

PRINCETON HOSTED SOLUTIONS, LLC

Robocall Mitigation Program

February 2024 Version

I. Robocall Mitigation Program Introduction

The following Robocall Mitigation Program (“RMP”) details the policies and practices that Princeton Networks Solutions, LLC (“PHS” “Princeton” or “Company”) is adopted to prevent unlawful robocalls from originating on, terminating to, or routing through PHS’s voice network.

A. Company Summary

Princeton Hosted Solutions was founded in 2012 by a veteran team of telecommunications and IT professionals with the goal of seamlessly transitioning businesses to cloud based services. Our management team has more than 100 years combined experience innovating in the telecommunications and IT fields.

Princeton offers both a hosted PBX and premise-based managed PBX to mid-to-large businesses. Princeton’s hosted offering utilizes the Broadsoft UCaaS platform and Princeton’s SIP trunking. Princeton also offers a managed premise-based PBX utilizing the Allworx platform with Princeton’s SIP trunking. PHS’s Operating Company Number (“OCN”) is 148H.

B. Implementation of STIR/SHAKEN

In accordance with FCC rules referenced below, PHS only accepts traffic from providers that at a minimum satisfy the following requirements:

- Accepting traffic from domestic Voice Service Providers. In accordance with 47 C.F.R § 64.6305(g)(1), PHS accepts calls directly from a domestic Voice Service Provider only if that Voice Service Provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action.
- Accepting traffic from Foreign Voice Service Providers or Foreign Intermediate Providers. In accordance with 47 C.F.R § 64.6305(g)(2), PHS accepts calls from Foreign Voice Service Providers or Foreign Intermediate Providers that use NANP resources that pertain to the U.S. in the caller ID field to send voice traffic to residential or business subscribers in the U.S., only if that foreign provider’s filing appears in the RMD in accordance with paragraph and that filing has not been de-listed pursuant to an enforcement action.
- Accepting traffic from Gateway Providers. In accordance with 47 C.F.R § 64.6305(g)(3), PHS accepts calls directly from a Gateway Provider only if that Gateway Provider's filing (a) appears in the RMD, (b) shows that the Gateway Provider has affirmatively submitted the filing, and (c) has not been de-listed pursuant to an enforcement action.
- Accepting traffic from Non-Gateway Intermediate Providers. In accordance with 47

C.F.R § 64.6305(g)(4), PHS accepts calls directly from a Non-Gateway Intermediate Provider only if that Non-Gateway Intermediate Provider's filing (a) appears in the RMD, (b) shows that the Non-Gateway Intermediate Provider has affirmatively submitted the filing, and (c) has not been de-listed pursuant to an enforcement action.

PHS's Know Your Upstream Provider procedure involves checking the RMD to see if the Provider's filing (a) appropriately appears in the RMD, (b) shows that the provider has submitted the applicable filing, and (c) has not been de-listed pursuant to an enforcement action. VoIP Innovations and Bandwidth.com serves as PHS's primary Intermediate Providers, which are currently and appropriately listed in the RMD.

II. Certification

Company, by submitting this RMP, hereby certifies that (a) all calls originating on its network are subject to this RMP which satisfies the FCC's requirements, (b) any prior certification of the Company has not been removed by Commission action and (c) PHS (including any parent and affiliates) has not been prohibited from filing in the Robocall Mitigation Database ("RMD") by the Commission. PHS (and any parent, affiliate or any entity that shares common ownership, management, directors, or control) has not been the subject of any formal Commission law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient RMD certification or RMP description.

III. Traceback Cooperation

PHS will cooperate in traceback investigations. To allow for timely and comprehensive law enforcement efforts against illegal robocallers, PHS will dedicate sufficient resources to provide prompt and complete responses to traceback requests from law enforcement and from US Telecom's Industry Traceback Group. PHS has identified a single point of contact in charge of responding to these traceback requests and will respond to traceback requests as soon as possible or within 24 hours.

PHS will require traceback cooperation. For all new and renegotiated service applications governing the transport of voice calls, our policy will specify the use of best efforts to require cooperation in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered its network or by identifying our own customer if the call originated in our network.

IV. Implementing Knowing Your Customer and Upstream Providers Protocols

The FCC requires that a Voice Service Provider's RMP "describe with particularity" its robocall mitigation techniques as follows: (1) a Voice Service Provider must describe how it is meeting its existing obligation to take affirmative, effective measures to "know its customers" and prevent new and renewing customers from originating illegal calls; and (2) Voice Service Provider must describe any "know-your-upstream provider" procedures in place designed to mitigate illegal robocalls. To comply with the requirements to describe their "new and renewing customer" and "know-your-upstream provider" procedures, such providers must describe any contractual provisions with end-users or upstream providers designed to mitigate

illegal robocalls. PHS's contractual provisions with its customers are described below.

PHS has implemented Know Your Customer and Upstream Provider procedures used when onboarding new or renewing customers to ensure that such customers and providers do not or are not likely to engage in any prohibited conduct. If the customer is a Voice Service Provider, Gateway Provider, Non-Gateway Intermediate Provider, Foreign Voice Service Provider, and/or Foreign Intermediate Provider, PHS confirms that the provider is appropriately listed in the FCC's RMD and has not been delisted pursuant to an enforcement action before accepting traffic from the provider. As indicated above, VoIP Innovations and Bandwidth.com serves as PHS's Intermediate Providers, which are currently and appropriately listed in the RMD, and PHS does not directly connect to any other provider, so traffic that PHS originates or terminates is carried or processed primarily by VoIP Innovations and Bandwidth.com.

In addition, when signing up new end user customers that will receive on-net VoIP services over PHS's FTTH/P network, PHS sufficiently vets such customers. For instance, as part of the vetting process, PHS collects information such as physical location, contact person(s), and for small businesses, the nature of the customer's business, among other things. Doing so is necessary to provide a prompt response to traceback requests and enforcement efforts.

With these measures and procedures along with those discussed herein, below, PHS takes "affirmative, effective measures to (1) prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic" and (2) know its upstream providers.

V. Requiring Contractual Provisions to Mitigate Illegal Robocalls

In satisfaction of the FCC's requirements that a provider "know its customers" procedures, PHS has revised its Terms and Conditions to include the following language:

12.1.1 Additional Prohibited Uses. Permitted use of the Service does not include certain activities including, but not limited to autodialing, robocalling, transmitting any material that contains viruses, time bombs, trojan horses, worms, malware, spyware, or any other programs that may be harmful or dangerous, spoofing, continuous or extensive call forwarding, continuous connectivity, fax broadcast, fax blasting, polling, transmitting any material that may infringe, misappropriate, or otherwise violate the foreign or domestic intellectual property rights or other rights of third parties, telemarketing (including without limitation charitable or political solicitation, junk faxing, fax spamming, calling/faxing any person through the use of distribution lists or otherwise who has not given specific permission to be included in such a process) or any other activity that would be inconsistent with reasonable business usage.

Customer further agrees not to transmit any material that encourages conduct that could constitute a criminal offense, violate the intellectual property rights of others, give rise to civil or criminal liability or otherwise violate any applicable local, state, national or international statute, regulation, or other law. You agree that you will, at all times, comply with all applicable law. You hereby acknowledge and agree to abide by the terms of the FCC's Declaratory Ruling (CG Docket No. 23-362) dated February 8, 2024 whereby the FCC clarified that calls made with AI-generated voices are "artificial" under the Telephone Consumer Protection Act ("TCPA") which means that voice cloning technology used in

common robocall scams targeting consumers is illegal. Applicable law includes, as applicable, the Telephone Consumer Protection Act and the Telemarketing Sales Rule, the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“TRACED Act”), the Truth in Caller ID Act, the Junk Fax Act, the CAN-SPAM Act, similar state laws, state laws regarding privacy and data subject rights, and the requirements of the Payment Card Industry Data Security Standard (“PCI DSS”). You agree that the Services are not intended for use with alarm systems or elevator telephone systems.

PHS has also including the following language in its language concerning reselling its service:

Robocalling Mitigation Database Registration. If Customer is considered a domestic or foreign voice service provider by the FCC, Customer is required to register with the FCC’s Robocall Mitigation Database. As mandated by the FCC, PHS will block or otherwise not transmit Customer’s voice calls to or from a United States phone number if Customer is not registered in the FCC’s Robocall Mitigation Database.

PHS’s Terms of Service are available at <https://princetonhs.com/wp-content/uploads/2020/09/General-Terms-and-Conditions-PHS-V4.pdf>

VI. Validating Customer’s Right to Use Telephone Numbers

When PHS establishes service to a retail end user voice customer, PHS confirms the end user customer has a verified association with the telephone numbers it uses for its originating telephone calls. In this connection, PHS either assigns the telephone numbers to its VoIP end user customers or ports an existing end user’s customer telephone number on to PHS’s network. For these reasons, PHS does not consider its end user customers to be a high risk of originating illegal robocalls or spoofed calls on PHS’s network. Nevertheless, PHS has adopted various measures discussed below to prevent the origination of such calls on its network.

If PHS detects a pattern consistent with or specific to illegal robocalls (including large bursts of traffic in small timeframes, low duration subscriber traffic and sequential dialing patterns, or call pattern that is consistent with illegal robocalls), or if it otherwise has good reason to suspect illegal robocalling or illegal spoofing is taking place over its network, PHS will seek to identify the party that is using its network to originate, route, or terminate these calls and take appropriate action. PHS may take such actions including, 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 name, trademark, or d/b/a name; reviewing complaints; suspending or terminating the party’s ability to originate, route, or terminate calls on its network; and notifying law enforcement authorities.

VII. Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues

To further ensure PHS’s network is not utilized for the origination, termination, or routing of unwanted and illegal robocalls, PHS provides the following name, title, department, business address, telephone number, and email address of the individual within PHS that leads PHS’s

team that handles robocall mitigation-related issues:

Contact Name: Bradley Bono
Contact Title: CEO
Contact Department: Executive
Contact Street Address: 30 Washington Avenue
Contact City State and Zip Code: Haddonfield, NJ 08033
Contact Telephone Number: (856) 470-1369
Contact Email: bbono@princetonhs.com

VIII. Employee Training and Updates to PHS's RMD Submission

PHS has implemented a training program that focuses on ensuring that personnel receive appropriate training on issues related to illegal robocalls. Employees are instructed to direct any questions about the Robocall Mitigation to the contact identified in Section VII above. The Company agrees to update its submission in the RMD within ten (10) business days of any change to the applicable information it must provide and update in the RMD.