

Safelink Internet, L.L.C.

Robocall Mitigation Plan

Introduction

Safelink Internet, L.L.C. d/b/a Anthem Broadband (“Company” or “Safelink”) provides high-bandwidth internet and digital voice services to business and residential customers in Idaho, Eastern Oregon, Montana, and Nevada. Safelink only serves as a Voice Service Provider. It is not an Intermediate Provider (i.e., it is not a Gateway Provider and is not a Non-Gateway Intermediate Provider).

Safelink does not have an Operating Company Number (“OCN”). Pursuant to 47 C.F.R. § 64.6305(d)(4)(vi), Safelink’s role in the call chain is as a Voice Service Provider that purely resells VoIP services of Atheral LLC.

Certification

Safelink, 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) Safelink (including any parent and affiliates) has not been prohibited from filing in the Robocall Mitigation Database (“RMD”) by the Commission. The Company also certifies that all calls it originates are compliant with Commission rules. Safelink (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.

Only Accepting Traffic from Providers that Have Affirmatively Filed in the RMD

In accordance with FCC rules referenced below, Safelink 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), Safelink 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), Safelink 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 this 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), Safelink 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), Safelink 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.

Safelink'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. As indicated below, Atheral LLC serves as Safelink's Intermediate Providers, which are currently and appropriately listed in the RMD, and Safelink does not directly connect to any other provider, so the Company satisfies the above requirements.

Traceback Cooperation

Safelink will cooperate in traceback investigations. To allow for timely and comprehensive law enforcement efforts against illegal robocallers, Safelink will dedicate sufficient resources to provide prompt and complete responses to traceback requests from law enforcement and from US Telecom's Industry Traceback Group. Safelink 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.

Safelink 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.

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.

Safelink 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, Safelink 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.

In addition, when signing up new end user customers that will receive on-net VoIP services over Safelink's FTTH/P network, Safelink sufficiently vets such customers. For instance, as part of the vetting process, Safelink collects information such as physical location, contact person(s), and for small businesses, 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, Safelink 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.

Requiring Contractual Provisions to Mitigate Illegal Robocalls

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

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 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").

Safelink's Terms of Service and Acceptable Use Policy are available at

<https://anthembroadband.com>.

Validating Customer's Right to Use Telephone Numbers

When Safelink establishes service to a retail end user voice customer, Safelink confirms the end user customer has a verified association with the telephone numbers it uses for its originating telephone calls. In this connection, Safelink either assigns the telephone numbers to its VoIP end user customers or ports an existing end user's customer telephone number on to Safelink's network.

Moreover, in providing VoIP services, Safelink preprograms so that it only allows DIDs assigned to the end user to be passed to Caller ID. With this preprogramming, Safelink's end-users cannot change the Caller ID telephone number they have been assigned and cannot otherwise engage in spoofing. This preprogramming occurs for all of Safelink's VoIP customers, whether the end user customer ported its telephone number from another provider to Safelink or Safelink assigned the telephone number to the end user customer. In addition, when using Safelink's VoIP service offering, such end-user customers cannot simultaneously send numerous calls over a few voice paths. For these reasons, Safelink does not consider its end-user customers to be a high risk of originating illegal robocalls or spoofed calls on Safelink's network. Nevertheless, Safelink has adopted various measures discussed below to prevent the origination of such calls on its network.

Analyzing and Monitoring Network Traffic Routing Through Safelink Internet, L.L.C.'s Network

If Safelink observes a high-volume voice traffic on its network (which would be highly unlikely for the reasons noted above), Safelink will analyze such traffic to identify and monitor patterns consistent with robocalls. For example, Safelink may employ tools to detect and act on such patterns. Safelink does not use a third-party analytics vendor.

If suspicious calling patterns are found, Safelink, after further investigation, takes appropriate action to address such behaviors. If the calls are determined to be illegal robocalls originating on Safelink's network, Safelink's service to the end user customer originating such calls will be suspended or terminated. If the robocalls are illegal and terminating on Safelink's network, Safelink will work with its Intermediate provider to address and block such traffic.

Investigating Suspicious Calling Patterns

If Safelink 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, Safelink will seek to identify the party that is using its network to originate, route, or terminate these calls and take appropriate action. Safelink 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. Safelink recognizes that foreign originating traffic that uses +1 USA Caller-ID values requires special scrutiny; however, Safelink does not originate foreign originated traffic on its network.

Notably, if calls are determined to be illegal robocalls originating on Safelink's network, Safelink's service to the end user customer will be suspended or terminated in accordance with Safelink's Terms of Service discussed above. If the robocalls are illegal and terminating on Safelink's network, Safelink will work with its Intermediate provider to address and block such traffic. To ensure that Safelink's residential and business end users and Safelink's network are protected from illegal and potentially fraudulent call traffic, and consistent with contractual limitations and legal considerations, Safelink takes these appropriate steps to combat such traffic being originated, terminated, or carried or processed on its network.

Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues

To further ensure Safelink's network is not utilized for the origination, termination, or carrying or processing of unwanted and illegal robocalls, Safelink provides the following name, title, department, business address, telephone number, and email address of the individual within Safelink that leads Safelink's team that handles robocall mitigation-related issues as well as responds to traceback inquiries from the FCC, ITG, and law enforcement agencies:

Contact Name: Wyatt Mickelsen
Contact Title: Director of IT
Contact Department: Information Technology
Contact Street Address: 906 S Oneida ST Unit 8
Contact City State and Zip Code: Rupert, ID 83350-8200
Contact Telephone Number: 208-473-7350
Contact Email: sysadmin@anthembusinessgroup.com

Updates to Safelink's RMD Submission and RMP

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.