

INPHONEX ROBOCALL MITIGATION PROGRAM

Below is the Robocall Mitigation Plan filing for InPhonex. This plan will be submitted to the FCC's Robocall Mitigation Database and will be adapted to adjust to the latest laws, regulations, and industry best practices.

Monitoring

InPhonex has monitoring and reporting systems in place to analyze high-volume voice network traffic to identify and monitor patterns consistent with robocalls. Our monitoring systems provide alerts on calling patterns with unusual spikes, traffic patterns, or attempted use of non-validated Telephone Number (TN) to detect patterns consistent with illegal robocalls.

If InPhonex detects a pattern consistent with illegal robocalls, or we have reason to suspect illegal robocalling or spoofing is taking place over our network, we will seek to identify the party that is using our network to originate, route, or terminate these calls. and take appropriate action.

Appropriate action may include:

- Validating that the originating party is authorized to use the TN.
- Suspending calling party's ability to originate, route, or terminate calls on InPhonex's network.

Traceback Cooperation

InPhonex commits to responding in a timely manner and supporting all traceback requests from the FCC, law enforcement, and the [Industry Traceback Group \(ITG\)](#).

Sansay's Robocall Mitigation Solution Overview

InPhonex has employed the Sansay to provide additional Robocall mitigation services, in addition to ones developed in house.

These combined efforts entail:

- Calls originating from InPhonex network (i.e., Robocall Protection)
 - Provide detailed reporting identifying suspected illegal robocalls and alerts if calls originate where the calling number is invalid, unallocated, on a Do-Not-Originate list.
 - If the platform detects a suspected robocalling patterns InPhonex will take appropriate action which may include suspending or terminating the subscriber.

- Supports a real time query to service to determine if a number originating on your network could be a robocall. Such calls can be blocked, or the terminating party can be notified via CNAM.
- For each new instance of robocalling using the Operating Service Provider (OSP) TNs, an alert is sent to the OSP in near real time. This alert will result in the OSP (manually) blocking the TN and all TSPs being alerted via CNAM , through an overlay such as "ROBOCALLER". The CNAM alerting helps address instances of spoofing of TNs that are not going through the OSP that owns the number.
- Termination (i.e., Robocall Mitigation)
 - Supports a real-time query to service to determine if a number terminating on your network could be a robocall. This protects subscribers from calls that come from networks that cannot authoritatively attest to the end user caller (i.e., all Communications Service Providers (CSPs) that do not have STIR/SHAKEN and all CSPs *with* STIR/SHAKEN, but who do not have a direct and vetted end user relationship.)
 - Such calls can be blocked or the called party can be notified via CNAM.