

CloudTalk.io, Inc.
Robocall Mitigation Plan

Updated: February 2026

Introduction

This document details the steps taken by CloudTalk.io, Inc. (“CloudTalk” or “Company”) to avoid originating illegal robocalling. CloudTalk is fully STIR/SHAKEN compliant and has implemented the Robocall Mitigation Plan described herein in accordance with FCC rules and orders.

CloudTalk provides resold interconnected VoIP services to business customers. It is an STI-GA authorized Service Provider registered with the Secure Telephone Identity Policy Administrator (STI-PA) and participates in the Signature-based Handling of Asserted Information Using toKENs (SHAKEN) ecosystem. The Company authenticates its customers following the Robocall Mitigation strategies described herein and based on that authentication, attaches the appropriate attestation level to its customers’ outgoing calls.

Know Your Customer

CloudTalk has an internal “Accounts Approval” department which is our operational department that reviews all new accounts signing up to the platform. We only accept verified business end users and verify the legitimacy of each account in several ways, including the following:

- We do not accept any student or free emails. Each business needs to have an externally verifiable business registration number which our team checks in the local business register.
- In case of a different trading name to legal business name, the company must provide a verifiable link between the two
- The email domain needs to match the legal business name or trading name
- The website, social media, and linkedin presence must be consistent
- The company representative must have a verifiable link to the company.
- Customer may not use a VPN when initially enrolling on the platform
- We use tools ZeroBounce and MaxMind to verify the legitimacy of the email and domain of the sign up

Items we check for verification on their website and social media pages:

- Interactive tabs
- Contact details
- Company address
- Company details
- Consistency in business name
- Creation date of the social media page, posts, etc.
- Others
 - Sanctioned Countries (i.e. Russia, Iran, Syria, etc.)
 - Disposable emails
 - Repeated signups with almost the similar domains

- Domain age
- Online reviews
- Payment methods matching previous suspicious companies

Traceback Requests

CloudTalk is committed and will respond fully within 24 hours to all traceback requests from the FCC, law enforcement agencies, and the Industry Traceback Consortium and will cooperate with these agencies to investigate and stop any illegal robocallers that use its service to originate calls. CloudTalk has a 24/7 compliance and fraud monitoring team that responds to all urgent requests, typically within 1-2 hours. In case of a traceback request, our first line anti-fraud support has full access to all subscribers call logs, call histories, end user IP addresses and can detect patterns consistent with robocalling and immediately close all traffic from the entire offending subscriber.

The Company's points of contact to handle traceback requests are:

Name	Title	Contact Email
Erica Hoelper	Carrier Operations Lead	Accounts.approval@cloudtalk.io

Telephone Numbers

CloudTalk primarily sells end users new numbers to be used on our platform directly from our licensed vendors: Twilio, Bandwidth, Telnyx.

If a customer ports their number into CloudTalk, then the standard porting protocol is followed with LOAs, PINs, CSRs, and invoices to verify that the number belongs to that company.

In the case that a customer wants to use their external number as an outbound verified caller ID, each number is called by our KYC team, and we keep a recent proof of ownership connecting our end user to that number.

These processes are employed for both US and international call originators that use North American Numbering Plan numbers.

CloudTalk does not use a 3rd-party validation service as every request is handled internally by our KYC/fraud detection team and numbering support/carrier operations team.

Call Analytics

CloudTalk relies on its own inhouse solutions and the analytics of its underlying providers and/or their third-party vendors to determine if originating calls should be blocked based on call analytics. CloudTalk does not directly engage any third parties for call analytics.

Ongoing Robocall Mitigation

CloudTalk reviews customer call detail records (CDRs) if it suspects suspicious call activity and/or calling patterns. When the Company and/or its underlying provider detect network usage patterns consistent with illegal robocalling, we will immediately seek to identify the party originating the calls. If illegal traffic is detected, traffic from the account is immediately turned off and our Accounts Approval Team immediately suspends the account, sending a termination notice to customer. This process is included in our Terms and Conditions, under permissible user policy - <https://www.cloudtalk.io/terms-and-conditions/>