

ROBOCALL MITIGATION PLAN (RMP)

Robocall Mitigation Plan

This Robocall Mitigation Plan describes the specific measures that **TruVista** has implemented to detect and prevent illegal Robocalls on its network. **TruVista** will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described. Should the **TruVista** determine that changes are appropriate, any changes made will be noted in the RMP and uploaded to the database.

TruVista is eligible for the continuing extension of the STIR SHAKEN implementation deadline on Non-IP networks as a small voice service provider (§64.6304 (a)(2) that has non-IP portions within its network §64.6304(d).

TruVista provides local service to fewer than 100,000 voice subscriber lines. The majority of customers are served on the non-IP portions of TruVista's network which relies on technology that cannot initiate, maintain, carry, process, and terminate SIP calls.

Consistent with § 64.6303 (a)(1), **TruVista** is ready to upgrade its entire network to allow for the initiation, maintenance, and termination of SIP calls and fully implement the STIR/SHAKEN framework. **TruVista's** non-IP network is connected to carriers that do not support IP connectivity, therefore, **TruVista** cannot upgrade its Non-IP network to IP.

Risk Assessment. **TruVista** is a voice service provider offering a variety of voice calling services. Its customers generally do not originate high volume calls and **TruVista** has not received information suggesting that Robocalls are originated on its network. Therefore, **TruVista** does not consider its network at high risk of originating illegal Robocalls.

SPECIFIC MEASURES TO IDENTIFY AND PREVENT ILLEGAL ROBOCALLS

Customer Due Diligence: **TruVista** conducts due diligence on new and renewing customers, confirming the customer's identity. **TruVista** confirms the customer's service address for all customers.

- **TruVista** verifies customer information when contracts are renewed or services are added.
- **TruVista** verifies the customer's identity
- **TruVista** has the policies that define the circumstances by which it will deny, suspend or terminate service to a customer.

Measures to Prevent or Avoid the Origination of Illegal Robocalls

- **TruVista** has in place an enforceable terms of use and/or an acceptable use policy. **TruVista** also has in place policies designed to detect and prevent fraudulent traffic on its network.
- **TruVista** uses TNS Call Guardian analytics technologies and services to monitor traffic on its network and identify potentially unlawful call origination activity. If **TruVista** has a reasonable basis to believe that a customer is originating illegal Robocalls, it will require the customer to remedy the problem and, if effective action is not taken, **TruVista** can suspend and/or terminate service to the customer.
- **TruVista** knows all the carriers from which it receives traffic and has confirmed that all of the carriers are listed in the Robocall Mitigation Database. **TruVista** monitors incoming traffic from all connected carriers for suspicious call patterns indicative of illegal robocall activity, notifies the upstream carriers of any such traffic and warns the carriers that if the traffic does not cease, the calls may be blocked from entering **TruVista's** network. In addition, **TruVista** is now incorporating traceback and prohibited traffic language in all contractual agreements with new upstream carriers.

Responding to Traceback Requests

- **TruVista** has designated an individual as a dedicated point of contact for addressing traceback requests, and a backup person to that individual. It either has provided the ITG with the contact information and business hours for those individuals, or will do so upon receipt of the first request from the ITG. See <https://www.ustelecom.org/the-industry-traceback-group-itg/for-providers/>
- **TruVista** will respond promptly to inquiries received from the Industry Traceback Group. If a pattern of questionable activity is detected, **TruVista** will require its customer to remedy the problem and, if effective action is not taken, service to the customer may be suspended and/or terminated.

Cooperation with State and Federal Regulators

TruVista commits to responding to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, within twenty-four (24) hours. Specifically, **TruVista** 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.

TruVista uses call authentication, call labeling, and call blocking services provided by TNS. We have made great strides to protect our networks and consumers from harmful calls. **TruVista** is pleased to play a role in that improvement and will continue the necessary work to protect our customers.

Sincerely,

Eric Ramey Digitally signed by Eric Ramey
Date: 2024.02.26 17:27:11 -05'00'

Eric Ramey
Secretary