

Exotel Robocall mitigation plan

Exotel is one of Asia's largest cloud communication platforms. Our aim is to help businesses, both large and small, manage their customer communication via a virtual phone system. Exotel's business phone system eliminates the need to invest in any hardware or maintenance. In order to support our clients here, Exotel partners with operator in various regions including India, Singapore, Malaysia, Indonesia, United States and others.

Coming to robocall mitigation plan, this can be divided in multiple methods and is described in the document below

Know your customer (KYC)

In Exotel each customer can have a trial account for a period of time, but here we restrict the usage till KYC is completed and validated from Exotel end till satisfied. In the trial experience, users cannot call any number, but the one registered in the Exotel platform. This helps in protecting Exotel and end users from platform abuse. Only after the KYC is completed, we allow the calls to go through.

Trace the call

Exotel platform provides a trace of each call triggered by customers. Call Detail Record(CDR) is maintained by Exotel for a period of 2 years and in this duration we can provide access to law enforcement agencies on request basis. Each customer also has a trace of all the calls, both successful and failure cases are stored. If customer enabled call recording feature, then each recording is stored at platform level for their access and this is stored for a period of 9 months from the date of CDR generation

API Usage

In Exotel, the majority of our customers are API users and they typically use the click2call APIs (as defined here <https://developer.exotel.com/>). Each customer gets a unique API key and token to use the API made available in their account. There are two ways in which the use case can be restricted

Throttle

The API supports throttling and platform can drop all the other calls from platform on breach. This was done to handle the scalability and this is dynamic in nature and can be configured runtime if law enforcement instructs to do so

Authentication

The API authentication can be revoked from backend at any given point in time to disable the use case