

Compliance Policies concerning law and rules of:

Telephone Consumer Protection Act (TCPA) - 47 U.S.C. § 227 et. seq.:
Telephone Robocall Abuse Criminal Enforcement and Deterrence Act of
2019(Pallone-Thune TRACED Act) amending the TCPA; and the Do-Not-
Call Implementation Act of 2003 – 15 U.S.C § 6101 et. seq.

Effective August 31, 2023, for

CIMA TELECOM, INC. (CIMA)

1728 SW 22nd Street 7th Floor, Miami FL 33145 (U.S.)

CORES/FRN: **0007705916**
FCC 499-A ID: **823122** (PSP/VoIP Gateway)¹
FCC 214: **ITC-214-20010116-00020**²

Prepared by assistance of:
Edward A. Maldonado, Esq.
Regulatory Counsel for

CIMA Telecom, Inc. (FL)



The Law Offices of Edward A. Maldonado, P.A.
MALDONADO LAW GROUP
2850 Douglas Road, Suite 303, Coral Gables FL 33134
Tel: 305-477-7580
Fax: 305-477-7504
E-mail: eam@maldonado-group.com
www.maldonado-group.com

¹ [FCC Form 499 Filer Database Detailed Information](#)

² [Office of International Affairs \(fcc.gov\)](#)

ADOPTED POLICY:

CIMA Telecom, Inc., a Florida corporation, (CIMA) is an international common carrier holding authority from the Federal Communications Commission (FCC) as an international carrier and is voice service provider as defined under amendments to the Federal Communications Act of 1934, as amended, and further amended by 47 U.S.C. § 227 et. seq (TRACED Act), generally, and under rules and orders promulgated by the FCC. Due to the nature of voice service traffic that CIMA routes it identifies itself as a gateway and intermediate provider under the TRACED Act. The nature of CIMA' voice services are wholesale resale of call termination to international points and within the United States primarily via VoIP/SIP routing. These policies are applicable to the termination of calls routed by CIMA and its role as a wholesale resale voice service provider. CIMA does not offer retail communication services directly to the public. CIMA does have retail services through affiliates, but the services underpinning any retail sale resides with CIMA for purposes of the Act. CIMA does not originate voice services directly from a calling party or terminate voice services directly to a called party. At times, CIMA may act as an intermediate voice service provider, and at other times as an international gateway provider of VoIP and telecommunications services. CIMA adopts the identification and requirements of a Gateway voice service provider under the Act for all its U.S. domestic call termination services in the abundance of caution. ³

³ A company is a gateway provider if it is a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider. See 47 CFR § 64.1200(f)(19). "U.S.-based" means that the provider has facilities located in the United States, including a point of presence capable of processing the call. "Receives a call directly" from a provider means the foreign provider directly upstream of the gateway provider in the call path sent the call to the gateway provider, with no providers in-between.

Under the TRACED Act, The FCC has promulgated rules and orders applicable to gateway providers, such as CIMA. The following policies apply to the compliance of CIMA with those rules in the rendering of its services and its responsiveness to mitigating illegal or unlawful suspected robocalls. CIMA has no technical means to have Privy to the call content of any suspected roll calls. CIMA's mitigation protocol is based upon reasonable mitigation methods either authorized by the FCC or otherwise in the custom and practice of identifying robocalls through trace backs requested from the FCC's Industry Traceback Group.

Pursuant to FCC rules in orders, CIMA has registered itself on the FCC's Robocall Mitigation Database⁴ as follows: (updated as of: August 1, 2023) ⁵

CIMA Telecom, Inc.	U.S. Jurisdiction
Gateway	RMD Number: RMD0003122

PROCEDURAL HISTORY CIMA IN COMPLIANCE WITH THIS TRACE ACT.

The following measures were implemented by CIMA pursuant to the prescribed dates:

- **CIMA dedicated ITG Traceback Response Staff.** CIMA maintains technical and administrative staff available to respond to FCC's Industry Traceback Group. Staff has access to the Network Operating Center of CIMA and customer contracts, KYC information and access to the ITG portal dashboard for Traceback requests and responses. CIMA Staff maintained is at a minimal number of eleven (11) personnel with this policy. All staff are employees of CIMA, not contractors. Staff has been maintained since **July 1, 2020**, for these purposes.

⁴ [Robocall Mitigation Database Opens; Filing Instructions and Deadlines | Federal Communications Commission \(fcc.gov\)](https://www.fcc.gov/robocall-mitigation-database)

⁵ [HTTPS://FCCPROD.SERVICENOWSERVICES.COM/RMD?ID=RMD_FORM&TABLE=X_G_FMC_RMD_ROBOCALL_MITIGATION_DATABASE&SYS_ID=0C9EF7A21BEFA01002BEEA82F54BCB11&VIEW=SP](https://fccprod.servicenowservices.com/rmd?id=rmd_form&table=x_g_fmc_rmd_robotcall_mitigation_database&sys_id=0c9ef7a21befa01002beea82f54bcb11&view=sp)

- **Calling Number Verification & Anti-Spoofing.** CIMA performs vetting incoming call traffic that touches its network by maintaining a database with the ITG's DNO lists since September of **2020**. CIMAs' internal DNO listing is compiled from internal mitigation methods discovery and ITG Tracebacks (when received) and other ITG sources of DNO numbers. The lists are vetted to cross reference duplicate calling numbers and are derived from the following sources:
 - Internal Discovery List (Monthly listing)
 - Reported Tracebacks received of suspected robocalling numbers.
- **Calling Number Verification & Anti-Spoofing.** CIMA conducts ANI confirmation for validation of numbers within the North American Numbering Plan as a measure to detect call spoofing or Pseudo ANI.
 - Cross reference with the Local Exchange Routing Guide (LERG) operated by *iconectiv* for NPX-NXX at block level referencing monthly activity of service providers on the PSTN as of August 1, 2023.
- **Do-Not-Call (DNC) Blocking.** CIMA performs vetting incoming call traffic that touches its network with calling numbers listed on the Federal Trade Commission's DNC list directly or via third-party vendors of affiliates who blend these lists into prohibited dialed numbers. The list is updated quarterly.
- **STIR/SHAKEN Tokenization.** CIMA performs STIR/SHAKEN attestation with a recognized certifying authority and NECA ONC Declaration with a provider specific Token unique to itself that is inserted into the IP Header of routed calls terminated in the U.S. Authentication is C level for Gateways.
 - **Certificating Authority:** **iconectivOCN**
 - **Designation:** **Interexchange Carrier**
 - **Token ID:** **To be provided upon request.**
- **Traffic Monitoring of Short Duration calls and anomalies.** Traffic study measures are automated and in place in near to real time of short duration calls, frequency, calling party number, and transmitting provider. Monitoring began on May 1, 2018. Anomalous traffic patterns or traffic increase of short duration calls not indicative of conversational traffic is flagged and customer is questioned on the

nature of traffic and traffic source as a preliminary warning to any future call blocking.

- **Call Blocking.** CIMA blocks the calling number and/or trunk attributable to a suspected robocall for which it receives a traceback request. Customer is informed of the issue at the time CIMA seeks further information on the call and CIMA reserves the contractual right to block and suspend customer accounts, for cause, with providers that transmit more than three (3) calls that result in Traceback requests within a 48-hour consecutive period, or more than three (3) independent Traceback requests within any given calendar month. Final review of customer suspension or termination is based upon business decision and further information found on the customer's KYC contact form, or otherwise provided by the customer after further inquiry by CIMA.

MINIMAL TRACED ACT REQUIREMENTS OF CIMA:

- I. Policy regarding **47 CFR § 64.1200**, as amended by 2023 (Delivery restrictions); AND Federal Communication Commission's *Sixth Report And Order In Cg Docket No. 17-59*, *Fifth Report And Order In WC Docket No. 17-97*, *Order On Reconsideration In WC Docket No. 17-97*, *Order, Seventh Further Notice Of Proposed Rulemaking In CG Docket No. 17-59*, And *Fifth Further Notice Of Proposed Rulemaking In WC Docket No. 17-97* (Issued May 20, 2022).

CIMA has implemented "Know Your Customer" (KYC) contact forms and traffic monitoring processes to mitigate the risk that it may inadvertently process or route illegal robocalls on behalf of its customers. Contact forms are acquired from all foreign and/or intermediate providers upon contract, or upon request, as a part of CIMA's onboarding of the customer. Existing clients have been secured from respective providers. Contact information is updated annually, or upon demand of CIMA. See, Exhibit A for ***Sample form of KYC Form.***

CIMA' robocall mitigation program takes guidance from ***the Best Practices for the Implementation of Call Authentication Frameworks*** by the NANC Call

Authentication Trust Anchor Working Group. See, Exhibit C of this Policy. The efficacy of the program is evidenced by the fact that, its responsiveness is well below required timetables by the FCC and has participated fully and proactively with the FCC's Industry Traceback Group (Industry Traceback Group (tracebacks.org)). As of the date of this policy, the average response time by CIMA to any trace back received from with the FCC's Industry Traceback Group is within six (6) hours or less from time first received by the company. This statement is based upon records of the FCC's Industry Traceback Group and not internal estimates by CIMA.

a. STIR/SHAKEN Compliance.

CIMA has implemented attestation level C (Gateway) as a voice service provider for all traffic pursuant to 47 C.F.R. § 64.6301 et. seq. Under this attestation level, The call is received from an authorized party, but CIMA cannot authenticate the call source received into its network as the call was received from other provider closer to the originating source of the suspected robocall. CIMA has deployed STIR/SHAKEN protocol fully under attestation level C as of July 1, 2023.

CIMA has implemented attestation level C (Gateway) under STIR/SHAKEN protocol in combination with the following reasonable mitigation protocols: as a Gateway voice service provider in furtherance of Know Your Customer (FCC R&O NFPRM FCC 22-37) and STIR/SHAKEN (47 C.F.R. § 64.6301 et. seq.) obligations. Token is inserted **on all** U.S. domestic calls routed for termination by CIMA.

b. TRACEBAK Requests from ITG.

i. Acknowledgement that one (1) Traceback of suspected robocall may represent multiple calls being introduced into the call flow that are violative of the TCPA.⁶ CIMA takes every traceback request from the ITG seriously. The mere presence of one trace back, or one call violative of the TCPA, has legal standing for enforcement by the FCC or through the courts. With a policy of best practices, every Traceback Request of a suspected robocall violative of the Federal Communications Act (FCA) will be treated as serious and result in the immediate blocking of that number, contact with the upstream customer, and addition of the number to standing DNA lists maintained by CIMA.

ii. Minimal Response Times

Upon receipt of a traceback request from the Commission, civil law enforcement, criminal law enforcement, or the industry traceback consortium: CIMA (when acting as Gateway) shall respond to the traceback request concerning a suspected illegal or unlawful robocall within **24 hours**. In accordance with 47 C.F.R. § 64.1200 (c) (2)(I)(n)(11), and at a maximum, this 24-hour clock for CIMA will not start outside of business hours, and requests received during that time are deemed received at 8 a.m. on the next business day. Should the 24-hour response period end on a non-business day, either a

⁶ See, *Drazen v. Pinto*, No. 21-10199, 2023 WL 4699939 (11th Cir. July 24, 2023).

weekend or a Federal legal holiday, the 24-hour clock does not run for the weekend or holiday in question and restarts at 12:01 a.m. on the next business day following when the request would otherwise be due. *(For example, a request received at 3 p.m. on a Friday will be returned before 3 p.m. on the following Monday, assuming that Monday is not a Federal legal holiday.)* Business days are deemed to be Monday through Friday, excluding Federal legal holidays, and *business hours* is deemed to be 8 a.m. to 5:30 p.m. Eastern Time. on any business day. 47 C.F.R. § 64.1200 (c) (2)(I)(n)(11).

iii. Complete Information logged within ITG Portal.

CIMA has trained its staff on accessing and providing information buying through the ITG portal in regard to all trace back request received. Complete information to the best of CIMA' KYC contact form, billing records and correspondence with the upstream provider customer shall be logged into the ITG portal based upon the particular request of the ITG. CIMA Shall not at any time withhold information that is readily available from disclosure through the portal. Special request by the ITG for information beyond the purpose of a traceback "hop" will be handled on a case-by-case basis. Complete disclosure shall comprise disclosure of transmitting call information between CIMA' upstream customer, CIMA, and the downstream provider to which CIMA transmitted the call. CIMA

shall identify that the calls it transmitted contained its token and confirm the token with the ITG.

iv. Procedures upon Traceback Request

Upon receipt of a Traceback Request, CIMA shall perform and adhere to the following as appropriate:

1. Promptly investigate each transmission identified by the ITG in the Traceback Request
2. If necessary, effectively mitigating the identified unlawful traffic by determining the source of the traffic and preventing that source from continuing to originate such traffic. This may involve one of three measures:
 - a. **Block Customer traffic.** Block Call Traffic from the voice service provider subject of the Traceback Request.
 - b. **Suspend Customer.** Suspend the Access to CIMA' network by the subject voice service provider of the Traceback Request. This measure is reserved for repeated traceback requests within a short period of time not exceeding 48 hours, or if reoccurrence of

Traceback Requests happens on an individual basis more than three times within any given calendar month.

- c. **Terminate Customer.** Terminate dealings with the voice service provide subject of the Traceback Request upon further occurrence within 48 hours of receipt of the Traceback Request(s). This action is reserved for repeated Traceback Requests from the same provider after CIMA has communicated with provider about the traffic and has been given assurances that it will not happen, but nonetheless trace back requests continue.

All above measures are intended to mitigate CIMA' platform from further transmitting illegal robocalls and is the Policy Goal of its Traceback Responses and mitigation measures.

3. Safeguarding CIMA and its communications network by using any other internal reasonable **means** to prevent entry into the U.S. of suspected traffic to prevent customers from using CIMA' network.

- c. **Compliance with 47 CFR 64.1200(k)(4) "FCC K4 Notice."**

CIMA recognizes and acknowledges that pursuant to 47 U.S.C. § 227 et. seq the FCC may determine certain providers to be violative of the TRACED Act and send Notice to all voice service providers as prescribed by 47 CFR 64.1200(k)(4). It is understood and recognized that this notice is a notice

to all voice service providers like CIMA to take immediate action with regard to the target provider and any traffic it sends to other voice service providers terminating calls within the United States. Public notice and copies of the FCC K4 Notice will be published by the FCC on its website and generally circulated through the Industry Traceback Group to warn the industry that it has made an initial determination that traffic passed from these providers is violative of the Federal Communication Act. CIMA upon such notice being made public shall take the following actions with regard to the subject provider until final resolution or determination is made in the matter.

1. **Call Blocking:** Block upstream traffic from “Bad Actors” (including known affiliate or sister companies providing voice service call termination into the U.S.) from passing through CIMA’ network. *CIMA shall inform the customer in writing This action being taken and sight the FCC K-4 Notice as reasonable cause for this action.*
2. **Customer Access suspension.** Immediately suspend the account of the suspected “Bad Actor” until final determination or resolution of the matter is authorized by the Commission. *CIMA shall inform the customer in writing This action being taken and sight the FCC K-4 Notice as reasonable cause for this action.*

3. **Termination of Customer Account.** Upon reliable information made public by the FCC, CIMA reserves the sole right to terminate the account of the customer target of the FCC K-4 Notice. *CIMA shall inform the customer in writing This action being taken and sight the FCC K-4 Notice as reasonable cause for this action.*

For purposes of this particular policy, e-mail is deemed sufficient writing for notice to the customer or voice service provider in question.

- II. Compliance with Do-Not-Call Implementation Act of 2003, 15 U.S.C § 6101 et. seq., as a voice service provider acting as a Gateway.

CIMA acknowledges that in its role as a voice service provider it does not have contractual privity with the calling party for any “commercial telephone call” that passes through its network. CIMA further acknowledges that called parties within the United States may register themselves and the Federal Trade Commission’s Do-Not-Call Registry to prohibit unwanted telephone sales solicitation and telemarketing via and through their subscriber number.

As reasonable compliance with the Do-Not-Call Implementation Act of 2003, CIMA has elected to database and vet numbers found on the Do-Not-Call Registry as subscribed historically by one of its affiliates and include these telephone numbers with blocked DNO telephone numbers within its network. CIMA has direct control of the affiliate that acquires the Do-Not-Call Registry telephone numbers and reasonably adds these numbers to calls blocked from its network.

III. Errors Occurring Under This Policy

Should an error in the performance of CIMA written policies occur, CIMA shall investigate the cause of the error and if within the control of CIMA for corrective action. Such investigation shall determine whether the cause was technical or due to human error and take remedial action to correct any technical problem and further educate any staff on the compliance requirements under this policy and under the Telephone Consumer Protection Act, Telephone Robocall Abuse Criminal Enforcement and Deterrence Act of 2019, and the federal Do-Not-Call Implementation Act of 2003. Staff education and research of regulatory changes will supplement this policy to curb any preventable errors.

This Policy is hereby authorized by:


Rafael Carvajal (Dec 26, 2023 10:17 CST)
Mr. Rafael Carvajal, President /CEO
CIMA Telecom, Inc.

Covered subsidiary entities under this Policy:

- CTI Wholesale Services, LLC (FL)
- Hola America, LLC (DE)
- Anew Broadband, Inc. (FL CLEC)

Date: December 19, 2023