

Steps to mitigate Robocalls

So far, we have not seen any instances of robocalls originating from our network. To ensure that it never occurs, we have implemented the following steps:

1. We verify the nature of business and identity of the customer before providing the services to any customer.
2. To prevent caller ID spoofing, we perform several checks at our end: We allow the calls to pass only those numbers which are provided by us to the customer after due verification. There is no option to pass any altered caller ID from our network. Any attempts to use a different caller ID fails because only the assigned caller ID is passed through. This is implemented through our cloud application platform.
3. All caller IDs assigned by us to our customers are callable and are verified before allowing any outbound calls.
4. We require that call center campaigns originate from our customer. The customer should not be a reseller of VoIP. The customer must be the end-user of these services.
5. We do not allow prerecorded messages of any type that do not identify the name of the entity responsible for initiating the call and a telephone number to reach that entity. The identity of the entity is cross verified with the KYC documents.
6. Any pre-recorded messages can be uploaded by the customer but can be used only after verification by our operations team through a maker-checker system built into our platform.
7. We have an abuse mitigation team which acts instantly on any misuse of services.