

NextPointe Robocall Mitigation Plan for STIR/SHAKEN Compliance

Operations Department

NextPointe Inc.

VERSION HISTORY

Version #	Date	Author	Key Differences
1.0	09/15/2021	Gabriel Ruiz	Doc Generation
1.1	09/16/2021	Luis Perez	Revisions
1.2	09/17/2021	Gabriel Ruiz	Grammar Fixes
1.3	02/26/2024	Gabriel Ruiz	Added STI-PA & TransNexus

TABLE OF CONTENTS

1 Introduction 4

2 Roles and Responsibilities 4

3 Robocall Mitigation Processes 5

 3.1 Before Establishing Service with New Customers.....6

 3.2 Preventing illegal Robocalling.....7

 3.3 After Service Has been Used for Illegal Robocalling8

 3.4 Robocall Monitoring and Control.....8

4 Summary.....10

1 Introduction

This Robocall Mitigation Plan defines the processes and structures that are directed towards realizing STIR/SHAKEN compliance, while simultaneously managing possible adverse impacts. From a service management perspective, Robocall Mitigation is a continuous activity conducted throughout the life of the service. It seeks to identify potential robocallers, evaluate their likely impact, develop mitigation plans, and monitor progress.

The Robocall Mitigation Plan is typically created early in the service's Planning Process Phase. Robocall Mitigation planning is the process of defining how to conduct Robocall Mitigation activities for a service. The plan includes how the organization will identify and address events or occurrences that could negatively or positively affect STIR/SHAKEN compliance. The plan outlines a methodology to identify, analyze, track, and mitigate robocalling during the service lifecycle. Identifying and managing risk increases the chance of a successful service completion by reducing uncertainty associated with the service.

2 Roles and Responsibilities

Name	Role	Responsibility
Gabriel Ruiz	<i>Service Sponsor</i>	• <i>Provides the necessary support to the Service Manager to ensure that resources are available to support the execution of this Plan.</i> • <i>Provides the necessary support to ensure that the service team and key stakeholders commit to the Robocall Mitigation efforts.</i> • <i>Monitors the efforts to address robocalling and provides leadership to focus resources on resolving open unplanned risk events.</i> • <i>Provides guidance on escalated risk events and assists in their resolution.</i> • <i>Responsible for management, administration, and delivery of assigned robocalling mitigation, including updating the Risk Register, the mitigation plan, and contingency plan details in the robocalling Register.</i> • <i>Shared responsibility with the robocalling mitigation Manager and the Service Manager for ensuring that robocalling mitigation is organized, managed, and controlled and that robocalling incidents are identified and</i>

Name	Role	Responsibility
		<i>mitigated in a timely manner to minimize impact to the service.</i> • <i>Provide status updates to Robocalling Mitigation Manager.</i>
Luis Perez	Service Manager	• <i>Tracks progress of the Robocall Mitigation effort by reviewing the Robocall Register and/or Robocall Mitigation reports.</i> • <i>Escalates mitigation approaches for identified high severity robocalling incidents that are beyond the Service Manager's span of control and decision authority.</i> • <i>Ensures the entire service team, state, and vendor, are following this Plan.</i> • <i>Ensures all other service processes that interact or provide input to the Robocall Mitigation effort are being adhered to.</i> • <i>Ensures there are sufficient resources to execute this Plan and that the Robocall Mitigation activities are being performed in a timely manner.</i> • <i>Assigns robocalling incidents to owners.</i> • <i>Responsible for maintaining the overall Robocall Mitigation process, the Robocall Register containing the risk details.</i> • <i>Ensures the robocall mitigation managed by this Plan are organized, managed, communicated, and controlled.</i> • <i>Ensures that any service related risks are identified and mitigated in a timely manner in order to minimize impact.</i> • <i>Periodically obtain status from Robocall Mitigation Owners on mitigation progress.</i>

3 Robocall Mitigation Processes

Robocall identification is the first step in the Robocall Mitigation process that the voip services should employ for STIR/SHAKEN compliance. Robocall identification involves identifying such incidents, identifying which of those calls are likely to affect the service and documenting characteristics of those services. Spotting a potential robocaller is accomplished by recognizing that an event, state, or condition within the boundaries of a service may occur with unplanned consequences, which are undesirable,

however it may be desirable leading to a positive opportunity. All 'Service' team members including Stakeholders, end users, subject matter experts, customers and sponsors are encouraged to identify and report potential risks to the service immediately upon detection.

Crucial to robocall identification is the input of service team members and other Stakeholders to recognize and report them as soon as possible. Robocall incidents can also be identified during service team meetings and should therefore be incorporated into the meeting agenda and minutes templates for all provisioning service meetings.

The following must be noted regarding NextPointe and robocall mitigation:

- NextPointe only uses voice service providers with STIR/SHAKEN implementation obligation serving end-users
- NextPointe has not been prohibited from filing a certification in the Robocall Mitigation Database.
- NextPointe does not have a history of enforcement actions for illegal robocalls, TCPA or TSR violations, or related state law violations.
- NextPointe uses the following affirmative, effective measures to prevent the origination or transit of illegal robocalls.

3.1 Before Establishing Service with New Customers

Identifying robocall incidents is an iterative process because new loopholes may become known as the service progresses through its service life cycle. Robocall information can initially be gathered from the Sales team, accumulated Lessons Learned and an initial Robocall mitigation brainstorming session. There are several robocall Identification techniques including reviewing service documentation, brainstorming, interviewing, root cause analysis, checklist analysis, analytics, cause and effect diagrams, process flow charts, SWOT analysis, and expert judgment.

3.1.1 Customer Vetting

NextPointe customers are predominantly small business; these pose the lowest risk of robocall origination; larger commercial customers and BPO customers pose the highest. Many foreign illegal robocallers use VoIP services and DID numbers from the North American Numbering Plan ("NANP") to suggest that their calls were originated within the United States. Customers located outside the United States using NANP numbers will require a much deeper investigation before onboarding those customers.

NextPointe collect and verify information for each commercial customer such as physical business location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the

customer's business. By establishing the existence of the customer can prevent spoofing of corporate identity by potential offenders.

3.1.2 Mitigation Through Contracts

Provisions requiring customer assistance in traceback investigations are to be included in all service contracts. NextPointe will not sell service to resellers but rather directly to the end customer thus preventing unknown downstream providers.

3.1.3 Participate in the FCC's Enforcement Database

The FCC has announced it will create a database of approved entities, the Service Provider Registration Portal, for use by law enforcement, as well as screening by intermediate and terminating voice service providers. NextPointe has registered with the STI-PA using OCN 819K. Along with its own STIR/SHAKEN certificate issued by the TransNexus Certification Authority (STI-CA) that it uses when authenticating calls it originates. Implementation of the STIR/SHAKEN solution is supplied by TransNexus.

3.2 Preventing illegal robocalling

Strategies for Preventing Robocalls:

- 3.2.1 **Caller ID and Blocking:** We follow the caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers as described by the NANC Call Authentication Trust Anchor Working Group. This process includes the collection and review of entity-identifying information to confirm that we have an authenticated relationship with the customer. We use this authenticated information to determine whether the customer is subject to any enforcement actions that restrict the type of calling that they may do, for example, if they have been banned from initiating telemarketing calls. We also validate, when possible, that the entity has a legitimate right to use its asserted calling numbers. We use this information to support the attestation level we assign to calls that we originate for that customer. Our contractual provisions with customers prohibit them from initiating illegal robocalls. If we find a customer initiating suspicious robocalls, we warn them to stop. If such traffic continues, then we terminate their service.

- 3.2.2 **Upstream Providers:** We have a vetting and review process for upstream providers, that is, providers that send us voice traffic that we terminate or transit to other providers. We confirm that the upstream provider has a certification in the Robocall Mitigation Database. We will not accept voice traffic from an unregistered provider. We require that upstream providers have a reasonable robocall mitigation plan, including a vetting process for their customers and upstream providers, and use call analytics to identify suspicious traffic. We establish an understanding of the upstream provider's role in the call path for the traffic they will send to us, for example, whether they are acting as an originating voice service provider, a foreign intermediate provider, or a U.S.-based intermediate provider. We use this information to understand whether we will be obligated to authenticate unsigned traffic that we receive from them. Our contractual provisions with upstream providers prohibit them from sending us illegal robocalls. If we find that an upstream provider is sending us suspicious robocalls, we warn them to stop. If such traffic continues, then we terminate their service.
- 3.2.3 **Third-Party: NextPointe** uses call analytics software provided by TransNexus to monitor all outbound voice traffic in real-time to prevent the origination or transit of illegal robocalls. The software provides detailed reporting to identify suspected illegal robocalls. The system alerts us if we process outbound calls where the calling number has a poor reputation or is invalid, unallocated, or on a Do Not Originate list. We perform the same mitigation steps for all outbound calls regardless of our role in the call chain for a particular call.
- 3.2.4 **Investigate Suspicious Activity:** When traffic analysis indicates the presence of likely illegal robocalling, NextPointe will immediately investigate any identified suspicious calls to determine if the caller or upstream provider was attempting to originate or transit unlawful robocalls. If we determine that the traffic was likely unlawful, then we warn them to stop sending such traffic. If they continue to send traffic that appears to be unlawful, then we terminate their service.

3.3 After Service Has been Used for Illegal Robocalling

- 3.3.1 **Traceback investigations:** NextPointe will be conducting traceback investigations into suspicious activity upon detection. Also NextPointe will comply with traceback requests by law enforcement, the FCC, or the Industry Traceback Group. NextPointe will designate a single point of contact to handle traceback requests and coordinate with outside investigations.

- 3.3.2 Communicate with Authorities:** NextPointe will respond within 24 hours to all traceback requests from the Commission, law enforcement, and the registered traceback consortium. NextPointe will cooperate fully with such entities in investigating and stopping any illegal robocallers that uses NextPointe service to originate, carry, or process illegal robocalls.

3.4 Robocall Monitoring and Control

3.4.1 Robocall Monitoring Activities

Once a robocall metric is established, it is monitored on an ongoing basis:

- Monitor if a robocall escalation trigger has occurred.
- Monitor if robocall response actions are as effective as anticipated.
- Monitor if robocall responses are implemented as planned.
- Monitor for robocalling incidents (element of a robocall that remains once the robocalling mitigation assessment has been made and responses implemented).
- Monitor systematically to:
 - Assess currently defined robocalling
 - Determine actions to be taken
 - Evaluate effectiveness of actions taken
 - Report on the status of actions to be taken
 - Validate previous robocall mitigation assessment (likelihood and impact)
 - Validate previous assumptions
 - State new assumptions
 - Identify new loopholes

3.4.2 Robocall Control Activities

Once a robocall is established, it is controlled on an ongoing basis:

- Validate mitigation strategies and alternatives
- Assess impact on the 'Service' of actions taken (scope, cost, time, schedule, & resources)
- Identify new robocalls resulting from robocall mitigation actions
- Ensure that the services' Robocall Mitigation Plan is maintained
- Revise Robocall Mitigation Response plan(s)

4 Summary

The following is a summary of the NextPointe robocall mitigation plan:

- NextPointe will take reasonable steps to avoid originating illegal robocall traffic, following the FCC recommendations of using reasonable analytics.
- NextPointe will commit to respond to requests from the Industry Traceback Group (also known as the Industry Traceback Consortium) to trace suspect calls back to their origin; and
- NextPointe must cooperate in investigating and stopping any illegal robocallers (meaning that NextPointe will block calls or callers that are believed to be illegal).
- NextPointe registered with the STI-PA using OCN 819K. We have our own STIR/SHAKEN certificate issued by the TransNexus Certification Authority (STI-CA) that we use when authenticating calls we originate. We have implemented a STIR/SHAKEN solution supplied by TransNexus