

Robocall Mitigation Plan

Business Information

M2ngage Telecommunications II Corp.
1025 Old Country Road
Suite 223
Westbury, NY 11590

Contact for Robocall Mitigation Issues

Vincent DePalo
CEO
(212) 675-7979
vincent@thetelecomcompany.com

Overview

In the Commission's 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) ("R&O") it is stated that all voice service providers ("VSPs") must file robocall mitigation plans ("RMPs") that, among other things, outlines "reasonable steps" taken to avoid originating illegal robocalls.

In addition to the "reasonable steps," the FCC requires that a RMP include:

- "know your customer" procedures;
- "know your upstream provider";
- ownership information;
- a description of any call analytics system used to identify and block illegal traffic; and
- whether a third-party vendor is used and if so, the name of the vendor.

The FCC previously stated that a RMP is sufficient if the detailed practices in the plan can reasonably be expected to significantly reduce the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

Purpose

M2ngage Telecommunications II Corp. ("M2") is a small VSP dedicated to stopping illegal calls from originating in our network and monitoring the calls traversing our network. As certified in the FCC's Robocall Mitigation Database, M2 has fully implemented STIR/SHAKEN. In compliance with the R&O, M2 submits this RMP and certification.

Know Your Upstream Providers

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls Call Authentication Trust Anchor, Seventh Report and Order In CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking In CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59* (Rel. May 19, 2023) ¶¶ 49-51, M2 provides the following information concerning its upstream voice service carrier:

Bandwidth Inc.
2230 Bandmate Way
Raleigh NC 27607
Stephen Thayer
voicesecurity@bandwidth.com

To the extent that M2 were to receive information from law enforcement or other sources that a customer is engaged in illegal robocalling, our policy is to cooperate fully, including providing the identity of any suspected illegal robocaller, pursuant to legal service or process. While M2's agreement with its upstream provider contains no provisions specific to robocall mitigation, M2 has received assurances from them that they have, and will continue to, sign calls transmitted to M2 and will abide by the FCC's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic.

Know Your Customers

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber. A subscriber is an entity that has a business relationship with M2 in which we transmit, originate, and/or terminate calls based on behalf of the subscriber. M2's KYC program involves obtaining specific subscriber information when a subscriber signs up for services. This process includes collecting such information such as:

- physical business location;
- contact person(s); and
- valid credit card information.

Acceptable Use Policy

M2 maintains an Acceptable Use Policy ("AUP") that subscribers must agree to before being permitted to use M2's network. The M2's AUP is found at <https://m2ngage.com/acceptable-use-policy/>.

Monitor Traffic with Analytics

M2 utilizes a system that flags suspicious activity in real time and alerts our team to respond. Examples of suspicious activity include:

- Anomalies in cost generated by calls from a single customer;
- multiple overlapping calls on the same account is a risk of not having a single subscriber using the service;
- velocity on initiate calls (synchron intervals, quick dialing back-to-back calls);
- recent volumes (last 60 min) vs weekly trends;
- number of unique destination numbers in a time frame (total account level);
- number of unique source numbers in a time frame (total and account level); and
- anomalies in call duration distribution (most calls having similar duration is not representative for residential service usage).

M2 does not work with third party vendors to deploy its analytics.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, M2 uses various procedures to investigate any suspicious activity:

- checking recent and past call detail records and benchmark against expected trends;
- checking recent and past account activity and purchases;
- investigating if any system issue generates the strange behavior;
- verifying that the call originating path is valid; and
- contacting the subscriber to understand his particular use case and validate that the activity belongs to that subscriber.

M2 follows Industry Traceback Group ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, M2 will devote sufficient resources to provide prompt and complete resources to traceback requests. M2 **certifies that it will comply with traceback requests within 24 hours of receiving same.**

M2 will investigate suspicious activity found by its monitoring systems or reported to M2 by subscribers or third parties. The investigation could potentially result in opening a traceback request or with M2 contacting a subscriber to correct improper use of the platform, or, if the subscriber does not respond or comply, to block their use of the platform.

Blocking

M2 will implement Do Not Originate requests it receives from the ITG. M2 works with its upstream carrier to block suspicious calls. If M2's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, M2 will take appropriate action which may include suspending or terminating the subscriber's use of M2's network. M2 will cooperate with investigative bodies (provide a single point of contact to address traceback requests from law enforcement (including state attorneys general offices), the FCC, or ITG; as well as documenting requests & actions taken in response thereto.

Plan Updates

This plan and industry best practices must evolve to response to the dynamic nature of mitigating illegal robocalling. M2 will monitor industry best practices and continuously improve our internal processes to ensure this plan and our system adapt to this ever-changing issue.

In the event of any material change to this plan, M2 will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.

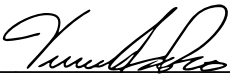
Certification of Vincent DePalo

I, Vincent DePalo, Chief Executive Officer of M2ngage Telecommunications II Corp. ("M2") do hereby certify, under penalty of perjury, the following:

- a. M2 has fully implemented STIR/SHAKEN in the IP portions of its network.
- b. M2's business name and primary address are as follows:

M2ngage Telecommunications II Corp.
1025 Old Country Road
Suite 223
Westbury, NY 11590

- c. M2 has one other business name in use: The Telecomcompany.
- d. M2 has not previously used any other business name except The Telecomcompany.
- e. The name, title, department, business address, telephone number, and email address of the individual responsible for addressing robocall-related issues are listed in the above robocall mitigation plan.
- f. M2 has one owner: Allied International Fund Inc., which owns 100% of the company.
- g. M2's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
- h. M2 and its interest holder have not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- i. M2 and its interest holder have not subject been to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- j. M2's Operator Code Number is 304K.



Vincent DePalo