

Robocall Mitigation Plan

Business Information

VPNet, Inc.
State Road 172, Km. 49.7
Plaza Cidra Mall
First Level, Retail Space 18
Cidra, Puerto Rico 00739

Robocall Contact

Felipe J. Hernandez
CEO
(787) 638-1080
fhdez@vpnet.net

Overview

In the Commission's release, *In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking*, WC Docket No. 17-97 (rel. March 17, 2023) ("R&O") it is stated that all voice service providers ("VSPs") must file robocall mitigation plans ("RMPs") that, among other things, outline "reasonable steps" taken to avoid originating illegal robocalls.

In addition to the "reasonable steps," the FCC requires that a RMP include:

- "know your customer" procedures;
- "know your upstream provider";
- ownership information;
- a description of any call analytics system used to identify and block illegal traffic; and
- whether a third-party vendor is used and if so, the name of the vendor.

The FCC previously stated that a RMP is sufficient if the detailed practices in the plan can reasonably be expected to significantly reduce the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

Purpose

VPNet, Inc. ("VPNet") is a small voice service provider ("VSP") that is dedicated to stopping illegal calls from originating on and passing through our network. This document delineates VPNet's RMP.

Know Your Upstream Provider

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls Call Authentication Trust Anchor, Seventh Report and Order In CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking In CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59* (Rel. May 19, 2023) ¶¶ 49-51, VPNet provides the following information concerning its upstream voice service carrier.

VPNet has one upstream provider from which it receives voice traffic:

Optivon, LLC
27 Calle Gonzalez Giusti, STE 100
Edif. Tres Rios
Guaynabo PR 00968
Felix Cardona
(787) 596-8933
fcardona@optivon.net

VPNet has a master service agreement with Optivon, LLC ("Optivon") and has received assurances in writing from Optivon officials it has, and will continue to, sign calls transmitted to VPNet and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to VPNet. VPNet and its upstream provider have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Know Your Customers ("KYC")

VPNet's KYC program involves obtaining specific subscriber information when payment is made for services. This process includes collecting such information such as:

- physical business location;
- contact person(s), including telephone number and email address; and
- nature of the customer's business.

Acceptable Use Policy ("AUP")

VPNet maintains an AUP that subscribers must sign before being permitted to use VPNet's network. Among other things, the AUP prohibits:

- providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call;
- violating any applicable local, state, or federal law, including robocall laws;
- violating applicable industry accepted guidelines; and
- using VPNet's service to engage in or in connection with fraudulent activities.

VPNet's contractual terms with subscribers specify that VPNet may take action up to suspension or termination of service for violation of the AUP.

Telephone Number Authorization

A Telephone Number ("TN")-based caller identity is the originating phone number included in call signaling used to identify an outbound caller for screening purposes that is uniquely associated with the subscriber. A subscriber is permitted to use a TN as a caller identity if a TN is directly managed by VPNet and/or obtained by VPNet from one of VPNet's underlying carriers for use by the subscriber. In most cases, VPNet directly manages the TNs used by its subscribers. VPNet tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of VPNet's assignment of the TN to its subscriber.

If a subscriber wishes to use a TN as a caller identity and that TN is not directly managed by VPNet, then TN validation is necessary. If a subscriber's end-user can provide a valid letter of authorization that they are the authorized user of such TNs, VPNet will attest calls originated with these TNs.

When originating a call, VPNet checks the calling party number against VPNet's inventory and will not attest the call unless the calling party number is a TN that has been properly validated.

Analytics for Monitoring Traffic

VPNet has a monitoring and reporting system in place to analyze high-volume voice traffic to identify and monitor patterns consistent with robocalls. Our server-based monitoring system alerts us to calling patterns with unusual spikes, traffic patterns, or attempted use of non-validated ANIs to detect patterns consistent with illegal robocalls.

If VPNet detects a calling pattern consistent with illegal robocalls, we will identify the party that is using our network to originate those calls and will take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating subscriber owns or is authorized to use the Caller ID number, and suspending or terminating the party's ability to originate calls on our network.

No third-party vendors are involved in deploying VPNet's analytics.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, our risk prevention team is alerted which follows the defined procedures on investigating such subscribers.

The procedures established include but are not limited to:

- checking recent and past call detail records and benchmark against expected trends;
- checking recent and past account activity and purchases;
- investigating if any system issue generates the strange behavior;
- verifying that the call originating path is valid; and
- contacting the subscriber to understand his or her particular use case and validate that the activity belongs to that subscriber.

VPNet follows Industry Traceback Group ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, VPNet will devote sufficient resources to provide prompt and complete resources to traceback requests. VPNet certifies that it will comply with traceback requests within 24 hours of receiving same.

Blocking

VPNet will implement Do Not Originate requests it receives from the ITG. VPNet has mechanisms to automatically block suspicious calls using internal analytics. If VPNet's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, VPNet will take appropriate action which may include suspending or terminating the subscriber's use of VPNet's network. VPNet will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement (including state attorneys general offices), to the FCC, and/or the ITG; as well as documenting requests & actions taken in response thereto.

Plan Updates

This plan and industry best practices must evolve to response to the dynamic nature of mitigating illegal robocalling. VPNet will monitor industry best practices and continuously improve our internal processes to ensure this plan and our system adapt to this ever-changing issue.

In the event of any material change to this plan, VPNet will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.

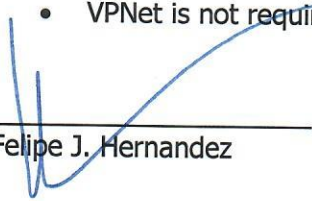
Certification of Felipe J. Hernandez

I, Felipe J. Hernandez, CEO of VPNet, Inc. ("VPNet"), do hereby certify, under penalty of perjury, the following:

- VPNet's business name and primary address are as follows:

VPNet, Inc.
State Road 172, Km. 49.7
Plaza Cidra Mall
First Level, Retail Space 18
Cidra, Puerto Rico 00739

- VPNet's d/b/a name is Red Verde.
- Except for Red Verde, VPNet has not previously used any other business name.
- The name, title, department, business address, telephone number, and email address of the individual responsible for addressing robocall-related issues are listed in the above robocall mitigation plan.
- The following persons/entities own more than 10% of VPNet: Felipe J. Hernandez
- VPNet has no subsidiaries or affiliates.
- None of the persons or entities listed above have had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- VPNet's role in the call chain is that of a voice service provider that does not have a STIR/SHAKEN implementation obligation serving end-users.
- VPNet has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- VPNet is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- VPNet is not required to, nor does it have, an Operating Company Number.



Felipe J. Hernandez