



ROBOCALL MITIGATION PLAN

Headland Communications is small voice service provider (VSP) that is dedicated to the reduction of fraudulent call termination and has implemented strict policies that have resulted in no known cases of Caller ID spoofing or Robocalls.

Due to the simplicity of Headland Communications voice offerings we have elected to defer the deployment of the STIR/SHAKEN protocol. In brief, Headland Communications call control platform cannot be used to terminate calls.

Headland Communications retail voice offerings do not allow the end user to set or manipulate their configured caller ID information (CNAM/CNUM). Moreover, all customer calls are originated manually (i.e. dialed by a human) and are limited with by concurrent calls of no more than four (4) per end user.

Headland Communications users the following practices to ensure that

Know Your Customer

Headland Communications follows the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group including but not limited to subscriber vetting and outgoing caller identity validation. (<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>).

Further, Headland Communications customers are bound to an Acceptable Use Policy that specifically prohibits Robocall activities.

Traceback

We are committed to responding to all traceback requests from the Commission, law enforcement, and the registered traceback consortium and will cooperate with such entities in investigating and stopping any illegal activities relating to CallerID Spoofing or Robocalls that originate from our network.

Specific Robocall Mitigation Practices

Headland Communications Signaling Servers:

- Do not allow end users to dynamically set or manipulate their sent Caller ID information (i.e. CNAM/CNUM)
- Only allows ANI to be configured on end user devices with telephone numbers that appear in that customer's CSR (Customer Service Record).
- Limit the number of concurrent calls for any given customer line/device to 4



Headland Communications Session Border Controllers:

- Further police customer originated calls to ensure calls sent to other carriers only contain ANI that appear in the Headland end customer's CSR.
- Validate the ANI is properly formatted and validate E.164 or NANPA 1+10-digit numbering schemes

Headland Communications Network Operations Staff :

- Utilizes a VOIP monitoring system that
 - Alerts on excessive call origination rates by any single number
 - Alerts on excessive call origination rates by any single customer
 - Alerts on excessive call origination rates by any single customer
- Follow strict protocols on identifying and blocking any suspicious call traffic.

Future Implementation

Headland Communications intends to implement authentication and verification the STIR/SHAKEN in advance of the deadline or extension provided for small carriers.

Summary

Headland Communications exposure to Caller ID spoofing and Robocall activities is extremely limited by the nature of our voice offering. The employment of the practices detailed above further limits exposure. To date, not a single known spoofed Caller ID call or Robocall has originated from the Headland Communications network.