

WORLDWIDE MARKETING SOLUTIONS

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN (RMP)

Pursuant to 47 C.F.R. § 64.6305, Worldwide Marketing Solutions Inc. (“WWMS”) submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. This report describes the status of its implementation of STIR/SHAKEN and the practices and procedures WWMS has in place to mitigate illegal robocalls. WWMS may modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time in order to respond to changes in its business, its capabilities and its needs.

WWMS has not been prohibited from filing in the Robocall Mitigation Database pursuant to a law enforcement action, and none of its prior certifications have been removed from the Database by the Commission.

WWMS has not been, at any time in the prior two years, the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with WWMS’s findings of actual or suspected wrongdoing due to it transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

STIR/SHAKEN IMPLEMENTATION

WWMS will comply fully with all conditions set forth in the FCC’S 2020 Report and Order mandating the implementation of the STIR/SHAKEN framework, as well as with the Commission’s rules and policies more generally.

WWMS is implementing STIR/SHAKEN through use of the Underlying Providers. This is a managed end-to-end call authentication solution that fully satisfies the FCC’s STIR/SHAKEN requirements. It provides a standardized approach to call authentication and verification (STIR – RFC 8224, RFC 8225, RFC 8226 and SHAKEN – ATIS-1000074-E, ATIS-1000080, ATIS-1000082).

WWMS has implemented this solution in the IP portions of its network by June 30, 2023. And the traffic is fully attested.

The Company’s Underlying Provider(s)/ Upstream Carriers are: Bandwidth.com, Vitelity and IDT who assess calls for the Company and then further attest and assign a level A certification to each call.

ROBOCALL MITIGATION PLAN

This Robocall Mitigation Plan describes the specific measures that the WWMS has implemented to detect and prevent illegal robocalls on its network as of June 30, 2023. The WWMS will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described. Should the WWMS determine that changes are appropriate, its practices may differ from those described below.

Risk Assessment. WWMS is a voice service provider offering a variety of voice calling services. Its customers generally do not originate high volume calls and WWMS has not received information suggesting that robocalls are originated on its network. Therefore, WWMS does not consider its network at high risk of originating illegal robocalls.

SPECIFIC MEASURES TO IDENTIFY AND PREVENT ILLEGAL ROBOCALLS

Customer Due Diligence: WWMS conducts due diligence on new and renewing customers, confirming the customer's identity and, if it is a business, is incorporation documents. The WWMS confirms the customer's service address for all customers.

- WWMS verifies customer's business reputation prior to providing service.
- WWMS verifies customer information when contracts are renewed or services are added.
- WWMS verifies the customer's identity and their right to use the telephone number presented on calls.
- WWMS has the policies that define the circumstances by which it will deny, suspend or terminate service to a customer.

Direct IP Intermediate Carrier Due Diligence: WWMS takes appropriate steps to know the immediate service provider to ensure that the immediate upstream provider is not using it to carry or process a high volume of illegal traffic.

Measures to Prevent or Avoid the Origination of Illegal Robocalls

- WWMS has in place an enforceable terms of use and/or an acceptable use policy. WWMS also has in place policies designed to detect and prevent fraudulent traffic on its network.
- WWMS uses analytics and technologies and services to monitor traffic on its network and identify potentially unlawful call origination activity. If WWMS has a reasonable basis to believe that a customer is originating illegal robocalls, it will require the customer to remedy the problem and, if effective action is not taken, WWMS can suspend and/or terminate service to the customer.
- WWMS verifies that the direct intermediate carriers that are used by WWMS are in the FCC RMD and does not accept traffic from intermediate carriers who are not in the RMD.
- WWMS blocks the following types of calls by default with such calls that are originating from invalid numbers per FCC Order 2017 Call Blocking Order and calls from DNO numbers as per FCC Order 2017 Call Blocking Order.
- WWMS also blocks the following types of calls:

- ✓ Describe any blocking based on FCC safe harbors – analytics, network-based blocking, etc.
- ✓ Describe any other blocking policies.
- ✓ As an originating service provider and/or intermediate carrier that is immediately downstream from a bad actor, will block traffic from the bad actors when notified by the commission

Responding to Traceback Requests

- WWMS has designated an individual as a dedicated point of contact for addressing traceback requests, and a backup person to that individual. It either has provided the ITG with the contact information and business hours for those individuals or will do so upon receipt of the first request from the ITG. See <https://www.ustelecom.org/the-industry-traceback-group-itg/for-providers/>
- WWMS will respond within 24 hours of receipt of traceback request to inquiries received from the Industry Traceback Group. If a pattern of questionable activity is detected, WWMS will require its customer to remedy the problem and, if effective action is not taken, service to the customer may be suspended and/or terminated.

Cooperation with State and Federal Regulators

WWMS will cooperate with state and federal regulators to prevent any and all illegal robocalls. Specifically, WWMS will:

- Respond to valid law enforcement requests;
- Provide relevant non-proprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities; and
- Implement mandated robocall mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls.

WWMS has deployed call authentication, call labeling, and call blocking services provided by the Company's Underlying Provider. We have made great strides to protect our networks and consumers from harmful calls. WWMS is pleased to play a role in that improvement and will continue the necessary work to protect our customers.

WWMS Networks primary place of business is:

12194 SW 25th Court, Miramar, FL, 33025

Address

City, State, Zip

Phone: +1(305)614-4472

Website: <https://mitelefono.com>, <https://wwmsolutions.com>

Leaders of the _____ are:

CEO

Name: Arturo Ayala
Address: 12194 SW 25th Court, Miramar, FL, 33025
City, State, Zip
Phone: +1(305)614-4468
Email: aayala@wwmsolutions.com

CTO

Name: Guillermo Cuppers
Address: 12194 SW 25th Court, Miramar, FL, 33025

City, State, Zip
Phone: +1(305)614-4469
Email: gcuppers@wwmsolutions.com

Designated RMD Contact:

Name: Cesar Davalos
Address: 12194 SW 25th Court, Miramar, FL, 33025
City, State, Zip
Phone: +1(305)873-8831
Email: cdavalos@wwmsolutions.com

MEASURES TO PREVENT ORIGINATION OF ILLEGAL CALLS:

Know Your Customer:

WWMS has a rigorous KYC policy for the in order to support the Business Customers that it sells and resells services to. WWMS has an in-depth presales process where representatives of WWMS work with the prospect or customer to understand all the unique factors of the Customer's business. The objective of this is twofold: a. to get to know the customer; and b. to provide the best possible service to the customer by fully understanding all facets of their business.

WWMS performs a thorough reputation check on each of its customers and verifies the following information: legal business name, legal form of business, federal tax ID, nature of the business, primary contact person, and service address.

Not only does WWMS have a rigorous intake and Onboarding process where it secures extensive information for Customers but all relationships between WWMS and customers are governed by an MSA which specifically states the business Customer is not able to resell any services which the WWMS resells and the services which are sold to the Customer are strictly for the Customers own internal use.

.