



ROBOCALL MITIGATION PLAN (RMP)

HIGHCODE GROUP FZCO, may be considered a voice service provider within the meaning of the TRACED Act and 47 C.F.R.

À 64.6300 of the rules of the Federal Communications Commission. In an abundance of caution, HIGHCODE submits this Robocall Mitigation Plan (RMP), which describes HIGHCODE's policies and procedures to prevent and

mitigate illegal robocalls using North American Numbering Plan (NANP) numbers that pertain to the United States. HIGHCODE reserves the right to modify, add, delete, or otherwise alter any of the policies and procedures

described in this filing at any time as it deems appropriate to reflect its business, its capabilities, and its needs.

HIGHCODE Introduction

HIGHCODE is an UAE enterprise which creates, maintains, and makes available for distribution, mobile telephony software. HIGHCODE applications are available for download from the iOS app stores. The applications provide a convenient and cost-effective solution for making and receiving mobile VOIP calls.

STIR/SHAKEN Implementation

Paragraph 40 of the FCC's First Call Authentication Report and Order (FCC 20-42) excludes providers that lack control over the network infrastructure necessary to implement STIR/SHAKEN from implementation obligations.¹ Because HIGHCODE, does not own or operate any infrastructure, networks, or facilities, it lacks control over the facilities and network infrastructure necessary to implement STIR/SHAKEN, and it is thus not required to implement STIR/SHAKEN pursuant to paragraph 40. Instead, HIGHCODE, relies on underlying carrier partners to implement and utilize STIR/SHAKEN. Based on the foregoing, HIGHCODE's role in the call chain would be as a voice service provider without a STIR/SHAKEN obligation, if it is considered a voice service provider under the TRACED Act and relevant FCC rules.

Robocall Mitigation Plan

HIGHCODE, (FRN 0037505609) has implemented a Robocall Mitigation Program, as required by Section 4(b)(5)(C) of the TRACED Act, and 47 C.F.R. À 64.6305, as documented below.

This Robocall Mitigation Plan describes the specific measures that HIGHCODE has implemented to mitigate and address the risk that it will originate illegal robocall traffic as of December 2024.

HIGHCODE will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described. Should it determine that changes are appropriate, its practices may differ from those described below.

Measures to Prevent or Avoid Exchanging Illegal Robocalls

- **Customer Due Diligence.** *HIGHCODE requires each customer to complete a detailed "Know Your Customer" questionnaire. Through this questionnaire and its sales order process, HIGHCODE collects customer information, including business name, the customer's service address, a customer employee contact, and billing information. Where necessary, HIGHCODE implements an even more detailed "Know Your Customer" process in response to our underlying carriers' call origination attestation requirements. Additionally, HIGHCODE requires all customers to*

agree to our Terms of Service and our Acceptable Use Policy, all of which restrict customers' use of the Services, including by prohibiting unlawful activities such as illegal robocalling.

- **Network Monitoring.** *In conjunction with its underlying carriers, HIGHCODE will monitor for fraudulent or suspicious traffic, including traffic that may be associated with illegal robocalling activity. In the event potential fraud is detected, HIGHCODE will take action to mitigate the potential fraud, including directing its underlying carriers to temporarily or permanently block traffic and undertaking efforts to identify the source of the traffic.*

- **Know-Your-Upstream Provider.** *As a customer care platform which sometimes relies on carrier partners to route incoming traffic to its customers, HIGHCODE takes steps to know its upstream carriers/providers. Specifically, HIGHCODE enters into Master Services Agreements with these carriers/providers which allow HIGHCODE to collect identifying information on*

2

them, including, inter alia, their names, addresses and contacts. These Master Services Agreements also contain binding provisions which prohibit unlawful activities such as engaging in or facilitating illegal robocalling.

- **Robocall Analytics and Blocking.** *HIGHCODE relies on its underlying carrier partners to adopt analytics software for monitoring call traffic and to block relevant calls. HIGHCODE*



itself does not use any call analytics systems to identify and block illegal traffic.

Additionally, HIGHCODE does not use any third-party analytics vendor(s) for analytics solutions.

To the best of HIGHCODE's knowledge, its underlying carriers identify and block calls from providers that have not filed in the Robocall Mitigation Database. Because such blocking is done at the network level, HIGHCODE does not have control over this.

Responding to Traceback Requests

- *HIGHCODE commits to responding, to the extent permitted under applicable law, to valid traceback requests from the Commission, law enforcement and the Industry Traceback Group (ITG) fully and within 24 hours.*

Cooperation with State and Federal Regulators

HIGHCODE will cooperate, to the extent permitted under applicable law, with valid requests from the Commission, or law enforcement to identify and stop any illegal robocallers that use HIGHCODE services to originate calls. Specifically, consistent with applicable law, HIGHCODE will:

- *Respond to valid law enforcement requests;*
- *Provide relevant non-proprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities; and*
- *Implement mandated robocall mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls.*

Robocall Mitigation Compliance Contact

Izzet Zakuto

CO-Founder and COO

support@nextlineapp.com