

Robocall Mitigation Plan

This Robocall Mitigation Plan is submitted by **BMI Telecom** 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 **BMI Telecom's** current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network. **BMI Telecom** views these policies and procedures as constituting “reasonable steps” to avoid the origination of illegal robocalls on its network. In addition to following these steps, **BMI Telecom** commits 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, **BMI Telecom's** status with respect to STIR-SHAKEN implementation is as follows:

- **BMI Telecom** has not implemented the STIR/SHAKEN authentication framework on any portion of its network, and all calls originating on its network are subject to the policies and procedures set forth in this Robocall Mitigation Plan, which are intended to stop anyone from using the service to originate illegal robocalls.
- Presently, **BMI Telecom** 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's network that rely on technology that cannot initiate, maintain, carry, process, and terminate SIP.

II. Traceback Requests

BMI Telecom 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, **BMI Telecom** will dedicate sufficient resources to promptly complete and provide responses to all traceback requests received from the FCC, law enforcement, and/or the ITG. **BMI Telecom** commits to fully responding to any traceback request received within 24 hours after receiving it. Appendix A identifies a single point of contact for receiving all traceback requests.

III. Customer Vetting Practices

To prevent or minimize the origination of illegal robocalls through its services, **BMI Telecom** uses best practices in vetting the identity of its voice service subscribers. These practices include collecting information such as physical location, contact persons, state or country of incorporation, federal tax ID, and the nature of the business. **BMI Telecom** also conducts regular monitoring of network traffic and investigates any unusual or suspicious activity.

IV. Telephone Number Validation Practices

BMI Telecom uses industry best practices to confirm the right of customers to use telephone numbers associated with their services. The company only allows calls from numbers assigned to the subscriber, ensuring secure and valid caller identity.

V. International Call Originators

Currently, **BMI Telecom** does not provide services to international call originators. If the company begins selling services to international customers, it will implement appropriate vetting and validation procedures.

VI. Know Your Upstream Provider Procedures

BMI Telecom maintains relationships with its upstream providers and ensures that they are committed to monitoring their networks to prevent the transmission of illegal robocalls. Contractual language concerning robocall prevention is included in agreements with upstream providers.

VII. Ongoing Robocall Mitigation Practices

BMI Telecom regularly monitors its network for suspicious calling activity and investigates any instances of potential illegal robocalls. The company takes appropriate action, including traceback investigations and the suspension of services for violators.

VIII. Third-Party Analytics

BMI Telecom uses third-party analytics to prevent illegal robocalls. These systems include fraud prevention and robocall blocking tools, such as blacklisting, whitelisting, and SIP analytics for real-time traffic monitoring.

Appendix A

Traceback Request Single Point of Contact:

Name: Ilia Lazarev

Title: CEO

Phone Number: +37166103061

Email Address: support@bmi.io

Upstream Provider Information:

Name of Upstream Provider: DIDWW

Nature of Business: Wholesale Provider

Network Location of Upstream Provider: Dublin, Dublin, Ireland

Contact Name: Gintare Laurinaitiene

Title: Sales Assistant

Phone Number: +1 (718) 766 7744

Email Address: gintare.l@didww.com

Call Analytics Vendor: VoIP Monitor

Name of Vendor: VoIP Monitor

Description of System: BMI Telecom utilizes a third-party “Analytics” platform provided by VoIP Monitor to support the effectiveness of its Robocall Mitigation Plan. 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.