

Robocall Mitigation Plan

1. **FIRSTSTEP TECHNOLOGY LIMITED** ("the Company") has established a robocall mitigation program in order to curb the origination of illegal robocalls from its network.

The Company has not implemented STIR/SHAKEN authentication framework on any portion of its network. However, all calls that originate from the Company's network are subject to the robocall mitigation program described in this document.

Additionally, the Company's terms and conditions require that calls to and from the service be initiated by humans with the purpose of business communication. Scripted or otherwise automated calls are prohibited.

Procedures for robocall mitigation

2.1. The Company has a history of cooperating with local and international law enforcement to investigate and stop fraudulent activities and will continue to do so in the future.

After a notice of an illegal robocall originating from the Company's network is received it will be handled as described in section 2.2.

2.2. Procedure for investigating robocalls.

Whenever the Company receives notice of an illegal robocall originating from its network, the Company's personnel will verify the information about the call and determine if it originated from the Company or one of its partners.

1. If the robocall originated from a partner's network, the notice will be forwarded to the partner for response and appropriate action.
2. If the robocall is found to have originated in the Company's network, the Company personnel will attempt to identify the offender.
 - a. If the offender is found to be a staff member appropriate disciplinary action will be initiated in line with the Company's internal policies.
 - b. If the offender is a customer, they will be notified via email, call or both.
 - i. If it is the first violation, they will be notified that such activities are against the terms and conditions of the Company's service and advised that any future violations may lead to the customer's account being terminated.
 - ii. For subsequent violations, if it is determined that the customer is deliberately misusing the Company's service for illegal robocalls or other fraudulent activities their account will be terminated.
 - iii. At its discretion, the Company may require the offender to complete additional verification before they are allowed to use the Company's services.
3. If the robocall is not found to have originated from the Company's network i.e., the caller ID in the robocall was spoofed then the Company will share that information with party that notified it of the robocall.

2.3. Customer Verification

All customers that wish to make or receive calls using the Company's service must undergo a mandatory verification process.

As part of this verification process, the Company will verify the customer's identity and address of their place of business. The customer is required to keep these details updated.

2.4. Automated Security Functions

In order to prevent the misuse of the Company's service, the Company has deployed multiple automated security functions.

These functions look for known patterns of misuse and take actions to either stop the offending traffic, block suspicious customer accounts or alert the Company's personnel for investigation.

Based on these automated security functions, if the Company determines that a customer is deliberately sending fraudulent traffic through the Company's service then it may proactively terminate the customer's account.

2.5. Subscriber Account Limitations

All subscriber accounts have limitations placed on them to prevent misuse of the Company's service.

Any request by the customer to remove or enhance these limits is subject to the customer completing additional verification steps such as submitting address and personal identity proof documents, or other documents as deemed fit by the Company on a case-by-case basis.

2.6. Service Limitations

In addition to limitations at a subscriber level, from time to time the Company also adds other limitations to its service.

These limitations are designed to prevent illegal robocalls and other such fraudulent traffic from originating on the Company's network.

2.7. RMD rules adherence

In accordance with 47 CFR § 64.305(c) , Company commits to avoid carrying or processing illegal robocall traffic and respond within 24 hours to all traceback requests from FCC, law enforcement and industry traceback consortium. Company further commits to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls.

2.8 Below you will find a summary of some of the steps that we have taken to avoid robotic calls:

- 24/7 First-, second- and third-level support
- Inbound call checks
- Daily voice traffic monitoring with checks of key metrics like for example ACD, ASR and MOS
- Regularly checking call patterns for possible abusive traffic.
- Monitoring the network to identify suspicious traffic patterns.
- Automated alerting system which checks for unusual peaks in calls and irregular patterns in call distribution
- We will promptly respond to requests and complaints from our Carrier partners
- We can undertake measurements to block robotic calls or any type of unusual traffic immediately
- Billing and account balance monitoring for all our clients
- We only use US service providers that have implemented STIR/SHAKEN