

## ROBOCALL MITIGATION PROGRAM

Below is the Robocall Mitigation Plan filing for ACHH LLC. 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

We have 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 we detect 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 we remove this client from our switch immediately.

Appropriate action may include:

- Validating that the originating party is authorized to use that DID or is their ANIS valid.
- Suspending calling party's ability to originate, route, or terminate calls on our switch network. \

### Traceback Cooperation:

- ACHH LLC, commits to responding to all tracebacks with in 1hr and supporting all traceback requests from the FCC, FTC, Attorney Generals, law enforcement, and the ITG.

## Robocall Mitigation Solution Overview

### General information

- STIR/SHAKEN Transaction Detail Records(TDRs) are now being added as an additional data source.
- Active numbers are assessed by the model for behavioral attributes typically associated with robocalling including:
  - Neighbor spoofing events
  - Sudden spikes in volume, such as driven by call spoofing
- Do-Not-Originate(DNO)numbers are also deemed to be robo calls if they are the calling party number. This is sourced from industry and directly from enterprises so they are blocked on our switch.
- The service covers both US domestic and international ANIs.
- Calls originating from your network (i.e., Robocall Protection)
  - Provides 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 we will suspending or terminate 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 robo calling using the ANIs, an alert is sent to our switch in near real time. This alert will result in (manually) blocking the ANI. The switch alerting helps address instances of spoofing of ANIs that are not going through our switch and prevents all scam and fraud traffic to be blocked.

#### Termination (i.e., Robocall Mitigation)

- Supports a real-time query to service to determine if a number terminating on our 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 that do not have 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 blocked on our switch.