

HMA COMMUNICATIONS LLC

ROBOCALL MITIGATION PLAN

Introduction

HMA Communications LLC, Inc. submits this report in compliance with 47 C.F.R. § 64.6305, which details its implementation of the STIR/SHAKEN call authentication framework and outlines its strategies for preventing and reducing illegal robocalls. This document provides an overview of the current status of the STIR/SHAKEN implementation and the measures HMA Communications LLC, Inc. has put in place to address illegal robocalls as of November 14, 2024. Additionally, HMA Communications LLC, Inc. retains the right to modify, add, remove, or adjust any of the policies and procedures described in this plan at any time to respond to changes in its business environment, capabilities, and requirements.

Sir/Shaken Implementation

HMA Communications LLC has successfully integrated the STIR/SHAKEN authentication framework throughout the entirety of its IP network. All calls initiated by the company adhere to the requirements set forth in § 64.6301(a)(1) and (2). This adherence is a result of HMA Communications LLC's compliance with the STIR/SHAKEN standards within its IP network segments. The company prohibits its customers from engaging in CallerID spoofing, ensuring that any outgoing CallerID can be reliably traced back to the respective HMA Communications LLC customer. Furthermore, the company does not utilize any third-party call analytics providers.

Robocall mitigation plan (RMP)

This Robocall Mitigation Plan delineates the specific measures that the Company has established to identify and prevent unlawful robocalls on its network, effective November 14, 2024. The Company will perform regular evaluations of the risks it faces, the effectiveness of its policies and procedures, and its capacity to execute the strategies outlined in this document. HMA Communications LLC, Inc. operates as a voice service provider, delivering a variety of voice calling services. Its clientele generally does not generate a substantial volume of calls, and the Company has not detected any

indications of robocalls originating from its network. As a result, the Company does not consider its network to be at a considerable risk of producing illegal robocalls.

Know your customer

The Company requires potential carrier clients to complete a detailed Profile, including legal information, filers and exemptions, industry and financial references, and verification of registration with the Robocall Mitigation Database. Key requirements include: -

- A corporate email address (no personal emails like Gmail or Yahoo).
- A functional client website.
- Verification of the corporate street address.
- Payments via bank transfer (or credit card); PayPal and cryptocurrency are accepted.

If a client violates guidelines or alters registered information without resolution, the Company may suspend or terminate interconnection. Similar standards apply to vendors.

Traceback request

The Company commits to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls. If a traceback exposes an existing customer as the source of fraudulent robocalls, or as having transmitted fraudulent robocalls, a demand for an explanation and verification of mitigation of the traffic is issued to the customer. If the fraudulent traffic is not remediated, HMA Communications LLC initiates blocking of all traffic from the offending customer.

The Company's point of contact to handle traceback requests is:

Anuj Kumar

anuj@hmacommunications.com

Mail- admin@hmacommunications.com

ADD- 349 KINDERKAMACK ROAD WESTWOOD, NEW JERSEY 07675

EIN- 98-1818943

FRN- 0036273316

cont- 2018820180

499A- 837220