

Peeringhub Inc.
Robocall Mitigation Plan

Introduction

This document outlines the comprehensive measures taken by Peeringhub Inc. ("Peeringhub") to prevent and eradicate illegal robocalling. Our commitment includes proactive steps such as pre-qualifying prospective customers, monitoring existing customers for suspicious traffic patterns, and collaborating with other providers and regulatory agencies to combat fraudulent voice activity.

Peeringhub operates as a provider of interconnected VoIP telecommunication services and has fully implemented the STIR/SHAKEN authentication framework throughout its network, ensuring compliance with § 64.6301(a)(1) and (2). We use Denovolab softswitch for call signing and verifying tokens of all inbound traffic. Our OCN is 818H.

Peeringhub pledges to update our Robocall Mitigation filings within 10 business days of any changes to the information outlined in this plan.

Know Your Upstream Providers

Peeringhub holds master service agreements with multiple CLECs. Written assurances have been obtained from their officials, confirming their commitment to signing calls submitted to Peeringhub and adhering to the FCC's STIR/SHAKEN and robocall mitigation rules. A collaborative effort between Peeringhub and its upstream providers is established to diligently mitigate all illegal robocalls, including full cooperation with traceback requests.

Know Your Customer

To understand potential customer business models and assess the risk of involvement in fraudulent robocalling schemes, screening interviews are conducted. Peeringhub mandates the completion of a Know Your Customer document for all customers. Prospects providing anonymous information or displaying data mismatches are not activated. Additionally, prospects must agree to Peeringhub's stringent policies prohibiting fraudulent voice activity. Individuals associated with prospects or customers engaged in improper activities related to fraudulent robocalling lead to rejection as a customer, and existing relationships may be terminated.

Traceback Requests

Peeringhub commits to responding fully within 24 hours to all traceback requests from the FCC, law enforcement agencies, and industry traceback consortiums. Cooperation with these agencies in investigating and stopping illegal robocallers using our service is paramount. Our point of contact for all traceback requests is:

Anne Kwong, VP of Operation
484-424-9683
akwong@peeringhub.com

Upon receiving a traceback request, Peeringhub identifies the call in question promptly, uses the provided URL to report findings, and notifies the traceback group of the customer or provider associated with the call. If an existing customer is identified as the source of fraudulent robocalls, a demand for explanation and verification of mitigation is issued. Failure to remediate fraudulent traffic results in immediately rejecting all traffic from the offending customer.

Telephone Numbers

Peeringhub defines Telephone Number (TN)-based caller identity and ensures that subscribers only use TNs directly managed by Peeringhub or obtained from upstream providers. For multi-line telephone systems, calls are allowed to connect only if the originating number matches one of the TNs assigned to the subscriber, providing an automated and secure method of validating originating telephone numbers.

International Calling

Although Peeringhub does not presently offer international voice services, any prospective decision to expand into international markets will entail a thorough process of familiarization and the development of best practices for the comprehensive vetting of international customers. Our commitment involves prioritized collaboration with upstream providers to conduct the necessary telephone number validation for all calls originating internationally. This strategic approach ensures that, if and when Peeringhub enters the international arena, we will do so with a well-established framework that prioritizes the integrity and security of our services.

Call Analytics

Peeringhub employs an advanced intelligent softswitch developed by Denovolab (www.denovolab.com) to proactively safeguard against unwanted calls marked as spam or fraud by Youmail. In our commitment to halt robodialer and fraud traffic effectively, Peeringhub leverages Denovolab's technology to automatically block all traffic destined for numbers listed in the Do-Not-Call database and any call traffic associated with Caller IDs in the Do-Not-Originate database. The Denovolab softswitch undergoes daily updates to synchronize with the latest information from Youmail, the Do-Not-Call (DNC) database, and the Do-Not-Originate (DNO) database. This ensures that Peeringhub remains at the forefront of call protection, employing real-time data to enhance our ability to thwart unwanted and potentially harmful communications.

Ongoing Robocall Mitigation

Peeringhub monitors and examines Call Detail Records (CDRs) regularly to detect suspicious call activity and patterns consistent with illegal robocalls. Upon identifying potential illegal robocalling, actions may include initiating a traceback investigation, verifying the originating

customer's authorization to use the Caller ID number, ensuring the Caller ID name matches the customer's corporate name, blocking the party's ability to originate, terminate, or route calls, and notifying law enforcement authorities. If traffic is deemed illegal, Peeringhub suspends the traffic immediately, instructs the customer to cease sending that traffic, and allows them to resume only after acknowledgement and commitment to cease such activities.

As part of our commitment to mitigate and prevent originating robocalls, we actively engage in early identification and investigation of possible robocalling conditions. Utilizing denovolab softswitch to identify blacklisted IP addresses and known offenders enables us to block malicious traffic proactively. Additionally, we monitor subscriber traffic volume, identifying abnormal patterns or spikes for further investigation.

Peeringhub Contact for Robocall Mitigation-Related Issues

For any inquiries related to Robocall Mitigation issues, please contact:

Anne Kwong, VP of Operation
3524 Silverside Road Suite 35B,
Wilmington, Delaware, 19810
484-424-9683
akwong@Peeringhub.com