



WiMacTel, INC.
13515 I Circle
Omaha, NE

Robocall Mitigation Plan for WiMacTel, Inc. (“WiMacTel”)

WiMacTel is a provider of operator services, directory assistance, collect calling, and other services (“OSP”) on behalf of third-party Telecommunications Service Providers (“TSP”). OSP calls are accepted by WiMacTel via SIP on a direct connected network or through SIP trunking via a wide area network. The calls forwarded to WiMacTel for OSP services do not originate from the Public Switched Telephone Network (“PSTN”) or via toll free.

When a call comes to WiMacTel, WiMacTel provides the OSP services for which it has been contracted to provide for the TSP. For example, if a customer of a TSP is looking for directory assistance, the TSP will send the call to WiMacTel who fulfills the customer’s request. If a customer requests a collect call, WiMacTel will put the call back to the network of the TSP through the same IP links from which the call was sent to WiMacTel and the TSP terminates the call. If WiMacTel is required to terminate the call, it does so as a reseller of its underlying carrier, TELUS.

Given that a portion of WiMacTel’s OSP services is provided simply as a feature service, STIR/SHAKEN regulations would not be applicable, because WiMacTel neither originates nor terminates the call. In those instances where WiMacTel is required to actively terminate a call to the called party, the call is sent through WiMacTel’s underlying network provider, TELUS. WiMacTel would therefore be deemed a reseller, and STIR/SHAKEN obligations would not apply. However, WiMacTel would be obligated to submit, and through this filing is submitting its Robocall Mitigation Plan.

WiMacTel commits to respond to all trace back requests from the FCC, law enforcement, the US Telecom Industry Traceback Group (ITG) and all other responsible entities, and will cooperate fully in investigating and stopping any illegal robocallers that use its service to originate calls. WiMacTel has a designated single point of contact to address tracebacks to

expedite the process to adhere to the 24-hour response time requirement.

WiMacTel Communications process to manage any critical issues is through our TAC (technical assistance center) - we have included the document that provides specifics around the TAC.

TAC - Phone: 1-855-798-6884 • E-mail: tac@WiMacTel.com • Self Service Portal: <https://tac.WiMacTel.com>

WiMacTel has taken the following steps to detect originating robocall traffic:

WiMacTel will monitor call thresholds during regular business hours and system logs are reviewed daily in order to identify suspicious calling activities.

WiMacTel has taken the following steps to prevent illegal originating robocalling traffic:

- A. Procedures are put in place to confirm the identity of new commercial customers by collecting information such as physical business location, contact person(s), state and country of incorporation, Federal Tax ID, general nature of the customer's business, names of all of the officers and directors of the business, public research into the history of the company, including public complaint data on other business reputation data, officers/directors and any other business in which they may be involved.
- B. WiMacTel's Acceptable Use Policies (AUP), Terms and Conditions and Terms of Service are contained in the carrier/service contracts with WiMacTel's customers and in certain instances are placed on its website. The information will be updated to reflect our stance on robocalls.
 1. Each new carrier customer of WiMacTel must sign a Service Contract. Within the Service Contract is incorporated a reference to the AUP under which the customer is obligated. The customer must sign a Service Contract, or it will not be permitted to use WiMacTel's service. Among other things, WiMacTel's AUP and service contracts prohibits:
 - (i) providing deceptive or false information about the identity of the sender or the origin of a message or phone call;
 - (ii) violating any applicable local, state or Federal law;
 - (iii) violating any applicable industry acceptable guidelines;
 - (iv) using WiMacTel's service to engage in or in connection with fraudulent activities;
 - (v) requiring carrier/service customers to participate in any US Telecom or ITG

traceback request.

2. WiMacTel's contractual terms with subscribers specify that WiMacTel may take action, up to and including suspension or termination of service, for violation of the AUP.
- C. WiMacTel will maintain participation in the FCC Robocall Mitigation Database (RMD) and will adhere to its guidelines and best practices.
- D. WiMacTel has not been subject to any investigation by Committee or other law enforcement agencies or requests to provide ITG Traceback, Robocall assistance to our originators in the prior two years.

INVESTIGATE SUSPICIOUS ACTIVITY:

WiMacTel regularly examines and analyzes its traffic make-up. If the analysis indicates the presence of likely illegal robocalling, management is alerted and defined procedures are followed on investigating the party who is generating the suspicious traffic.

The procedures include but are not limited to:

- Responding to any Traceback or other requests by VSP's on robocalls within 24 hours.
- Checking recent and past call detail records and benchmarking them against expected trends
- Checking recent and past account activity and purchasing
- Investigating if any system issue generates the abnormal traffic patterns
- Verifying that the call originating path is valid
- Contacting the customer to understand its particular use case and validate that the activity belongs to that customer

BLOCKING:

WiMacTel implements Do Not Originate requests it receives from the Industry Traceback Group.

PLAN UPDATES:

This plan and industry best practices will evolve to respond to the dynamic nature of mitigating illegal robocalling. WiMacTel will monitor industry best practices and

continuously improve its internal processes to ensure this plan and our systems adapt to ever-changing issues.

In the event of any material changes to this plan, WiMacTel will republish this plan to its employees, consultants and contractors and file such an update with the FCC Robocall Mitigation Database.

All questions, inquiries or notices regarding this plan should be sent to Craig Needels at cneedels@viiz.com.

Sincerely,

[Craig A Needels](#)

VP – Technology and Operations