

Interactive Services Network, Inc.
Robocall Mitigation Program
V.2 February 2024

STIR/SHAKEN Implementation

Interactive Services Network, Inc. dba IPFone("IPFone" or "Company") is a small voice service provider ("VSP") with less than 100,000 voice service subscriber lines. IPFone 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, IPFone 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

IPFone 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 use its service to originate calls.

Traceback Contact Information

Name	Title	Contact Information
Samuel Madeh	Carrier Management	814-601-0219 carriermanagement@ipfone.com

IPFone utilizes the following procedures, working with its DID vendors, to conduct the investigations and to determine if the calls are actually illegal robocalls:

ORIGINATING CALLS

- For all incoming traffic, our DID vendors have fully implemented STIR/SHAKEN to sign the calls with full attestation and secure the identity of the calls.

-

OUTBOUND CALLS

- For all outgoing traffic, our underlying long distance carriers have also fully implemented STIR/SHAKEN and will sign IPFONE's calls with A and/or B attestation to make our calls traceable back to us in the case of any abuse scenario.

[Call Blocking/Analytics for Monitoring Traffic:](#)

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 situations, including blocking such calls. As part of its analysis and monitoring procedures, we work closely with our DID vendors and terminating providers, we are able to collect call data from those providers as well as our own CDRs from our softswitch so that we can immediately block any calls originating within our network that are identified as robocalls.

[Know Your Customer](#)

IPFone 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. IPFone has implemented Know Your Customer ("KYC") protocols when onboarding new or renewing customers. These protocols include:

- * Confirming the identity of new commercial VoIP customers by collecting information such as physical business location, contact person(s), state or county of incorporation, federal tax ID, and the general nature of the customer's business.

[Validating Customer's Right to Use Telephone Numbers:](#)

IPFone has procedures in place to authenticate the proper use of telephone numbers associated with calls routed over its network. IPFone assigns customers numbers that are registered to IPFone. However, in instances where the call utilizes a number that is not directly assigned to IPFone, the following procedures are followed:

- Check the logs of its softswitch to confirm the call was received. After that, we check Broadworks XSLog and then verify it with our DID vendor, Bandwidth.

- The Company also uses a proprietary Fraudcheck system to verify that the calls were legitimately placed by our customers, which allows the Company to:
 - * Prevent our users from calling too many numbers in a certain amount of time
 - * Prevent users from calling numbers previously involved in fraud.
 - * Block those lines/DIDs/users we suspect have been hacked
 - * Block any line/DID/user should its outgoing traffic be deemed illegal
 - * Record the fraudulent events to take all measures to avoid future events of fraud
 - * Notify customers and support them –should it be needed- when illegal activity is detected.

Acceptable Use Policy

The Company has specific Terms and Conditions within the customer contract to aid 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. These terms include a section on “unauthorized use of services” that allows the Company to take the appropriate action it deems appropriate (to include blocking calls) to prevent any fraud or misuse of the network, which includes the detection of illegal robocalls.

CONCLUSION

The Company submits this Robocall Mitigation Program consistent with FCC Regulations, 47 C.F.R. §64.6305 (a)(1) & (d)(5). IPFone 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.