

VIATALK ROBOCALL MITIGATION PLAN

Purpose and Table of Contents

ViaTalk's Robocall Mitigation Plan sets forth the actions ViaTalk takes to:

- I. SCREEN its customers prior to providing voice services ("Know-Your-Customer");
 - II. CONSTRICT existing customers for traffic to prevent transmission of fraudulent robocalls
 - III. MITIGATE the transport of fraudulent robocall traffic via ViaTalk.
-

I. SCREEN

ViaTalk undertakes the following Know-Your-Customer ("KYC") activities prior to providing voice services:

A. Information Collection. All ViaTalk customers must provide their names, addresses, verified e-mail address(es), verified phone number(s), validated payment information, and, if the customer is a legal entity, the state or country of formation, contact person, and company registration number.

B. Contractual Provisions. Customers must agree to ViaTalk's terms of service that prohibit fraudulent traffic. Additionally, the terms of service provide that ViaTalk may suspend or terminate services for violating ViaTalk's acceptable use provisions. Customers may also be held liable for any financial penalties imposed on ViaTalk for fraudulent traffic sent from the customer.

C. Know Your Upstream Provider.

1. Procurement Processes. ViaTalk has a robust procurement process that includes sanctions screening and collecting documentation and information about its upstream providers that includes, but is not limited to:

- a. Contact Person(s);
- b. State or country of incorporation; and,
- c. Federal tax identification number.

2. Contractual Terms. ViaTalk's contracts with upstream providers require that the provider comply with all relevant laws, including in many instances specific provisions prohibiting the transmission of fraudulent traffic and robocalls. ViaTalk's contracts also permit ViaTalk to

terminate the upstream provider's right to send traffic to ViaTalk if any contractual provision is violated.

II. **CONSTRUCT.**

A. **Traffic Limitations.** ViaTalk has concurrent call limits in place that prevent high volumes of calls from a single account.

III. **MITIGATE**

A. **Commitment to Respond to Traceback Requests.** ViaTalk commits to respond fully and within twenty-four (24) hours to traceback requests from law enforcement, the Federal Communications Commission, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocalls that use its services to originate such calls.

B. **Robocall Mitigation Database Filings.** ViaTalk checks the Robocall Mitigation Database and only accepts calls from the following categories of providers if those providers' filings appear in the Robocall Mitigation Database and that filing has not been de-listed pursuant to an enforcement action:

1. Domestic voice service providers;
2. Foreign voice service providers or foreign intermediate providers that use North American Numbering Plan resources that pertain to the United States in the caller ID field to send voice traffic to residential or business subscribers in the United States; and,
3. Gateway providers.

C. **Blocking/Discontinuance.** ViaTalk employs a variety of effective measures to block fraudulent calls. When ViaTalk identifies actual fraudulent traffic or traffic with a high likelihood of being fraudulent, its fraud team takes prompt action to block such traffic. In addition to blocking the offending traffic, ViaTalk may suspend or terminate the offending customer's service.

D. **Selective Call Blocking.** Certain ViaTalk products have selective call blocking that rejects or sends to voicemail incoming calls based on their risk profile determined by STIR/SHAKEN validation status and Telephone Number (TN) validation.

This Robocall Mitigation Plan describes the specific measures that ViaTalk has implemented as of December 11, 2024. ViaTalk continually evaluates the efficacy of its measures to combat bad actors and takes appropriate steps to improve these measures when needed.