

Hopi Telecommunications, Inc. ROBOCALL MITIGATION PLAN

STIR/SHAKEN Continuing Extension

Hopi Telecommunications, Inc. (Hopi) is eligible for the continuing extension of the STIR SHAKEN implementation deadline on Non-IP networks as a small voice service provider (§64.6304 (a)(2) that has non-IP portions within its network §64.6304(d)).

Hopi Telecommunications, Inc. provides local service to fewer than 100,000 voice subscriber lines. All customers are served on the non-IP portions of Hopi Telecommunications, Inc.'s network which relies on technology that cannot initiate, maintain, carry, process, and terminate SIP calls.

Consistent with § 64.6303 (a)(1), Hopi Telecommunications, Inc. is ready to upgrade its entire network to allow for the initiation, maintenance, and termination of SIP calls and fully implement the STIR/SHAKEN framework. However, Hopi Telecommunications, Inc.'s non-IP network is connected to carriers that do not support IP connectivity; therefore, Hopi Telecommunications, Inc. cannot upgrade those Non-IP portions of its network to IP connectivity.

Robocall Mitigation Plan

All voice traffic that originates on Hopi Telecommunications, Inc.'s network is subject to the following Robocall Mitigation Plan.

Call Analytics

Hopi Telecommunications, Inc. currently contracts with TransNexus, a third-party vendor, and utilizes their robocall mitigation services.

The company is also taking reasonable steps to avoid the origination, carrying, or processing of illegal robocall traffic which are outlined herein such as investigating calls identified by its internal traffic monitoring as suspicious calls or those that have abnormal call volumes, patterns or activity consistent with illegal robocalls, has procedures in place to prevent new & renewing customers from using our network to originate illegal robocalls.

Investigation

Hopi Telecommunications, Inc. investigates calls identified by its internal traffic monitoring as suspicious calls or those that have abnormal call volumes, patterns or activity consistent with illegal robocalls.

In addition, if Hopi Telecommunications, Inc. has any other reason to suspect illegal robocalling or spoofing is taking place over its network, Hopi Telecommunications, Inc. will work internally

to identify the party that is using our network to originate, route, or terminate such calls and take appropriate action.

Enforcement

Illegal robocalls and fraudulent spoofing is prohibited on our network. If it is determined a Hopi Telecommunications, Inc. customer is using our network to fraudulently spoof calls or to originate illegal robocalls, Hopi Telecommunications, Inc. will either warn the customer to stop such practices or terminate their service as allowed per Hopi Telecommunications, Inc.'s service policy.

Acceptable Use Policy

Hopi Telecommunications, Inc. includes specific terms and conditions in its customer contracts to clarify the intended and permissible uses of our services. These provisions are designed to help customers understand proper usage while safeguarding against exploitation, fraud, and abuse of our calling plans and features. As part of the terms, Hopi reserves the right to pause, suspend, or otherwise terminate service for any customer engaged in illegal activities, including the generation of unlawful robocalls.

Know Your Customer Protocols

Hopi Telecommunications, Inc. has implemented proactive and effective measures to prevent both new and renewing customers from using its network to originate illegal robocalls. These measures include conducting thorough due diligence and ensuring that its services are not misused for such activities. As part of this process, Hopi verifies the identity of new and renewing customers by asking personally identifiable questions for additional security on each account and collecting key identifying details, such as Social Security Number (SSN), date of birth, business contact information, physical location of the business, state or country of incorporation, and federal Tax ID, as applicable.

Know Your Upstream Providers

Hopi Telecommunications, Inc. knows all the carriers from which it receives traffic and has confirmed that all the carriers are listed in the Robocall Mitigation Database. No provider is using Hopi Telecommunications, Inc.'s network to carry or process a high volume of illegal traffic. Hopi Telecommunications, Inc. monitors incoming traffic from all connected carriers for suspicious call patterns indicative of illegal robocall activity. The connected carriers are made aware of any suspicious or illegal traffic and notified that, if the traffic does not cease, the calls may be blocked from entering Hopi Telecommunications, Inc.'s network. In addition, Hopi Telecommunications, Inc. is now incorporating traceback and prohibited traffic language in all contractual agreements with new upstream carriers.

Traceback

Hopi Telecommunications, Inc. is dedicated to preventing its network from being used to originate or terminate illegal robocalls. Hopi commits to fully respond to all traceback requests from the Commission, law enforcement agencies, and the industry traceback consortium within twenty-four (24) hours. Furthermore, it is committed to cooperating with these entities to investigate and halt any illegal robocall activities utilizing its services to originate, process, or carry calls.

Robocall Mitigation Database Eligibility

Hopi Telecommunications, Inc. has not been involved in any recent, formal law enforcement or regulatory investigation into suspected unlawful robocalling. Hopi Telecommunications, Inc. has not been prohibited from filing in the Robocall Mitigation Database (RMD).

Conclusion

Hopi Telecommunications, Inc. submits this Robocall Mitigation Program in accordance with Federal Communications Commission Regulations, 47 C.F.R. §64.6305 (a)(1) & (d)(5). Hopi will ensure that any updates to the required information, including its Robocall Mitigation Program, are reflected in the RMD within 10 business days of any changes.