

Robocall Mitigation Plan

1. Freshphone has implemented STIR/SHAKEN and will respond to all traceback requests from the Federal Communications Commission, law enforcement and the industry traceback consortium and to cooperate with such entities in investigating and stopping any illegal robocalls from using its services to original calls. All voice traffic that originates on our network is subject to this robocall mitigation program.
2. Freshphone controls the configuration of inbound and outbound routes to prevent number spoofing.
3. Freshphone limits the connections to prevent autodialing and other robocall technology from utilizing our services. Our systems provide insight if a customer is exceeding reasonable utilization so that we can restrict unauthorized use.
4. Freshphone screens all customers and have in-depth knowledge of the business utilization of their phone system to prevent unauthorized use. This always involved a conversation between someone at Freshphone and someone at the business. In this way, we verify customers are who they say they are. Our terms of service prohibit its use for fraudulent activity and prohibit any resale of our services. Any customer that is determined to have violated the terms of service will have their account terminated.
5. Freshphone systems provide inbound number blocking capability. Our systems are configured to automatically block certain types of robocalls. They also provide tools for customers to report and block any calls that get through.
6. Freshphone only accepts off network traffic for termination from third party carriers that are in the Robocall Mitigation Database.

If there are any questions or concerns regarding this plan, please contact Freshphone.



Joel Kallman

CEO

Freshphone, Inc.