

**Kloud Communications, Inc.**  
**Robocall Mitigation Plan**  
**FRN 0031457740**

---

***Designated Contact:***

Jim Chiu  
President, Kloud Communications, Inc.  
168 W Pomona Av, Monrovia, CA 91016  
Email: [regulatory@kloudcomm.com](mailto:regulatory@kloudcomm.com)  
Tel: (213) 996-1998  
Mob: (213) 810-8188

---

**Introduction**

Kloud Communications, Inc (“we”, “us”, “our”) is a small internet and voice-over-internet service provider with under 100,000 subscribers and is committed to stopping illegal calls from originating in our network and monitoring the calls coming into our network.

We submit this report on our implementation of our plan to prevent and mitigate the origination of illegal robocalls from our network. We describe below our practices and procedures that are currently in place to achieve the goal of robocall mitigation.

**Assessment of Risk**

We periodically assess the risks that are associated with our voice business, evaluate the effectiveness of our policies and procedures, and strengthen our capabilities to support the measures outlined in this document. As such, we may modify this document from time to time in response to changes in our business, capabilities and needs.

Kloud Communications is a service provider offering a variety of calling plans, and our customer profile includes both residential and small-to-medium business customers. To date, we have not received information suggesting that robocalls have originated from our network, and we consider our network to be at low-to-medium risk of originating these illegal robocalls.

**Measures to Identify and Prevent Illegal Robocalls**

**Due Diligence: Know Your Customers**

Kloud Communications conducts due diligence of new and renewing customers, requiring proof of identity and/or organizing documents, as applicable. Service addresses are verified and confirmed, and physical installation of devices at customer premises, when applicable, is supervised by our own technicians.

All new Customers go through identity verification protocols as follows:

- Residential customers are required to provide proof of identity and service/billing address.
- For small and medium business customers, we use best efforts to confirm their identity by collecting information such as physical business location, contact person(s), state or country of incorporation, federal tax ID, and understanding the nature of the customer's business including if/how they will employ auto-dialers or other robocall style tools in the conduct of their business.
- For Enterprise customers, we obtain and record physical business location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business.
- We currently do not cater nor actively solicit the following types of customers, but in the event such customer comes on board, we will require certain documentation/information as described below:
  - For Wholesale customers, we obtain and record physical business location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business; participation in any least-cost routing agreements and the details of such agreements, identification of any upstream wholesale customers, domestic call center customers, foreign customers as per below, proof of registration in the FCC's Enforcement Database.
  - For Domestic Call Center customers, we obtain and record physical business location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business, including details about the customer's customers' planned use of the provider's services.
  - For Foreign customers, including Call Center Customers and Customers Using NANP Numbers, we obtain and record physical business location, contact person(s), state or country of incorporation, federal tax ID (if any), and the nature of the customer's business, including details about the customer's customers' planned use of the provider's services.

We regularly update customer information in our system; each contact with end users is documented by our in-house customer service representatives and serves as opportunity to confirm/validate customer information whenever an end user calls into our customer service number.

## Acceptable Use Policy (AUP)

In addition to incorporating robocall mitigation language into our service agreements, terms and conditions, and other documents where applicable, we have in place an Acceptable Use Policy prohibiting the use of our services to conduct illicit or fraudulent activities, including making illegal robocalls. In addition, this AUP prohibits the following:

- Providing altered, deceptive or false information about the identity of the sender or the origin of a message or phone call
- Violating any applicable local, state or federal law
- Violating applicable industry standards
- Using Kloud Communications' network or service to engage in or in connection with fraudulent activities.

Our terms and conditions specify the actions we may take against end users violating this AUP, and penalty includes suspension and/or termination of service.

## Contractual Agreements as a Mitigation Tool

- In addition to the mitigation language in our terms and conditions, our customers agree to participate in traceback requests.
- We deal entirely with vendors and service providers who have already certified as to their compliance to the Robocall Mitigation requirements and are listed in the Robocall Mitigation Database.

## Telephone Number Authorization

A Telephone Number ("TN")-based caller identity is the originating phone number included in call signaling used to identify the caller for screening purposes that is uniquely associated with the customer. A customer is permitted to use a TN as a caller identity if a TN is directly managed by us and/or obtained by us from one of our underlying carriers for use by the customer. In most cases, we directly manage the TNs used by our customers. We track these numbers in its inventory system and monitor the assignment of these numbers. In these cases, TN validation is the inherent result of the assignment of the TN to our customer.

If our customer wishes to use a TN as a caller identity and that TN is not directly managed by us, then TN validation is necessary. If a customer can provide a valid letter of authorization that they are the authorized user of such TNs, we will attest calls originated with these TNs.

When originating a call, we check the calling party number against our inventory and will not attest the call unless the calling party number is a TN that has been properly validated.

### Monitoring and Analytics

We conduct traffic analysis to identify patterns indicative of illegal call activity, such as intermittent bursts of high activity, suspiciously low call completion rates/short call times, and evidence of systematic calling, or “war dialing.” Abnormally high-volume call patterns from a commercial customer are also timely investigated as it is a common sign of illegal robocalling.

### Cooperation with Law Enforcement and Industry Body

We designated a single point of contact to address traceback requests from law enforcement, the FCC, or the Industry Traceback Group (“ITG”); as well as to document requests & actions taken in response thereto.

We will implement Do Not Originate requests that we receive from the ITG. We have mechanisms to automatically block suspicious calls using internal analytics. In the event that our monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, we will take appropriate action which may include suspending or terminating the Customer’s use of our network and services.

Kloud Communications certifies that it has the ability and agrees to provide for traceback requests and as always, agrees to fully cooperate with any empowered authorities request to assist in abatement.

Kloud Communications has completed the stir/shaken certification process, and is now compliant with STIR/SHAKEN.

Date: January 13, 2026