

SMART COMMUNICATIONS HOLDING, INC.

Robocall Mitigation Plan

STIR/SHAKEN IMPLEMENTATION

Smart Communications Holding, Inc. (“Smart Communications” or “Company”) is a voice service provider (“VSP”), providing Incarcerated People’s Communications Services (“IPCS”) to correctional facilities throughout the United States. Smart Communications has fully implemented STIR/SHAKEN and has submitted its certification that all voice traffic originating on its network is authenticated with STIR/SHAKEN consistent with 47 CFR 64.6301(a). Smart Communications has implemented a Robocall Mitigation Program (“RMP”) to include the obligations outlined in the Commission’s recent release, *In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking*, WC Docket No. 17-97 (rel. March 17, 2023). In compliance with the Report & Order, Smart Communications submits this RMP and certification into the Robocall Mitigation Database.

ROBOCALL MITIGATION

Background

The FCC Order requires that a RMP include the following affirmative obligations for voice service providers:

- Outline reasonable steps VSP has taken to avoid originating illegal robocall traffic;
- Commitment to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls;
- Know Your Customer procedures;
- Describe any call analytics system used to identify and block illegal traffic

Traceback:

The Company will commit to respond fully and within twenty-four (24) hours to all traceback requests received from the Commission, law enforcement, and the industry traceback consortium, and to cooperating with such entities in investigating and stopping any illegal robocalls. Smart Communications works closely with its vendors to constantly review reports from the network, which are used to aid in the investigation. Smart Communications has numerous law enforcement customers and regularly responds to law enforcement requests.

Traceback Contact Information

Name	Title	Contact Information
Andy Bringhurst	Technical Support Specialist	andy.bringhurst@smartcommunications.us
Brian Keller	Technical Support Specialist	Brian.keller@smartcommunications.us

Measures to prevent origination of illegal calls.

Know Your Customer:

Smart Communications' systems and services allow Incarcerated People to remain in contact with family, friends and other associates while still providing facility administrators with the necessary control over inmate communications. The system utilizes IP-enabled technology by routing the calls over the existing broadband carrier's facilities that currently serve the confinement facility. There is no wireline facilities used in the delivery of services. Smart Communications system is designed so that calls are completed only to those called parties who specifically accept the charges for a call. Equipment utilized by Smart Communications requires a positive response from the called party before the connection is established and billing can begin.

Due to the specialized nature of Smart Communications' services, it is highly unlikely that illegal robocall traffic could be originated via Smart Communications inmate calling services system. Smart Communications works closely with its underlying third-party providers to prevent, detect, and mitigate the delivery of illegal robocall traffic. In addition, Smart Communications will respond to all traceback requests from the FCC, law enforcement and the registered traceback consortium and fully cooperate to the extent of our ability with investigation and prevention of illegal robocalls as necessary.

Telephone Number Authorization:

Smart Communications obtains all the telephone numbers used to serve the correctional facilities via third-party vendors, as Smart Communications has no access to direct numbering assignments. All outbound calls utilize numbers that are assigned to Smart Communications by their third-party vendor. Smart Communications is registered with the STI-PA using OCN 248L. 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.

Call Blocking:

Smart Communications' system is not designed to accept inbound calls. For outbound calls, if Smart Communications identifies any illegal calls originating from one of the correctional facilities they serve, they immediately notify the correctional facility as well as the appropriate law enforcement agency. Smart Communications reserves the right to suspend traffic if it suspects illegal calls or robocalls are being generated from the facility and works closely with the facility as well as their vendors to identify and mitigate any calls that may appear to be illegal robocalls.

Analytics for Monitoring Traffic:

The Company 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.

The various monitoring systems provide detailed reports that help identify suspected illegal calls and will send an alert if this type of activity is detected. No third-party vendors are involved in the monitoring process.

CONCLUSION

The Company submits this Robocall Mitigation Program consistent with FCC Regulations, 47 C.F.R. §64.6305 (a)(1) & (d)(5). Smart Communications will update its submission in the RMD within 10 business days of any change to the applicable information it must provide in the RMD, including its Robocall Mitigation Program.