



Robocall Mitigation Plan

Prepared By:

Daniel White – Co-Founder
April 29th, 2024

TABLE OF CONTENTS

<i>Introduction</i>	<i>3</i>
<i>Mitigation Plan</i>	<i>4</i>
Know Your Customer.....	4
Caller Identity Vetting and Telephone Number Authorization.....	4
Investigation of High-Volume Network Traffic, Suspicious Calls, and Calling Patterns	5
Examples of calling patterns monitored.....	5
Terms of Service.....	5
International Subscribers	6
Traceback.....	6
<i>STIR/SHAKEN Implementation Timeline</i>	<i>6</i>

INTRODUCTION

The North America Numbering Council (NANC) Call Authentication Trust Anchor Working Group introduction to *Best Practices for the Implementation of Call Authentication Frameworks*¹ states:

Fighting illegal robocalls is a top consumer protection priority for the Federal Communications Commission (FCC), and call authentication is an important part of solving this critical challenge. With the recent passage of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, Congress expressed its support for a robust call authentication system². As part of the TRACED Act, Congress directed the Commission to “issue best practices that providers of voice service may use as part of the implementation of effective call authentication frameworks...to take steps to ensure the calling party is accurately identified.”³

The FCC requires that, by June 30, 2021, all small voice service providers (VSPs) certify in the Robocall Mitigation Database that they have (1) fully implemented STIR/SHAKEN across its entire network, (2) implemented STIR/SHAKEN on a portion of its network and that the remainder 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.⁴

The FCC requires that VSPs develop an RMP that⁵:

- Lists the specific, reasonable steps the VSP has taken to avoid originating illegal robocall traffic
- States a commitment to respond fully and in a timely manner 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

¹ <https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>

² Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, S. 151, 116th Cong., at § 4(b)(l) (2019) (TRACED Act).

³ TRACED Act § 4(b)(7)

⁴ 47 CFR § 64.6305(b)

⁵ 47 CFR § 64.6305(b)(2)

MITIGATION PLAN

Know Your Customer

Athermal is a white-label interconnected VoIP provider primarily reselling services to Internet Service Providers (ISPs). The nature of this business can be classified as wholesale as we are selling services (origination, termination, hosted switch, etc.) to Resellers who, in turn, are selling those services to end-users. Athermal vets our wholesale relationships by:

- Comparing information filed with the FCC via Form 499 against information collected during the sales and onboarding process
- A one-hour introduction/sales/demonstration with a company executive to determine if Athermal is a good fit for the proposed business
- Industry research on the inquiring reseller, including membership to organizations like the Wireless Internet Service Provider Association (WISPA)⁶ or credit references provided on the signed Master Service Agreement
- Four hours of training with an engineering team member on Athermal's hosted softswitch solution

Caller Identity Vetting and Telephone Number Authorization

>99% of all traffic that originates from Athermal is via our softswitch or session border controllers (SBC). Resellers are prevented from utilizing Caller ID Telephone Numbers (TNs) that have not been directly assigned to them by Athermal from one of Athermal's underlying carriers for use by the end user. The fields in our switch that allow the selection of a TN for Caller ID purposes are restricted to a drop-down menu of available TNs for the Resellers end user or tenant. Telephone Number validation is the inherent result of Athermal's assignment of the TN to its subscriber. As an example, a screenshot from our softswitch is provided:



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

Atheral uses TransNexus's ClearIP⁷ 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 us 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. We immediately investigate any identified calls to determine if the caller was attempting to originate unlawful robocalls. If we determine that the caller was attempting to originate unlawful robocalls, then we either warn them to stop or terminate their service as based on our Terms of Service.

Examples of calling patterns monitored

- Higher than expected cost generated by calls from an end user or reseller
- 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 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

Terms of Service

Atheral has each reseller sign our Master Service Agreement (MSA) which requires each Reseller to agree to our Fair Use Policy (FUP), which states:

*Atheral maintains the right to immediately terminate any or all services to any Customer or End User who Atheral, at its sole determination, engages in, reasonably suspected to be involved in, or related to without limiting the generality of the preceding:*⁸

- *In a fraudulent, illegal, or criminal manner*
- *Providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call*
- *In a manner which causes or is likely to cause unreasonable congestion of Atheral's network including, but not limited to the use of automated dialing equipment, dialing sequential numbers and the dialing of telephone numbers that do not exist*

Should Atheral detect via our call monitoring of suspicious calls and calling patterns behavior that violates our Terms of Service, Atheral will contact the Reseller to understand the end-users particular use case and validate that the activity belongs to that end-user. If it does, and Atheral determines that a Reseller or its end-user has allowed robocall traffic to originate from our service subject to the Atheral FUP, the service is subject to immediate termination.

⁷ <https://transnexus.com/clearip/>

⁸ Atheral Master Service Agreement, Section 3.4

International Subscribers

Currently, Atheral does not permit its Resellers to sell Atheral services outside of the United States of America, her territories, or the District of Columbia. Accounts found to have been sold outside of the United States are subject to immediate termination by Atheral.

Traceback

Atheral is committed to responding in a complete and timely manner to all traceback requests from the Federal Communications Commission, law enforcement, state attorneys general, and the industry traceback consortium. Furthermore, Atheral is committed to cooperating with such entities to investigate and stop illegal robocallers that use Atheral service to originate calls. Resellers are required to comply with traceback requests via our Master Service Agreement. Traceback requests can be sent to robocall@atheral.com for immediate processing by the Atheral Network Operations team.

STIR/SHAKEN IMPLEMENTATION TIMELINE

As of July 1st, 2022, Atheral has been authenticating and verifying with STIR/SHAKEN voice traffic that originates and terminates on our network.