

Robocall Mitigation Plan

Business Information

Pennsylvania Computer Connections Inc.
789 East Pittsburgh St.
Greensburg, PA 15601

Robocall Contact

Jessy Marker
Operations Manager
(724) 838-7526, Ext. 112
jmarker@paconnect.com

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 an RMP must 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

Pennsylvania Computer Connections Inc. ("PAconnect") 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 PAconnect'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, PAconnect provides the following information concerning its upstream voice service carrier.

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

Bandwidth, Inc.
2230 Bandmate Way,
Raleigh, NC 27607
Stephen Thayer
919-704-3069
voicesecurity@bandwidth.com

PAconnect has a master service agreement with the above-referenced carrier and has received assurances from that carrier that it has, and will continue to, sign calls transmitted to PAconnect and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to PAconnect. PAconnect 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")

As a means of preventing or minimizing the origination of illegal robocalls through its voice services, PAconnect uses best practices in vetting the identity of all our voice service subscribers. The subscriber vetting process is intended to help determine the legitimacy of a customer for the purpose of establishing a service relationship. PAconnect looks to confirm 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, as well as an on-site inspection and installation of the phone system. PAconnect vets retail and business/commercial subscribers occurs during the process of provisioning customer requested services (*e.g.*, appropriately sizing the facilities to their claimed intended use), executing the PAconnect'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 the PAconnect's discretion, may be subject to an additional review, including a more stringent background check.

Acceptable Use Policy

PAconnect utilizes service agreements and acceptable use policies ("AUPs") as means of preventing our new and existing customers from using their voice and broadband services in ways that violate local, state, or federal laws, or to engage in deceptive or fraudulent activity. These documents govern the use of PAconnect's services and include terms specifically stating that customers may not use our services to make illegal robocalls. PAconnect reserves authority within its service agreements and AUPs to suspend or terminate a subscriber's voice service for violating applicable service-related terms.

Telephone Number Authorization

Telephone Number Authorization ("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 accordance with industry best practices, PAconnect has procedures in place to confirm the calling customer's right to use a telephone number. Specifically, a subscriber is permitted to use a telephone number as their caller identity if a number is directly managed by the PAconnect and/or obtained by PAconnect via an underlying partner. Further, for: (1) single line voice service subscribers, both services connected via TDM or IP, the switching equipment has been set up to

only accept calls from the number assigned to that subscriber; and (2) subscribers with multi-line telephone systems, for both services connected via TDM or IP, PAconnect screens all originating calls and only allows calls to be connected if the originating number matches one of the numbers assigned to the subscriber. These screening capabilities enable an automated and secure method of validating originating telephone numbers.

Analytics for Monitoring Traffic and Investigating Suspicious Activity

PAconnect monitors the usage of our 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 appear consistent with illegal robocalls are detected or PAconnect otherwise suspects that illegal robocalling or spoofing may be taking place on our network, we immediately endeavor to identify the party that is originating, terminating, or routing these calls and take appropriate action. These actions 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 our network, and providing notice to law enforcement authorities.

As part of our plan to mitigate and prevent any originating robocalls on its network, PAconnect is committed to early identification and investigation of possible robocalling situations. In monitoring usage of our network, particular attention is given to: (1) higher than normal subscriber traffic volume including large bursts of traffic in small timeframes 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.

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

No third-party vendors are used in deploying PAconnect's analytics.

Blocking

PAconnect will implement Do Not Originate requests it receives from the ITG. PAconnect has mechanisms to automatically block suspicious calls using internal analytics. If PAconnect's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, PAconnect will take appropriate action which may include suspending or terminating the subscriber's use of PAconnect's network. PAconnect will cooperate with Investigative Bodies 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. PAconnect 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, PAconnect 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 Jessy Marker

I, Jessy Marker, Operations Manager of Pennsylvania Computer Connections, Inc. ("PAconnect"), do hereby certify, under penalty of perjury, the following:

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

Pennsylvania Computer Connections Inc.
789 Pittsburgh St.
Greensburg, PA 15601

- PAconnect and Computer Connections are the d/b/a names of Pennsylvania Computer Connections Inc.
- Except as listed above, Pennsylvania Computer Connections, Inc. 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 10% of or more of PAconnect: Jude Daigle
- PAconnect's principals are: Jude Daigle
- PAconnect 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.
- PAconnect'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.
- PAconnect has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- PAconnect is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- PAconnect is not required to, nor does it have, an Operating Company Number.



Jessy Marker