

Movius Interactive Corporation Robocall Mitigation Plan

This Robocall Mitigation Plan is submitted by Movius Interactive Corporation pursuant to the provisions of 47 C.F.R. § 64.6305, adopted by the Federal Communications Commission (FCC) which require all “voice service providers” to establish a “robocall mitigation plan”. This document sets forth the Provider’s current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network. The Provider views these policies and procedures as constituting “reasonable steps” to avoid the origination of illegal robocalls on its network and in addition to following these steps the Provider commits to responding to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG), and to cooperate with such entities in investigating and stopping any illegal robocallers that may use its service to originate calls.

I. STIR-SHAKEN IMPLEMENTATION STATUS

As indicated in the FCC’s Robocall Mitigation Database, the Provider’s status with respect to STIR-SHAKEN implementation is as follows:

- Movius in conjunction with their partner provider have implemented the STIR/SKAKEN authentication framework all calls originating on its network are subject to the policies and procedures set forth in this Robocall Mitigation Plan which are intended to stop anyone from using the Provider’s service to originate illegal robocalls.
Presently, Movius relies on their partner network who are responsible for Caller ID Authentication and actioning any STIR-SHAKEN responsibilities to ensure that the calls are annotated correctly to enable correct classification this information is presented to Movius so that correct call handling is achieved.

II. TRACEBACK REQUESTS

As noted above, the Provider will cooperate with the FCC, law enforcement and the (ITG) on all traceback requests and investigations. To allow for timely and comprehensive law enforcement response efforts against illegal robocallers, the Provider will dedicate sufficient resources to promptly complete and provide responses to all traceback requests received from the FCC, law enforcement and/or the ITG, and commits to fully responding to any traceback

request received within 24 hours after receiving the same. Within **Appendix A** to this Plan, the Provider identifies a single point of contact for receiving all traceback requests.

As part of its efforts to assist in the successful traceback of illegal robocalls, the Provider will going forward include within its carrier interconnection and/or service agreements language requiring traceback cooperation on any voice service calls exchanged. In part, these related contract provisions will specify the need for parties to promptly identify the upstream provider from which a suspected illegal robocall entered its network or the customer of the service from which the call originated.

III. *CUSTOMER VETTING PRACTICES*

As a means of preventing or minimizing the origination of illegal robocalls through its voice services, Movius will use best practices in vetting the identity of all of its voice service subscribers. The subscriber vetting process is intended to help determine the legitimacy of a customer for the purpose of establishing a service relationship. Generally, Movius looks to confirm the identify of customers using its voice services through collecting information such as business name, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business. Movius efforts to vet business/commercial subscribers occurs during the process of provisioning the customer based on the services which have been contracted, executing the Provider's required service agreements, and granting the customer the right to use either Mobile or Fixed line telephone number resources. At Movius discretion, they may subject customers to an additional review, including a more stringent background check and possibly a site visit.

Further, with respect to meeting existing obligations to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls, Movius has the ability to block malicious calls in three ways, via our network provider, directly by Movius on our own platform, or end user can block the call using the "Block Caller" capability on the Multiline Application.

Movius utilizes service agreements and acceptable use policies as a means of preventing its new and existing subscribers from violating local, state, or federal laws, or to engage in deceptive or fraudulent activity. These documents governing use of Movius services include terms indicating specifically to all customers that their services should not be used for the purpose of making illegal robocalls, and Movius reserves authority within its service agreements to suspend or terminate a subscriber's voice service for violating applicable service-related terms.

Movius has established a routine process for monitoring of the usage and quality of its network facilities and conducts recurring and timely reviews of its call detail records (CDRs) to facilitate early identification of unusual or suspicious calling activity or patterns that may indicate use of the network for originating illegal robocalls. In those instances where the Provider identifies activity or a pattern consistent with illegal robocalls the customer will be contacted within twenty-four hours for further investigation and possible action regarding their subscribed to voice service.

IV. TELEPHONE NUMBER VALIDATION PRACTICES

Telephone Number Validation refers to the confirmation of the customer or end-user right to use a telephone number in connection with their subscribed voice service(s). In accord with industry best practices, the Provider has procedures in place to confirm the calling customer's right to use a telephone number. Specifically, a subscriber of the Provider's services is permitted to use a telephone number as their caller identity if a number is directly managed by the Provider and/or obtained by the Provider via an underlying partner.

V. INTERNATIONAL CALL ORIGINATORS

Movius provides international voice services via external providers, where they can instigate international calls using North American Numbering Plan resources.

Movius uses our US telecommunications partner to ensure full compliance and performing telephone number validation on all international originated calls.

VI. KNOW YOUR UPSTREAM PROVIDER PROCEDURES

As a provider of secure mobile voice services, the number of upstream providers within the United States is limited to a couple. The Provider has longstanding relationship with these upstream provider(s) and maintains its awareness of the nature of their businesses and the legitimacy of their call transmission services. Further, the Provider, in the interest of providing the highest quality services to all of its voice service customers, is committed to taking those steps necessary to ensure that any upstream provider providing connectivity are equally committed to monitoring their networks and preventing their use for the transmission of illegal robocalls. This includes the use of robocall prevention language in any contracts that the Provider may directly have with any upstream provider entities. Included as part of Appendix A to this Robocall Mitigation Plan document is a list of the Provider's current, immediate "Upstream Provider" along with contact information.

VII. ONGOING ROBOCALL MITIGATION PRACTICES

Movius and its provider(s) monitor the usage of its network and examines call detail records (CDRs) on a recurring basis for the purpose of detecting suspicious call activity and/or calling patterns. When network usage patterns consistent with illegal robocalls are detected or the Provider otherwise suspects illegal robocalling or spoofing is taking place on its network, it immediately seeks to identify the party that is originating, terminating, or routing these calls so that it may take appropriate action. The actions taken may include, but are not limited to: initiating a traceback investigation; verifying that the originating customer owns or is authorized to use the Caller ID number; determining whether the Caller ID name sent to a receiving party matches the customer's corporate name, trademark, or d/b/a name; terminating the party's ability to originate, terminate, or route calls on the Provider's network; and providing notice to law enforcement authorities.

As part of its Plan to mitigate and prevent any originating robocalls on its network, the Provider is committed to early identification and investigation of possible robocalling situations. In monitoring usage of its network, particular attention is given to: (1) higher than normal subscriber traffic volume including large bursts of traffic in small timeframes or inconsistent volumes of traffic (spikes in usage); (2) originating calls of short duration and low call completion percentages; (3) originating calls with sequential called to number dialing patterns; (4) repeated calls made to do-not-call registry or invalid numbers; and (5) calls to NPA-NXXs not assigned by the North American Numbering Plan Administrator.

Appendix A

Traceback Request Single Point of Contact:

Name: Bill Pettit

Title: Head of DevSecOps & IT & Compliance

Phone Number: +1 4048493545

Email Address: li@moviuscorp.com