

Global Net Communications , Inc.
Robocall Mitigation Plan
V.1 February 2024

STIR/SHAKEN IMPLEMENTATION

Global Net Communications, Inc. (“Global Net” or “Company”) is a small voice service provider (“VSP”), providing managed data solutions to service providers and enterprise customers, with access to their own numbers from NANPA. Global Net has fully implemented STIR/SHAKEN and on October 19, 2022 submitted its certification that all voice traffic that originates on its network is authenticated with STIR/SHAKEN consistent with 47 C.F.R. §64.6301(a). Global Net has implemented a Robocall Mitigation Program (“RMP”) to include the obligations outlined in the Commission’s recent 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). In compliance with the Report & Order, Global Net submits this RMP and certification into the Robocall Mitigation Database.

ROBOCALL MITIGATION

Background

The FCC Order requires that a RMP include the following affirmative obligations for voice service providers:

- Outline reasonable steps VSP has taken to avoid originating illegal robocall traffic;
- Commitment to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls;
- Know Your Customer procedures;
- Describe any call analytics system used to identify and block illegal traffic

Traceback:

Global Net commits to responding fully and within twenty-four (24) hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperating with such entities in investigating and stopping any illegal robocallers that may be using our service to carry or process calls. Traceback monitoring and examination is conducted on no less than a weekly basis. Global Net retrieves logs from our SBCs and Class 5 switches and checks the subscriber’s live CDRs. The Company focuses on call volume, call velocity, call duration and, if needed, checking how many numbers the subscriber dialed that were disconnected.

Traceback Contact Information

Name	Title	Contact Information
Christian Banister	President	480-503-9298
Scott Lake	Director of Operations	480-503-9298

Measures to prevent origination of illegal calls.

Know Your Customer:

Global Net has implemented affirmative, effective measures to prevent new & renewing customers from using its network to originate illegal robocalls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal calls. Global Net has implemented Know Your Customer (“KYC”) protocols when onboarding new or renewing customers. These protocols include screening interviews, verifying the customer’s full legal name, state or county of incorporation, physical address of its operations, and federal tax ID. The Company also checks the applicant’s LOA information against public databases, including ownership and business qualifications filed with the Secretary of State Authority. The Company also checks for any prior or current litigation involving fraudulent activities, as well as scrutinizing the submitted bill copies. The LOA is utilized as well as requesting a copy of the potential subscriber’s current telephone invoice. The Company does not use any third-party validation services currently.

Validating Customer’s Right to Use Telephone Numbers:

Global Net has procedures in place to authenticate the proper use of telephone numbers associated with calls routed over its network. In cases where the call utilizes a number that is not directly assigned to Global Net, the customer must agree to additional contractual terms governing their traffic and use of their phone numbers. Global Net’s standard service order contains language prohibiting the misuse of telephone numbers.

Call Blocking:

The Company analyzes and monitors all call traffic that originates on its network to identify behaviors that are consistent with illegal robocalling. If the Company identifies such calling patterns, it will take appropriate action to address these behaviors, including blocking such calls. As part of its analysis and monitoring of network traffic, it has implemented a process to block calls from providers not registered in the Robocall Mitigation Database (“RMD”). The RMD is monitored weekly for updates. The Company’s process incorporates a list of OCNs that are identified as needing to be blocked and will block any calls received from these OCNs.

Acceptable Use Policy

The Company has prepared a Terms of Use as a guide for its customers to understand the intended and permissible uses of our service, and to prevent exploitation, fraud, and abuse of our calling plans and features.

Analytics for Monitoring Traffic:

Global Net's SBC and Class 5 switches have SNMP traps set up to monitor in real time the outbound voice traffic to prevent the origination of illegal robocalls. These SBCs and switches provide detailed reporting which identify suspected illegal robocalls and will send an alert in situations where the calling number is invalid or is unallocated. Additionally, we monitor current call volume, call velocity, as well as recent call durations to aid in identifying suspect activity on the network.

CONCLUSION

The Company submits this Robocall Mitigation Program consistent with FCC Regulations, 47 C.F.R. §64.6305 (a)(1) & (d)(5). Global Net will update its submission in the RMD within 10 business days of any change to the applicable information it must provide in the RMD, including its RMP.