

Southern Ohio Communications Services Inc Robocall Mitigation Plan

The FCC requires that all providers certify in the Robocall Mitigation Database their status for compliance with STIR/SHAKEN. Those not yet fully compliant must implement and certify to the implementation of a Robocall Mitigation Plan to ensure that this illegal traffic does not originate on their networks as they work within the industry to become fully compliant.

The Commission requires voice service providers to develop a Robocall Mitigation Plan that:

- ☐ details the reasonable steps taken to avoid originating illegal robocalls
- ☐ demonstrates a commitment to respond to traceback requests to cooperate with investigating and stopping illegal robocalls
- ☐ is filed in the Robocall Mitigation Database.

This mitigation plan is submitted on behalf of Southern Ohio Communication Services Inc, and will be referred to as SOCS throughout this document.

SOCS is a small voice service provider with SIP services in its network.

SOCS is partnering with multiple upstream providers that currently implement STIR/SHAKEN to all calls originating from SOCS Cloud Hosted SIP Server. Those providers are

Voip Innovations

Voyant “Vitelity”

Bandwidth

Thing

SOCS Uses Bicom Systems to provide Voice Over IP Telephone to its end-users.

II. General Prohibition Against Illegal Robocalling

SOCS end user services are subject to restrictions contained in its published legal notices and all executed services orders include the requirement that service is provided pursuant to its terms of service (“TOS”) requirements.

Its existing TOS prohibit activities normally associated with Robocalling including, but not limited to:

Robocall Mitigation Policy

- ☐ providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call;
- ☐ violating any applicable local, state, or federal law; using the SOCS service to engage in or in connection with fraudulent activities

In addition, the company is updating its TOS to expressly reference the prohibition on robocalling and all current subscribers will receive notice of the publication of its updated TOS.

SOCS end users are notified that SOCS may take action up to suspension or termination of service for violation of the TOS.

III. Know Your Customer

SOCS utilizes the mitigation technique of “Know Your Customer.” SOCS is a small long established provider that maintains a close relationship with its subscribers. Its customers are generally “mom and pop” users and currently none of its customers have large enough call paths to produce a high call volume.

SOCS has set a call path level based on its average customer size. The level – referred to as “large volume calling capability” – is subject to change.

SOCS has a screening for new customers requesting service at or above large volume calling capability

levels:

- ☐ We will not deploy large volume calling capability as a residential service or at an address shown in the company records as being residential
- ☐ Businesses requesting large volume calling capability must provide a tax ID and verification as to the nature of the business
- ☐ We verify addresses to look for overlapping / multiple deployed voice path subscriptions
- ☐ A SOCS representative will work with the business to verify the number of users at the location along with call needs to help determine the appropriate call volume settings needed.

IV. Network Monitoring

SOCS is currently monitoring call flows using a 3rd party app. SOCS also subscribes to enhanced tech support with Bicom Systems to help with troubleshooting and CDR related issues.

Robocall Mitigation Policy

V. Traceback and Enforcement Cooperation

SOCS will actively cooperate with the traceback community including the FCC, law enforcement, and The Industry Traceback consortium (ITC) to investigate and stop illegal robocalls. SOCS will dedicate sufficient resources to provide prompt and complete responses to traceback requests.