION TECHNOLOGY SERVICES.

Telephone Number Validation

If a subscriber wishes to use a telephone number (TN) as a caller identity and that TN is not directly managed by FRACTALVISION TECHNOLOGY SERVICES or our wholesale partner Atheral LLC, then TN validation is necessary by requiring the subscriber to provide a valid letter of authorization that they are

an authorized user of such TN. Should the subscriber provide sufficient documentation to FRACTALVISION TECHNOLOGY SERVICES of authorization to use a TN, documentation will be provided to Atheral LLC so that they can attest calls originated with these TNs.

Investigation of High-Volume Network Traffic, Suspicious Calls, and Calling Patterns

Our wholesale VoIP provider, Atheral LLC, uses TransNexus's ClearIP solution to monitor our origination voice traffic in real-time to prevent the origination of illegal robocalls. The software provides detailed reporting identifying suspected illegal robocalls and alerts Atheral LLC if we originate any calls where the calling number is invalid, unallocated, on a Do Not Originate list, in the FCC consumer complaint database, or has a poor reputation. Atheral will immediately ask FRACTALVISION TECHNOLOGY SERVICES to investigate any identified calls to determine if the caller was attempting to originate unlawful robocalls. If FRACTALVISION TECHNOLOGY SERVICES or Atheral LLC determines that the caller was attempting to originate unlawful robocalls, we either warn them to stop or terminate their service based on our AUP.

Examples of calling patterns monitored:

- Higher than expected cost generated by calls from a subscriber

- Targeted pumping of repeated calls to a specific called number within a 15-minute period

- Fast traffic pumping of repeated calls to a specific called geographic location within a 5-minute period

- Slow traffic pumping of repeated calls to a specific called geographic location within a 60-minute period

- Theft of service traffic pumping of repeated calls to a high-cost geographic location within a 60-minute period

- Recent call volumes (last 60 min) vs weekly trends

- Number of unique destination numbers in a 60-minute time frame

- Irregularities in Short Call Duration (SDC) and Average Call Duration (ACD) distribution

- Anomalies in Answer-Seizure Ratio (ASR)

- Robocalling triggers monitoring for a high volume of outbound calls or excessive incoming calls from the same calling number

- Wangiri trigger monitoring for origination calls to high termination rate destinations with short duration (to trigger end-users to call back) for all calls over a 5-minute duration

Analysis of recent and past Call Detail Records (CDRs) to benchmark against expected trends

STIR/SHAKEN Implementation Timeline

Atheral LLC has fully implemented STIR/SHAKEN as of June 30th, 2022.