

ROBOCALL MITIGATION PLAN

Know Your Customer

SIPSTATUS Communications has a strong KYC policy with procedures that enable us to better evaluate and understand our customers.

We always verify the identity of our potential customers and scrutinize the contractual documents before starting any business.

All traffic from existing customers is monitored continuously for patterns of known abuse.

We have implemented risk management procedures to identify, evaluate and prioritize risks and we take immediate action when it comes to preventing robocalling or other forms of fraud.

Trace-back & Compliance

We will respond to all trace-back requests from the Commission, law enforcement, and the registered trace-back consortium and will cooperate with such entities in investigating and stopping any illegal robocallers that use our service.

STIR/SHAKEN

We are a carrier, not an operator so, since we do not have any subscribers, there is no traffic originated from our network. Still, all voice traffic that passes through our network is subject to the robocall mitigation program described below.

Robocall Mitigation Program

We actively monitor the voice traffic flowing through our network by using automatic and manual tools (as we have a 24/7 monitoring NOC team). We have automated tools for real-time tracking of calls that appear fraudulent and automatically blocking offending caller IDs and/or customers. Our NOC team also investigates any suspicious activity to determine if any customer is sending us illegal calls. If we conclude that a customer tried to send illegal calls, we warn him to assess the risk of illegal calls and request him to comply with our robocall mitigation program. In case he fails to comply we immediately block all the traffic coming from that customer.

We also collect real-time and accurate CDR information that can be used in the trace-back process.