

Subject: Explanation of Compliance Status for Robocall Mitigation Database

To Whom It May Concern,

I am writing to provide details about our company's compliance with the FCC's Robocall Mitigation Database requirements.

At this time, we have not fully implemented the STIR/SHAKEN protocol across our IP-based networks. Because we are using this service for our own business. i.e. Inbound Call Center. All of our traffic is based on IP Authentication plus Digest. However, we are actively working to mitigate illegal robocalls through other measures. In compliance with FCC rules, we have submitted a robocall mitigation plan that outlines the steps we are taking to prevent illegal robocall traffic on our network.

Our robocall mitigation plan includes (*See page # 2*). We understand the importance of protecting consumers from illegal robocalls and are committed to ongoing efforts to enhance our compliance in this area.

We are aware that, until STIR/SHAKEN is fully implemented, we are required to maintain our mitigation efforts and regularly update the FCC on our progress. We will continue to submit any necessary documentation to the Robocall Mitigation Database as required.

Thank you for your understanding, and please let us know if any further information is needed.

Sincerely,

Satwinder Saimbi
Co Founder

Robocall Mitigation Plan for Call Centtral USA Inc

1. Monitoring and Analysis of Call Traffic

We monitor all inbound and outbound call traffic using [software/tools] to detect patterns indicative of illegal robocall activity. Suspicious activity is flagged based on thresholds for call frequency, call duration, and geographic anomalies.

2. Blocking or Labeling Suspicious Calls

We have implemented [blocking/labeling technologies] that automatically block calls or label them as potential spam when certain criteria are met. We review this system regularly to ensure accuracy and minimize false positives.

3. Caller ID Authentication

While we are working towards implementing STIR/SHAKEN, we currently use alternative methods to verify caller identity and ensure that calls are properly authenticated when feasible.

4. Preventing Traffic from Bad Actors

We have strict vetting processes in place for onboarding new customers, and we regularly monitor our existing customer base. Accounts that are linked to illegal robocalling are immediately terminated.

5. Cooperation with Law Enforcement and Regulatory Agencies

We actively collaborate with law enforcement and regulatory bodies to report illegal robocall activity and assist in investigations as necessary.

6. Customer Education and Support

We provide our customers with information on how to protect themselves from robocalls, including the use of call-blocking apps and best practices for avoiding scams.

7. Ongoing Review and Updates

We review our robocall mitigation practices on a quarterly basis and update them as necessary to remain compliant with FCC guidelines and incorporate new technologies as they become available.