

Northampton IT Robocall Mitigation Plan

Overview

This Robocall Mitigation Plan is submitted by Northampton IT (NIT) pursuant to the provisions of 47 C.F.R. § 64.6305, adopted by the Federal Communications Commission (FCC) which require all voice service providers to establish a robocall mitigation plan. NIT is a U.S. based company that resells the VoIP services of VoIP.ms (FRN: 0022699458), a STIR/SHAKEN compliant provider, based in Canada. All Public Switched Telephone Network (PSTN) connectivity for NIT's customers is managed through VoIP.ms. NIT does not originate calls onto the PSTN or hold telephone numbers directly. NIT relies on VoIP.ms infrastructure for call origination and termination. This document describes NIT's current practices, policies and procedures designed to eliminate illegal robocalls using its service. NIT uses these practices, policies and procedures to avoid the origination of robocalls using its service, and in addition to following these steps, NIT commits to responding to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG), and to cooperate with these entities in investigating and stopping any illegal robocallers that may use NIT's service to originate calls.

STIR/SHAKEN Implementation Status

NIT's has not implemented the STIR/SHAKEN authentication framework as it falls under 47 CFR § 64.6304 (d) which exempts from STIR/SHAKEN Caller ID Authentication for those portions of a voice service provider network that rely on technology that cannot initiate, maintain, carry, process, and terminate SIP. NIT does not originate or terminate calls on the PSTN as stated above. Subsequently, STIR/SHAKEN for NIT's voice services is handled by VoIP.ms.

Customer Vetting Practices

To prevent or minimize the origination of illegal robocalls through its voice services, NIT carefully vets the identity of all of its voice service customers. The customer vetting process is intended to help determine the legitimacy of a customer for the purpose of establishing a service relationship. NIT confirms the identify of customers using its voice services by collecting information such as physical customer location, contact person(s), state of incorporation, federal tax ID, and the nature of the customer's business. NIT additionally vets customers during the process of provisioning customer services by understanding the types of calls they will be making, appropriately sizing the service to their intended use, and granting the customer appropriate telephone number resources.

Further, NIT utilizes service agreements and acceptable use policies as a means of preventing its new and existing customers from using their voice and broadband services in ways that would be in violation of local, state, or federal laws, or to engage in deceptive or fraudulent activity. These agreements, governing the use of services, indicate specifically to all customers that their services should not be used for the purpose of making illegal robocalls, and that NIT reserves the right to suspend or terminate their service for violating the service agreements.

Know Your Upstream Provider Procedures

NIT's provider is VoIP.ms, an FCC registered voice services provider (FRN: 0022699458), located at 200-2480, boul. des Entreprises, Terrebonne, QC, Canada, J6X 4J8. NIT routes traffic exclusively through VoIP.ms for centralized accountability. The point of contact at VoIP.ms for robocall mitigation issues is David Rouleau, Chief Executive Officer, 844-886-4767, drouleau@voip.ms.

As NIT is, so VoIP.ms is committed to monitoring their networks and preventing their use for the transmission of illegal robocalls. This includes fully complying with STIR/SHAKEN, signing all outbound calls

from U.S. phone numbers using its own certificate, algorithms that trigger real-time alerts, notifications and systematic blocks on radical or suspicious calling activities, and 24/7 fraud and on-duty network teams.

VoIP requires customers to pass a valid CallerID format when attempting to place outgoing calls. Everything has to be set in the VoIP.ms platform beforehand. VoIP.ms verifies the identity of users for CallerID purposes. A real-time block system is in place as soon as abnormal activities are detected (including but not limited to abnormal spike of calls, abnormal trends, low call completion statistics, systematic calling, unusual amount of calls, etc.). The VoIP.ms system blocks suspicious traffic. VoIP.ms has a zero-tolerance policy when it comes to potential fraud, scam and robocall activities. VoIP.ms reviews outbound call logs and analytics regularly to monitor for any possible abuse. VoIP.ms also works with its upstream providers to identify behaviors which indicate illegal call activity and patterns.

VoIP.ms has an internal Do Not Originate list to combat fraud and robocalls which is updated regularly with available information shared by government institutions. Additionally, VoIP.ms's upstream carriers make use of the Industry Traceback Group Do Not Originate list as well as Do Not Originate lists from third-party vendors including Somos and Neustar.

VoIP.ms cooperates fully with law enforcement, traceback entities and other sources, including providing the identity of any suspected illegal robocaller, replying to requests within 24 hours. VoIP.ms cooperates in traceback and trace forward investigations. VoIP.ms offers a single point of email contact for any law enforcement requests at law.enforcement@voip.ms.

VoIP.ms updates the FCC Robocall Mitigation Database within 10 days in the event of any material changes to its plans and procedures.

Ongoing Robocall Mitigation Practices

NIT routinely monitors customer usage and conducts timely reviews of call detail records (CDRs) to allow early identification of unusual or suspicious calling activity or patterns that may indicate illegal robocalls. Particular attention is given to: higher than normal volume including large bursts of traffic in small timeframes; inconsistent volumes of traffic; calls of short duration and low call completion percentages; calls with sequential called to number dialing patterns; calls made to the do-not-call registry or invalid numbers; and calls to numbers not assigned by the North American Numbering Plan Administrator.

If NIT suspects illegal robocalling or spoofing is taking place, it immediately seeks to identify the party that is originating, terminating, or routing these calls so that it may take appropriate action. These actions may 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 name; terminating the party's ability to originate, terminate, or route calls; and providing notice to law enforcement authorities.

NIT will file and update this Robocall Mitigation Plan with the FCC Robocall Mitigation Database, as required. Our filing will be accurate and updated within 10 days of any material changes.

Traceback Request Compliance

NIT will cooperate with the FCC, law enforcement, and the ITG on all traceback requests and investigations. NIT will respond within 24 hours after receiving such requests. The single point of contact for all traceback requests is Lee Feldscher, President, 413-303-9514, lfeldscher@northamptonit.com.