

Robocall Mitigation Plan and Policies

April 5, 2024

I. Overview

This mitigation plan is submitted on behalf of Preferred Connections Inc., NW and Vobis Software Inc. it's software and technical service provider. Preferred Connections Inc., NW (PCI) and Vobis Software Inc. (Vobis) share operations and technical services including the respective Robocall Mitigation Plan and will be referred to as PCI throughout this document. 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 the Provider's current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network. PCI views these policies and procedures as constituting "reasonable steps" to avoid the origination of illegal robocalls on its network and in addition to following these steps the PCI 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.

II. STIR-SHAKEN IMPLEMENTATION STATUS

PCI originates calls via SIP connections within its network. PCI has registered with the Policy Administrator and is an authorized service provider in the STIR|SHAKEN ecosystem. PCI has implemented STIR|SHAKEN within its IP-network and signs the calls originating on the IP portions of PCI's network. Our Certificate provider is Telonium, who is a recognized Certificate Authority approved by iConnectiv.

III. TRACEBACK REQUESTS

As noted above, the PCI will cooperate with the FCC, law enforcement and the (ITG) on all traceback requests and investigations. To allow for timely and comprehensive law enforcement response efforts against illegal robocallers, the PCI will dedicate sufficient resources to promptly complete and provide responses to all traceback requests received from the FCC, law enforcement and/or the ITG, and commits to fully responding to any traceback request received within 24 hours after receiving the same. Within **Appendix A** to this Plan, PCI identifies a single point of contact for receiving all traceback requests.

As part of its efforts to assist in the successful traceback of illegal robocalls, PCI will going forward include within its service agreements language requiring traceback cooperation on any voice service calls exchanged. In part, these related contract provisions will specify the need for parties to promptly identify any suspected illegal robocall in its network or the customer of the service from which the call originated.

IV. CUSTOMER VETTING PRACTICES

As a means of preventing or minimizing the origination of illegal robocalls through its voice services, the PCI will use best practices in vetting the identity of all of its voice service subscribers, whether a residential or business/commercial subscriber (including any entities that are purchasing the PCI's services for resale). The subscriber vetting process is intended to help determine the legitimacy of a customer for the purpose of establishing a service relationship. Generally, PCI looks to confirm the identity of customers using its voice services through collecting information such as physical customer location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business. PCI's efforts to vet retail and business/commercial subscribers occurs during the process of provisioning customer requested services (for example in appropriately sizing the facilities to their claimed intended use), executing PCI's required service agreements, and granting the customer the right to use telephone number resources. Commercial end users, comprised of larger businesses with more complex service configurations, are generally recognized as presenting a higher risk of perpetrating illegal robocalls and thus those customers, at PCI's discretion, may be subject to an additional review, including a more stringent background check and possibly a site visit.

Further, with respect to meeting existing obligations to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls, PCI:

- Utilizes service agreements and acceptable use policies as a means of preventing its new and existing subscribers from using their voice services in ways that would be in violation of local, state, or federal laws, or to engage in deceptive or fraudulent activity. These documents governing use of PCI's provided services include terms indicating specifically to all customers that their services should not be used for the purpose of making illegal robocalls, and PCI reserves authority within its service agreements to suspend or terminate a subscriber's voice service for violating applicable service-related terms.
- Has established a routine process for monitoring of the usage and quality of its network facilities and conducts recurring and timely reviews of its call detail records (CDRs) to facilitate early identification of unusual or suspicious calling activity or patterns that may indicate use of the network for originating illegal robocalls. In those instances where P C I identifies activity or a pattern consistent with illegal robocalls the customer will be contacted within twenty-four hours for further investigation and possible action regarding their subscribed to voice service.

All PCI customers and end users are advised of and are subject to our Acceptable Use Policies (AUP) and our Terms Of Service (TOS). Each of these documents are part of the agreement of service and contract signed and acknowledged by all end users and customers. Our existing AUP and TOS prohibit the actions and activities normally associated with Robocalling including but not limited to:

- 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;
- Using any PCI service to engage in any deceptive or fraudulent activities;

In addition to our current policies all customers and end users are provided a copy of our AUP and TOS reminding them of the restrictions and requirements regarding continued use of our service and products.

All PCI customers and end users are advised that PCI may take various actions up to and including suspension or termination of service for violation of the AUP or TOS.

V. TELEPHONE NUMBER VALIDATION PRACTICES

Telephone Number Validation refers to the confirmation of the customer or end-user right to use a telephone number in connection with their subscribed voice service(s). In accord with industry best practices, PCI has procedures in place to confirm the calling customer's right to use a telephone number. Specifically, a subscriber of the PCI's services is permitted to use a telephone number as their caller identity if a number is directly managed by PCI and/or obtained by PCI via an underlying partner.

VI. INTERNATIONAL CALL ORIGINATORS

PCI is not currently an international voice services provider, and currently has no plan to become such. If at any time the PCI does sell its services to customers which are international call originators using North American Numbering Plan resources it will familiarize itself with and develop best practices for fully vetting such customers and performing telephone number validation on all international originated calls.

VII. KNOW YOUR UPSTREAM PROVIDER PROCEDURES

As a rural provider of voice services, the number of upstream providers used by PCI to receive and deliver its originated voice calls for termination are somewhat limited. The PCI has longstanding relationships with these upstream providers and maintains its awareness of the nature of their businesses and the legitimacy of their call transmission services. Further, PCI, in the interest of providing the highest quality services to all of its voice service customers, is committed to taking those steps necessary to ensure that any upstream providers providing connectivity are equally committed to monitoring their networks and preventing their use for the transmission of illegal robocalls. This includes the use of robocall prevention language in any contracts that PCI may directly have with any upstream provider entities. Included as part of **Appendix A** to this Robocall Mitigation Plan document is a list of the Provider's current, immediate "Upstream Provider(s)" along with contact information for each.

VIII. ONGOING ROBOCALL MITIGATION PRACTICES

PCI monitors the usage of its network and examines call detail records (CDRs) on a recurring basis for the purpose of detecting suspicious call activity and/or calling patterns. When network usage patterns consistent with illegal robocalls are detected or PCI otherwise suspects illegal robocalling or spoofing is taking place on its network, it immediately seeks to identify the party that is originating, terminating, or routing these calls so that it may take appropriate action. The actions taken may include, but are not limited to: initiating a traceback investigation; verifying that the originating customer owns or is authorized to use the Caller ID number; determining whether the Caller ID name sent to a receiving party matches the customer's corporate name, trademark, or d/b/a name; terminating the party's ability to originate, terminate, or route calls on the PCI's network; and providing notice to law enforcement authorities.

As part of its Plan to mitigate and prevent any originating robocalls on its network, PCI is committed to early identification and investigation of possible robocalling situations. In monitoring usage of its network, particular attention is given to: (1) higher than normal subscriber traffic volume including large bursts of traffic in small time-frames or inconsistent volumes of traffic (spikes in usage); (2) originating calls of short duration and low call completion percentages; (3) originating calls with sequential called to number dialing patterns; (4) repeated calls made to do-not-call registry or invalid numbers; and (5) calls to NPA-NXXs not assigned by the North American Numbering Plan Administrator.

Appendix A

Traceback Request Single Point of Contact:

Name: Mark Grigsby

Title: Operations Manager

Phone Number: 541-762-1171

Email Address: mark@pcinw.net

Upstream Provider Information:

Name of Upstream Provider: Commio

Nature of Business: SIP gateway and telecommunications provider

Network Location of Upstream Provider: Raleigh, NC. 27607

Name of contact: Ryan Garrett

Title: Sales Representative

Phone Number: 919-626-9913

Email Address: rgarrett@commio.com

Technical services

support@commio.com

919-490-0000 Option 1

Upstream Provider Information:

Name of Upstream Provider: Sangoma Wholesale Carrier Services (formerly Voip Innovations).

Nature of Business: SIP gateway and telecommunications provider

Network Location of Upstream Provider: Greensburg, PA 15601

Technical support Phone Number: 866-509-5040 or 877-478-6471 (option 2, then 2).

Technical support email: support@voipinnovations.com