

Inatech Solutions Inc.

Robocall Mitigation Plan

470 Stoney Ridge Ct

Johns Creek, GA 30022

404-828-0474

CEO: Maulik Patel

Email: mgpatel@inatechsolutions.net

Introduction

This Robocall Mitigation Plan is submitted by Inatech Solutions Inc., pursuant to the provisions of 47 C.F.R. § 64.6305, adopted by the Federal Communications Commission (FCC), which require all “voice service providers” to establish a “robocall mitigation plan.” This document sets forth Inatech Solutions Inc.’s current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network. Inatech Solutions views these policies and procedures as constituting “reasonable steps” to avoid the origination of illegal robocalls on its network. In addition, the company commits to responding to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG), and to cooperate with such entities in investigating and stopping any illegal robocallers that may use its service to originate calls.

I. STIR/SHAKEN Implementation Status

Inatech Solutions has not implemented the STIR/SHAKEN authentication framework on any portion of its network and all calls originating on its network are subject to the policies and procedures set forth in this Robocall Mitigation Plan.

At present, the company relies on the continuing extension from STIR/SHAKEN implementation provided under 47 CFR § 64.6304(d), which exempts from STIR/SHAKEN Caller ID Authentication those portions of a voice service provider network that rely on technology that cannot initiate, maintain, carry, process, and terminate SIP.

II. Traceback Requests

Inatech Solutions will cooperate with the FCC, law enforcement, and the ITG on all traceback requests and investigations. The company dedicates sufficient resources to promptly complete and provide responses to all traceback requests, with full responses provided within 24 hours.

A single point of contact for traceback requests is designated in Appendix A. Inatech will also require traceback cooperation clauses in all carrier interconnection and service agreements.

III. Customer Vetting Practices

To prevent illegal robocalls, Inatech Solutions applies strict customer vetting, including collecting and validating customer identity details (physical location, incorporation status, tax ID, contact information, and nature of business).

Commercial and wholesale customers are reviewed more stringently, with possible

background checks or site visits. Service agreements and acceptable use policies explicitly prohibit illegal robocall activity and authorize immediate suspension or termination if violations are detected.

Inatech monitors call usage patterns to identify suspicious activity, with customer contact and investigation initiated within 24 hours if abuse is suspected.

IV. Telephone Number Validation Practices

Inatech ensures subscribers only use telephone numbers assigned or authorized by the company or its partners. For single-line subscribers, originating calls are restricted to assigned numbers. For multi-line systems, originating calls are screened to confirm they match assigned numbers, preventing spoofing.

V. International Call Originators

Inatech Solutions does not currently provide international origination services. Should it begin serving international customers, the company will adopt industry best practices for vetting and validating their use of numbering resources.

VI. Know Your Upstream Provider Procedures

Inatech maintains long-term relationships with a limited number of upstream providers. The company requires robocall prevention clauses in interconnection agreements and ensures providers share its commitment to monitoring networks and blocking illegal traffic. Appendix A includes upstream provider information.

VII. Ongoing Robocall Mitigation Practices

Inatech Solutions continuously monitors call traffic to detect and respond to unusual traffic spikes or bursts, short-duration calls or low completion rates, sequential number dialing patterns, calls to invalid or Do-Not-Call listed numbers, and calls to unassigned NPA-NXXs. Suspicious activity triggers investigation, traceback, number validation, and possible suspension of the customer's service. Law enforcement may be notified where applicable.

VIII. Third-Party Analytics

Inatech Solutions employs ClearlyIP's call analytics and fraud prevention tools to fulfill its Robocall Mitigation responsibilities. These include real-time SIP analytics, blacklisting/whitelisting, "Do Not Originate" list checks, reputation-based number validation, and monitoring anomalous calling patterns such as short-duration, burst traffic, sequential dialing, or spoofed numbers.

Appendix A

Traceback Request Single Point of Contact:

Name: Maulik Patel

Title: CEO

Phone Number: 404-828-0474

Email: mgpatel@inatechsolutions.net

Upstream Provider Information:

Name of Upstream Provider: ClearlyIP

Network Location of Upstream Provider (Headquarters): Appleton, Wisconsin

Name of Contact at ClearlyIP: Tony Lewis

Title: CEO

Phone Number: 920-383-3100

Email Address: tlewis@clearlyip.com

Call Analytics Vendor Information:

Name of Vendor: ClearlyIP

Description of System: Inatech Solutions employs ClearlyIP's call analytics and fraud prevention tools to fulfill its Robocall Mitigation responsibilities. The tools include:

- Real-time SIP analytics for detecting and resolving suspicious or fraudulent robocall activity.
- Blacklisting and whitelisting mechanisms to block high-risk traffic.
- "Do Not Originate" list checks and reputation-based telephone number validation.
- Monitoring for anomalous calling patterns such as short-duration or burst traffic, sequential dialing, or spoofed numbers.
- Automated safeguards preventing unauthorized use of assigned numbers.