

WebMagic, Inc.
Robocall Mitigation Plan
April 23, 2024

This Robocall Mitigation Plan is submitted by WebMagic Inc. (“Provider”), pursuant to the provisions of 47 C.F.R. § 64.6305, adopted by the Federal Communications Commission (“Commission”) which require all “voice service providers” to establish a “robocall mitigation plan”.

This document sets forth the Provider’s key 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 Commission, 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 Commission’s Robocall Mitigation Database, the Provider has implemented the STIR/SKAKEN authentication framework on its network and all calls are compliant with § 64.6301(a)(1) and (2). All calls originating on its network are subject to the policies and procedures set forth in this Robocall Mitigation Plan. Any prior certification has not been removed by Commission action and Provider has not been prohibited from filing in the Robocall Mitigation Database by the Commission.

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, and to cooperate with such entities in investigating and stopping illegal robocallers that use Providers service to originate calls.

III. KNOW YOUR CUSTOMER

Provider complies with the obligation to know its customers pursuant to § 64.1200(n)(3). Provider does not do business with anonymous customers, nor is Provider a foreign service provider. The majority of Provider’s customers have additional business relationships with Provider or its affiliates, beyond just call and other communication services. As such,

Provider tends to work with fewer clients but have deeper relationships with same than is the industry average. Provider is not currently providing voice network services to non-US customers.

Provider looks at its existing business relationship with a customer, and additionally collects information including but not limited to physical customer location, contact person(s), state of incorporation, federal tax ID number, and the nature of customer's business and calling purposes.

IV. BEST PRACTICES

Provider utilizes both technical blocks to potential network misuse as well as service agreements and personal communication that makes clear its expectations of customer behavior.

Provider's propriety security solutions monitor, trigger upon anomalies, and report unusual or suspicious activity including but not limited to watching for attempts to use Caller ID numbers that are not pre-authorized, higher than normal traffic volume or traffic spiking, originating calls of short duration, originating calls with suspicious number grouping, calls to invalid numbers, and other potential anomalies.

Customers are not allowed to use Provider's network in ways that would be in violation of local, state, or federal laws, to engage in deceptive or fraudulent activity, or to take any actions which might damage the reputation of Provider. Provider does not allow its network to be used for bulk marketing call purposes. Provider reserves authority within its service agreements to suspend or terminate service to a customer for violating service-related terms.

Provider works with a very small number of upstream providers, each of which are industry leaders in both size and reputation. The Provider has longstanding relationships with these upstream providers 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 its customers, is committed to taking those steps necessary to ensure that any upstream providers providing connectivity are equally committed to monitoring their networks and preventing their use for the transmission of illegal robocalls.

V. NO ENFORCEMENT ACTIONS

Provider (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has never been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging,

assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

VI. BUSINESS INFORMATION.

Provider:

WebMagic, Inc.
Attn: Greg McLemore
530 S. Lake. Ave. Ste. 450
Pasadena, CA 91101

626-794-5000 x110
robotcall-mitigation-database@webmagic.com

It is requested that anyone contacting Provider regarding Providers Robocall Mitigation Program and/or any potential abuse concerns to please email first (or writing to the physical address above) rather than calling first to achieve the best possible response time in an efficient manner. To ensure a response, please include your contact information as well as a clear description of why you are contacting Provider.

VII. CERTIFICATION

Provider certifies that the above is correct and true on the submittal date as noted above.

/Greg McLemore/

Greg McLemore
C.E.O.