

ImOn Communications Robocall Mitigation Plan

This Plan is also applicable to the following voice service providers/carriers which are ImOn Communications wholesale customers (receiving network switching and certain other carrier support services, including Third-Party Call Analytics Services)

**Indianola Municipal Utilities
Board of Water Electric and Communication aka Muscatine Power & Water
Vinton Municipal Communications Utility
The Municipal Communications Utility of The City of Cedar Falls
Waverly Utilities
City of Pella
Waterloo Municipal Communications Utility dba Waterloo Fiber.**

This Robocall Mitigation Plan is submitted by and for ImOn Communications (hereinafter referenced as “ImOn” or the “Provider” and also for the above referenced voice service providers (hereinafter referenced as “Wholesale Customer(s)”) 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 from Provider’s end users and also end users of its Wholesale Customers. The Provider and Wholesale Customers view these policies and procedures as constituting “reasonable steps” to avoid the origination of illegal robocalls and in addition to following these steps the Provider and/or Wholesale Customers commit 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, ImOn’s status with respect to STIR-SHAKEN implementation is as follows:

- ImOn has implemented the STIR/SHAKEN authentication framework on a portion of its network and calls it originates on that portion of its network are compliant with 47 CFR § 64.6301(a)(1) and (2). In addition, ImOn has established the policies and procedures set forth in this Robocall Mitigation Plan which are intended to stop anyone from using its network or services to originate illegal robocalls.

Presently, ImOn relies on the continuing extension from STIR-SHAKEN implementation provided under 47 CFR § 64.6304 (d) which exempts from STIR-SHAKEN Caller ID Authentication those portions of a voice service provider network that rely on technology which is unable to initiate, maintain, carry, process, and terminate interconnected VoIP

calls. More specifically, although all of ImOn's network facilities are at this time IP capable and able to originate and deliver VoIP calls, certain of its upstream provider(s) receiving originated local or interexchange voice traffic are only offering non-IP connectivity for such traffic – no IP connectivity is currently available from these upstream provider(s) enabling the continued transmission of all of Provider's VoIP traffic in Session Internet Protocol (SIP), with a continued transfer of STIR-SHAKEN attestation data.

Imon's wholesale customers, listed above and made a part hereof, do not have a STIR-SHAKEN implementation obligation as they do not have control or ownership of the voice network infrastructure. The wholesale customers all understand and acknowledge the responsibility to use best practices under III. Customer Vetting.

II. TRACEBACK REQUESTS

As noted above, 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 use of Provider's network and services the Provider and its Wholesale Customers, named above, accept responsibility for and will use best practices in vetting the identity of their voice service subscribers, whether a residential or business/commercial subscriber (including any entities that are purchasing services for resale). The subscriber vetting process is intended to help determine the legitimacy of a customer for the purpose of establishing a business relationship. Generally, Provider and its Wholesale Customers look to confirm the identify of customers using their voice services through collecting information such as physical customer location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business. Provider and Wholesale Customer efforts to vet residential and business/commercial subscribers occurs during the process of provisioning customer requested services (for example in appropriately sizing the facilities to their claimed intended use), executing the Provider or Wholesale Customer service agreements, and granting a subscriber the right to use telephone

number resources. Commercial end users, comprised of larger businesses with more complex service configurations, are generally recognized as presenting a higher risk of perpetrating illegal robocalls and thus those customers, at the Provider's or Wholesale Customer's discretion, may be subject to an additional review, including a more stringent background check and possibly a site visit. The Provider also understands the special importance of vetting any wholesale customers it may have. If necessary, Provider may vet identity information for its wholesale customers by confirming whether the customer is an FCC Form 499-A filer in the FCC Form 499-A Filer database or in the FCC's Intermediate Provider Registry. If the customer is not registered within those databases further investigation is conducted to better understand the nature of the customer's business.

Further, with respect to meeting existing obligations to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls, the Provider and/or its Wholesale Customers:

- Utilize service agreements and acceptable use policies as a means of preventing new and existing subscribers from using their voice services in ways that would be in violation of local, state, or federal laws, or to engage in deceptive or fraudulent activity. These documents governing use of Provider and Wholesale Customer provided services include terms indicating specifically to all customers that their services should not be used for the purpose of making illegal robocalls, and the Provider and Wholesale Customers reserve authority within their service agreements to suspend or terminate a subscriber's voice service for violating applicable service-related terms.
- Provider in monitoring the usage on its network watches specifically for unusual or suspicious calling activity or patterns that may indicate use of the network for originating illegal robocalls. In those instances where the Provider and/or Wholesale Customers identify activity or a pattern consistent with illegal robocalls the customer will be contacted as soon as possible 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 or the Wholesale Customer'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. Further, for: (1) single line voice service subscribers, both services connected via TDM or IP, the switching equipment has been set up to only accept calls from the number assigned to that subscriber; and (2) subscribers with multi-line telephone systems, for both services connected via TDM or IP, all originating calls are automatically screened and such will only be connected if the originating number matches

one of the numbers assigned to the subscriber. These screening capabilities enable an automated and secure method of validating originating telephone numbers.

If a business with a multi-line telephone system has a legitimate business need to send a caller ID which they do not own, they will be allowed to send any valid caller ID. ImOn requires a written justification and customer acknowledgement of the acceptable use policy. Sample business cases might be an off-hours voicemail forward which presents the original caller ID to an on-call technician's cell phone, or a company that has multiple voice providers and sends a caller ID owned by the other provider.

V. INTERNATIONAL CALL ORIGINATORS

The Provider is not currently an international voice services provider. If at any time the Provider does sell its services to customers which are international call originators using North American Numbering Plan resources, it will familiarize itself with and develop best practices for fulling vetting such customers and performing telephone number validation on all international originated calls.

VI. KNOW YOUR UPSTREAM PROVIDER PROCEDURES

The Provider has longstanding relationships with its 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 all of its voice service 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. 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(s)" along with contact information for each.

VII. ONGOING ROBOCALL MITIGATION PRACTICES

When network usage patterns consistent with illegal robocalls are detected or 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, ImOn is committed to identification and investigation of possible robocalling situations. ImOn gives particular attention when finding higher-than-normal subscriber traffic volumes including large bursts of traffic in small timeframes or inconsistent volumes of traffic (spikes in usage).

VIII. ADDITIONAL CERTIFICATION RELATED INFORMATION

ImOn and all wholesale customers also certify entities have not been prohibited by the Commission from filing in the Robocall Mitigation Database and that none of its prior certifications submitted in the Robocall Mitigation Database have been removed by Commission action.

Appendix A

Traceback Request Single Point of Contact:

Name: ImOn NOC
Title: Network Operations Center
Phone No: 319-261-2673
Email Address: noc@imon.net

Upstream Provider Information:

Name of Upstream Provider: Aureon
Nature of Business: Tandem Switch Provider
Network Location of Upstream Provider: West Des Moines, Iowa
Title: Switch Engineer
Phone Number: 515-830-0478
Email Address: tech.help@aureon.com

Name of Upstream Provider: Sinch
Nature of Business: LD Provider
Network Location: Chicago and other
Name of contact: Stacy Graham
Phone: 952-314-1317
Email of contact: stacy.graham@sinch.com

Name of Upstream Provider: Peerless
Nature of Business: LD Provider
Network Location: Chicago IL
Name of Contact: Virginia Bodyfelt
Title: Regulatory Affairs
Email: Regulatory@peerlessnetwork.com

Call Analytics Vendor Name and Description of System:

Name of Vendor - TransNexus

Description of the call analytics system

ImOn utilizes a third-party “Analytics” platform provided by TransNexus to support the effectiveness of its Robocall Mitigation Plan. This includes, as examples, the use of “Telecom Fraud Prevention” and “Robocall and Telephone Denial of Service (TDos) Prevention” services, which include more specifically the use of the following methods/tools as a means of preventing and blocking fraudulent and illegal robocalls on its network: the use of CDRs and related reports for determining mitigation actions; use of SIP Analytics enabling real time traffic analysis and detection and mitigation of robocalls at origination; use of blacklisting and whitelisting to mitigate calls with specific attributes; use of CAPTCHA gateway services to distinguish whether calls are from humans or autodialers; use of a “Shield” database that screens calls at origination for calling numbers that are invalid, high-risk, or appear on “Do Not Originate” lists; and use of reputation look up services on calling numbers at origination.