

Robocall Mitigation Plan

Business Information

CMPLTE Inc.
535 5th Avenue
New York, NY 10017

Contact Information

Michael Gutman
CEO/President
212.519.2298
gutmanm@cmlpte.com

Overview

The FCC requires that, by June 30, 2021, all small voice service providers ("VSPs") certify in the Robocall Mitigation Database that they have implemented a Robocall Mitigation Plan ("RMP") to ensure that they are not originating illegal robocalls.

The FCC requires that VSPs develop a RMP that:

- details the reasonable steps taken to avoid originating illegal robocalls;
- demonstrates a commitment to respond to traceback requests to cooperate with investigators and stopping illegal robocalls; and
- is filed in the Robocall Mitigation Database.

The FCC states that a RMP is sufficient if the detailed practices in the plan can reasonably be expected to significantly reduce the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

Purpose

CMPLTE Inc. ("CMPLTE") is small VSP that is dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network. This document delineates CMPLTE's RMP.

Know Your Customer

CMPLTE engages in a strict KYC policy, no self-installation for new customers is permitted, no new customer direct online orders are permitted and CMPLTE engages in a call debit balance system to enable monitoring of unauthorized calls. This system keeps a balance of funds with our underlying carrier and uses an available call balance refill process which generates an alert each time the balance is below our desired threshold. Our threshold is calculated by the average total call volume we expect from our customers divided over the course of the month.

The system will not allow more than 2 refills within a 24-hour period, significantly limiting any exposure to any unauthorized use of our systems and providing adequate time to investigate and remediate any issues that arise.

If a refill occurs prematurely, our internal processes call for an investigation into the cause by reviewing the call data records. If we detect any unusual activity, we immediately take the appropriate action. This effectively means that if an unauthorized use of our system does occur it will allow, at most, a limited number of calls before we are alerted and take action.

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber. A subscriber is an entity that has a business relationship with CMLTE in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

New Subscribers

- Every customer that signs up for service must provide their IRS EIN # when submitting their initial paperwork. This field is located on our auto-pay form which is required for service to start.
- We require a valid US credit card or US bank account on file that matches the customer information.
- Our Master Services Agreement ("MSA") requires the authorized contact from the company to provide their name, title and signature.
- We require an E911 form which lists the customer service address.
- We do not provide a "self-installation" service for new customers. Every customer must have an installation by CMLTE or a CMLTE authorized technician. During an installation a technician will visit the customer location and install any required hardware as well as verify the business.

Existing Subscribers

CMLTE require updates of subscribers' information on all their orders. Each order's identity markers are verified again to ensure the account is not compromised and is being used for its intended purpose.

Know Your Upstream Providers

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls Call Authentication Trust Anchor, Seventh Report and Order In CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking In CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59* (Rel. May 19, 2023) ¶¶ 49-51, CMLTE provides the following information concerning its upstream voice service carrier.

CMLTE has one upstream provider from which it receives voice traffic:

Intrado Communications, LLC (d/b/a Flowroute)
11808 Miracle Hills Drive
Omaha Nebraska 68154
Todd Kawamura
tkawamura@flowroute.com

CMPLTE has a master service agreement with its upstream provider and has received assurances in writing from its officials it has, and will continue to, sign calls transmitted to CMPLTE, and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to CMPLTE. CMPLTE and its upstream provider have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Acceptable Use Policy

CMPLTE maintains an Acceptable Use Policy ("AUP") that subscribers must sign before being permitted to use CMPLTE's network. Among other things, this AUP:

- permits "only continuous dialog between two individuals"; any autodialing, robocalling or other forms of "spam calling" are explicitly prohibited;
- enables CMPLTE to assess abnormal calling patterns; and
- prohibits use of CMPLTE's network for any illegal or fraudulent activities.

CMPLTE's contractual terms with subscribers specify that CMPLTE may take action, including suspension or termination of service and, when necessary, report suspicious activity to the proper authorities when the AUP is violated.

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 subscriber. A subscriber is permitted to use a TN as a caller identity if a TN is directly managed by CMPLTE and/or obtained by CMPLTE from one of CMPLTE's underlying carriers for use by the subscriber.

Every outbound call placed on CMPLTE's network requires an outbound caller ID.

Each customer is assigned an internal "alias" to their outbound caller ID. This allows tracking of calls in and out of their direct inward dial numbers ("DID"). This allows CMPLTE to operate several important security measures:

- tracking of outbound calls;
- tracking of inbound calls;
- billing; and
- assignment of CNAME and E911.

Every customer extension must use an outbound caller ID registered with CMPLTE. We do not permit customer spoofing of numbers, even if they prove ownership. We do not permit calls to be placed on our network without an outbound caller ID.

The only exception is when a call is being forwarded from our system in the following manner:

Inbound call from an outside line enters CMPLTE system -> Rings to a CMPLTE customer extension which has some forwarding setup (such as forward to cell phone or forward to outside line) -> CMPLTE will "spoof" the originating caller ID and pass the call along to the forwarded number assigned. This system is automated and uses the original caller ID of the inbound caller so that the CMPLTE customer can understand who is calling them. In this event, the call is logged by the PBX IP address, time-stamped and passes along the original SIP headers as we received them.

The above is the only exception to outbound caller ID. Any outbound call placed on our network by our customers must originate with an outbound caller ID that is inside of our system and that telephone number is always tied to the customer's name. Every outbound call is tagged by the customer "alias."

Monitor Traffic with Analytics

CMPLTE has a semi-automated billing fraud detection system that will block unusual high volume of calls and a manual monitoring process every 30 days and every 90 days. This system is simple and uses a low balance / replenishment approach. CMPLTE keeps a balance of funds with our underlying carrier so they carry our outbound calls.

The system conducts an auto-refill which is adjusted every 6 months. The formula CMPLTE uses is LAST 30 DAYS OF CALL TRAFFIC/4=REFILL CAPACITY.

The system will only refill a maximum once within 24 hours. CMPLTE is notified of the refill by email, and if the system attempts to refill twice within 24 hours it will not be allowed without manual intervention. This means that if a spam caller does gain access to CMPLTE network and begins to use our network to exceed our normal use, it will allow a maximum amount of calls before the attacker will be automatically blocked.

Manual Monitoring

Every 90-180 days CMPLTE pulls a review the call detail records of all calls made within our system and review two data points:

- Total calls (quantity of calls)
 - CMPLTE reviews this data at the level tracking our overall usage throughout all customers; and
 - CMPLTE also reviews this information on a customer by customer basis.

CMPLTE compares these data points to the previous 90-180 days to notice and flag any discrepancies. For example, if Q1 customer A made 5000 calls and Q2 10000 calls, CMPLTE investigates further.

- Total duration (Minutes spent on calls)
 - CMPLTE reviews this data at the CMPLTE level tracking our overall usage throughout all customers;
 - CMPLTE also reviews this on a customer-by-customer basis.

Every 30 days CMPLTE pulls a review statistic of all calls made within its system and reviews the following data points:

- Total calls made via CMPLTE's underlying carrier.
 - For example, if there is an increase of more than 15% of total processed, we will investigate.
- Total duration made via CMPLTE's underlying carrier.

- For example, if there is an increase of more than 10% in total minutes processed by CMLTE, we will investigate.

Investigate Suspicious Activity

As CMLTE owns the full call path from customer dialing to sending the call to our underlying carrier we are able to pinpoint the specific extension where calls may originate. CMLTE has a helpdesk that can be reached by help@cmlte.com as well as a support hotline at 646 685 8647 that can handle reports of suspicious activity and open a traceback ticket. Any traceback ticket opened is submitted to our helpdesk to be tracking the call.

CMLTE is able to identify the customer assigned the number in question by using the "alias." As well if for some reason that number does not have an assigned alias either due to error or technical glitch, every call made on our network is tagged with an originating IP address. That IP address record allows us to identify the specific server which originated the call. Because of our network design once we identify the IP address, we can access further records about the call such as the originating user and customer.

Either by Alias or by IP address, CMLTE is able to identify the call time and any extension which made the call. We are able to identify any active registrations of that extension and relevant IP addresses of that registration.

Upon the identification of any report of suspicious activity, once CMLTE locates the offending user, we immediately disable the extension from being able to make outbound calls effectively blocking the spam. We would then reach out the customer to continue our investigation and resolve the issue.

Blocking

CMLTE will implement Do Not Originate requests it receives from the ITG. CMLTE has mechanisms to automatically block suspicious calls using internal analytics. If CMLTE's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, CMLTE will take appropriate action which may include suspending or terminating the subscriber's use of CMLTE's network. CMLTE will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement (including the state attorney general's office), to the FCC, and/or the ITG; as well as documenting requests & actions taken in response thereto.

Plan Updates

This plan and industry best practices must evolve to response to the dynamic nature of mitigating illegal robocalling. CMLTE monitors industry best practices and continuously improve our internal processes to ensure this plan and our system adapt to this ever-changing issue.

CMLTE subscribes to multiple mailing lists that deal with telecommunications. Specifically, the outages discussion mailing list. Our PBX platform also has a community forum which regularly discusses plans and issues in telecom.

In addition, CMLTE has hired the best compliance firm in the country to support us and their provide regular newsletters keeping us apprised of any updates or changes so that we may implement best practices.

In the event of any material change to this plan, CMPLTE will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.

Certification of Michael Gutman

I, Michael Gutman, CEO/President of CmplTE, do hereby certify, under penalty of perjury, the following:

- (1) CmplTE has fully implemented STIR/SHAKEN in the IP portions of its network.
- (1) CmplTE's Business name and primary address are as follows:

CmplTE Inc.
535 5th Avenue
New York, NY 10017
- (2) CmplTE has no other business names in use.
- (3) CmplTE has not previously used any other business name.
- (4) The name, title, department, business address, telephone number, and email address of the individual responsible for addressing robocall-related issues are listed in the above robocall mitigation plan.
- (5) Michael Gutman is the sole owner and director of CmplTE and has not had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (6) CmplTE 's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
- (7) CmplTE has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (8) CmplTE is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (9) CmplTE's Operator Code Number is 101K.


Michael Gutman