

HYPERCUBE NETWORKS, LLC
Certification and Robocall Mitigation Plan
February 2024

HyperCube Networks, LLC
3200 W Pleasant Run Rd Ste 300
Lancaster, TX 75146

INTRODUCTION

Pursuant to the applicable orders and regulations of the Federal Communications Commission (“FCC”), this document supports the certification by HyperCube Networks, LLC (“HyperCube”) where it is operating as a Voice Service Provider, Gateway Provider, or Non-Gateway Intermediate Provider that;

(i) it has fully implemented the STIR/SHAKEN authentication framework across its entire network, and all calls it originates are compliant with [§ 64.6302\(b\)](#);

(ii) it has no type of extension or extensions under [§ 64.6304](#);

(iii) it commits to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls;

(iv) It is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.

Hypercube Networks role in the call chain includes:

1. Voice Service Provider with STIR/SHAKEN implementation
2. Acting as a Wholesale Provider originating calls on behalf of another provider or providers
3. Gateway Provider with STIR/SHAKEN implementation
4. Non-Gateway Intermediate Provider with a STIR/SHAKEN implementation

The specific reasonable steps that HyperCube has taken to avoid carrying or processing illegal robocall traffic as part of its robocall mitigation program, including a description of how it has complied with the know-your-upstream provider requirement in [§ 64.1200\(n\)\(4\)](#) is described below.

Entities Covered by Certification

The following entity is subject to robocall mitigation policies and procedures described in this document:

HyperCube Networks, LLC

HyperCube Networks, LLC, “the Company” has previously been known by the names of West Telecom Services, LLC and Intrado Communications, LLC.

HyperCube Networks OCNs

STATE	OCN
AL	807C
AR	9556
AZ	890G
CA	808C
CO	809C
CT	810C
DC	812C
DE	811C
FL	813C
GA	814C
IA	860C
ID	815C
IL	816C
IN	817C
KS	818C
KY	861C
LA	819C
MA	116E
MD	820C
MI	821C
MN	822C
MO	824C
MS	823C
MT	825C
NC	832C
ND	891G
NE	826C
NH	828C
NJ	829C
NM	830C
NV	827C
NY	831C
OH	9557
OK	833C
OR	834C
PA	835C
RI	836C
SC	837C
SD	838C
TN	845C
TX	9558

VA	840C
VT	839C
WA	841C
WI	843C
WV	842C
WY	844C

STIR/SHAKEN IMPLEMENTATION

HyperCube Networks is an Intermediate Provider, as defined in 47 CFR 64.1600(i). For its end user traffic, the Company has upgraded its network to allow for the initiation, maintenance, and termination of SIP calls and fully implemented the STIR/SHAKEN framework as required in §64.6301 throughout all IP portions of its network. Neustar is the Authentication Service/Verification Service (AS/Vs) authority Hypercube Networks uses today for STIR/SHAKEN. Pending availability of STIR/SHAKEN solutions for non-IP based traffic, the Company has implemented rigorous procedures to mitigate illicit robocalls and unauthorized Caller-ID spoofing in addition to being a highly cooperative and engaged member of the industry traceback consortium.

HyperCube Networks upgraded its Routing Engines to allow for the Response Profile which provides enhanced configurable Call-Info. If the user provisions a Call-Info value, it is sent to the SBC in the policy response. The SBC adds this value only when the SBC rejects the call with a 608 SIP status code and only when the IPSP flag "Support Call-Info with SIP cause 608 (RFC8688)" is enabled.

Our Media Gateways supports the "607/608 Unwanted" response code on the Cause Code Mapping profile. The range of CDR fields, Call Disconnect Reason, Status Message for Call Release, and Call Disconnect Reason Sent to the Ingress of Attempt Record are extended to new values. The SBC also supports rejecting calls with SIP status code 607/608 when returned from the Response Profile and provides capability in SIPTOCPC cause code mapping to map 607/608 to ISUP 21 with the location user.

ROBOCALL MITIGATION PROGRAM

The Company participated directly in the FCC's Robocall Strike Force and is one of the founding members of the USTelecom Industry Traceback Group ("ITG"). The Company remains highly engaged in combatting illicit robocalling and unauthorized Caller-ID spoofing. Further, the Company has been actively engaged in the FCC's proceedings involving methods to mitigate illicit robocalling and unauthorized Caller- ID spoofing. Below are the steps and efforts taken to mitigate illegal robocall traffic:

Traceback

The Company agrees to comply with efforts to traceback the source of suspected robocalls.

- We will respond fully and within 24 hours to all traceback requests from the

- Commission, law enforcement, and the industry traceback consortium.
- We shall continue to cooperate with traceback requests received directly from carriers, industry associations, law enforcement, and other authorities.
 - Call records are created for all calls and are searchable.

The Company's contact for traceback requests is:

Name	Title	Contact Information
Jaddeus Fears	Manager – Information Technology	Ph: 334-710-9974 Email: jnfears@west.com or Fraud@west.com

Compliance to Mitigate Illegal Traffic

The Company will continue to assist with the mitigation of suspected illegal activity when it has been notified by the Commission through its Enforcement Bureau.

Measures to Prevent Origination of Illegal Calls

The Company implemented steps described below to prevent illegal calls on both non-IP and IP- based tandem traffic:

We use software provided by RouteTrust to monitor our voice traffic in near real-time to prevent illegal robocalls from traversing our network. The software allows for the writing and refining of traffic monitoring rules to detect suspected robocall traffic. The software alerts us if we receive calls where the calling number is invalid, unallocated or on a Do Not Originate list (provided by ITG and SOMOS). We take reasonable and effective steps to ensure that our immediate upstream providers are not using our network to carry or process a high volume of illegal traffic by exercising due diligence with our customer's traffic.

We also extensively investigate new customers seeking to send high-volume short duration (non-notification or non-conversational duration traffic) to determine if a potential robocall situation exists. We immediately investigate any identified calls (whether by a downstream provider or our own alerts) and escalate to our upstream customers to work with them regarding the flagged traffic. If we determine that the upstream provider was attempting to negligently pass unlawful robocalls, then we either warn them to stop or terminate their service as appropriate.

Know Your Customer

As exemplified by the Company's completion of millions of consumer-consented notification calls every month, the completion of legitimate robocalls is as crucial as the mitigation of illicit robocalls. The Company has committed substantial resources in its efforts and has significantly strengthened its practices to ensure legitimacy of calls that traverse its network.

For example, before the Company initiates service for a new wholesale customer, the Company requires that the new customer provide detailed traffic-profile information including, but not limited to the average length of call ("ALOC"), estimated call types

(including whether calls will be manually- or computer-generated, and whether the traffic is opt-in or otherwise), projected call volumes, and similar information (“opt-in” traffic referring to, for example, pharmacy customers opting-in to receive notices about prescription availability). See Customer Screening examples below. The Company then compares actual call traffic to characteristics listed in the customer-provided traffic profile.

The Company remains alert and responds to any reports from consumers and from other carriers of suspected fraud calling. If fraud calling is detected, or if the customer’s actual traffic is different from that reflected in the customer-provided traffic profile, then the Company takes steps ranging from requiring the customer to demonstrate traffic legitimacy and explain the differences, to stopping traffic ingress from the customer until the traffic is proven to be legitimate and compliant. The Company typically limits calls per second (“CPS”) to 1CPS per each 100 sessions of service provisioned. And the Company continues its post-production traffic analysis to identify failures attributable to use of unallocated telephone numbers and similar behaviors.

The Company’s process is dynamic and evolves to address changes in fraud-calling patterns using metrics to identify certain factors – for example, identifying short duration calls with high completion rates to limit the number of false positives targeted for blocking.

The Company uses initial customer surveys in its effort to know its customers and anticipate usage profiles. EXAMPLES 1 and 2, below, reflect some of the mechanisms now utilized by the Company in such efforts.

EXAMPLE 1 (VIA EMAIL AND HARD COPY)

**HyperCube Networks, LLC
Screening and Onboarding Questionnaire**

HyperCube Networks is a regulated entity within the United States and holds a leading role in the market for setting new standards of excellence as well as compliance. As part of that effort, we have implemented additional screening and onboarding processes, and have partnered with like-minded organizations to provide secure and compliant telecom services. It is our duty to ensure that our customers who originate or terminate calls agree to work cooperatively with us and within the regulations that involve and govern our networks. The following information and authorizations are sought as the first part of this process:

BUSINESS INFORMATION		
Legal Company Name:		
Entity Type:	☐ Corporation ☐ Individual ☐ Partnership ☐ LLC ☐ Other:	
Type of Business:	☐ Wholesale ☐ Retail ☐ Both – <i>provide percent of mix:</i>	
Year Incorporated:	# Years in Business:	
FCC Registration #:	Business Registration #:	State or Country of

				Incorporation:	
Physical Address (Headquarters):	Address 1:		Address 2:		
	City:		State:		Zip:
Email Address:		Website:		IP Address:	
List any and all business and trade names, fictitious names, DBAs for which you have transacted business for the previous three (3) years:					
Direct or Indirect Owner of the Business:	Name:		Email:		
	Address 1:		Address 2:		
	City:		State:		Zip:
Person Responsible for Compliance with U.S. state and federal laws prohibiting robocalls:	Name:		Email:		
	Address 1:		Address 2:		
	City:		State:		Zip:

CUSTOMER QUESTIONNAIRE	
Do we have your permission to share any and all profile information that we may possess regarding your call traffic including your call-traceback history and performance as part of our KYC requirements? <i>(Information will only be shared with government entities as requested.)</i> ☐Yes ☐No	
Tell us in your own words how you plan to use the HyperCube network and which products will be used directly or indirectly by your company? If you are a Reseller, please define the platform that originates or terminates calls.	
Does your plan include any of the following activities? <i>Please mark all that apply.</i>	☐ Originate or carry conversational call traffic ☐ Originate or carry autodialed call traffic ☐ Act as an Originator or U.S. Point of Entry ☐ Have customers that engage in telemarketing ☐ Other <i>(please specify)</i>:
List a brief description of any technology that you support or promote in your offers that may originate or terminate calls whether directly to the HyperCube network and through its	

suppliers:

Provide evidence of your strong, credible preventive measures and written practices to combat illicit and illegal calls, including unsolicited robocalls and calls reflecting unauthorized (spoofed) Caller-ID information. This may include any links to your relevant published terms of service.

Mark all that apply:

☐ Has your company ever been determined by US Telecom's Industry Traceback Group, in its sole discretion, to be a "Non-Cooperative Voice Service Provider" as defined in the January 2020 edition, or any subsequent edition, of its Policies and Procedures?

☐ Has your company ever been blocked from another voice service provider's network after being determined to be a "bad-actor upstream voice service provider" pursuant to a notice to the Federal Communications Commission in a process more formally described in Paragraphs 35-45 of the Federal Communication Commission's Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 and adopted July 16, 2020?

☐ Has your company ever had an adverse judgment against it in a civil lawsuit alleging claims under the TSR, the TCPA, or any other lawsuit regarding Robocalls, automated dialing, calls to the DNC Registry or any state do not call registry, spoofed caller ID numbers, or otherwise unlawful telemarketing or solicitations?

☐ Has your company implemented or is currently implementing the STIR/SHAKEN Authentication Framework (to the extent legally required) unless changed pursuant to applicable legislation, or a successor authentication framework if subsequently mandated by applicable federal law or regulation?

ATTESTATION	
Customer attests that you and your company to the best of your ability and knowledge do not engage in any illicit activity as defined by the FCC/FTC or AG when it refers to TCPA or Telecommunications.	
Customer attests that you and your company are not an access stimulator as defined by the FCC order number 47§ 51.914.	
Customer affirms and certifies that all information and answers to questions herein are complete, true and correct to the best of signatory's knowledge and belief.	
The signatory below represents and warrants that he/she has full capacity and authority to sign on behalf of customer.	
Customer Name	
Signature	
Printed Name	
Title / Position	
Date	

* The Industry Traceback Group ("ITG"), comprised of industry members such as HyperCube Networks, is designated by the FCC Enforcement Bureau as the single consortium to conduct private-led call traceback efforts. See <https://www.ustelecom.org/the-ustelecom-industry-traceback-group-itg/>.

EXAMPLE 2 (VIA ONLINE PORTAL AND ELECTRONIC SIGN-UP)

<https://hypercube.me/> (Customers must login in order to see and complete the online portal form and electronic sign-up entry fields.)

Contractual Obligations to Mitigate Illegal Robocalls

Hypercube Networks LLC requires via its contracts with customers they will not participate in or assist in any fraudulent usage, in any form or by any means. If customer suspects, knows of, or should have known of any fraudulent usage, customer will immediately stop all fraudulent usage and notify Company at fraud@west.com.

If Company becomes aware of unusual usage volumes or patterns, Company will make commercially reasonable attempts to notify customer; provided, however, Company will have no obligation to notify customer of any such volumes or patterns. Company's sole obligation to customer with respect to any actual, alleged or suspected fraudulent usage will be to reasonably cooperate with customer to stop the fraudulent traffic before shutting down the customer's trunk group.

Calling-Number Do-Not-Originate ("DNO")

Automatic call blocking is implemented on telephone numbers for which the legitimately-

assigned person or entity never originates outbound calls. Both geographic and toll-free telephone numbers are subjected to DNO upon the Company's receipt of authorization. Reversal of DNO is performed upon the Company's receipt of authorization from the same person or entity for situations in which outbound calling becomes desired. DNO may be performed on both the Company's wholesale network and on retail services that the Company may provide.

Cease and Desist, and Service Termination

The Company issues cease and desist notices to customers whose traffic-origination practices appear to violate laws, rules, and terms and conditions. The Company continues its traffic-monitoring practices to ensure customer compliance and removes customers that do not respond to such notices and who remain non-compliant.

Subscription List Analysis/Mitigation

The Company analyzes telephone numbers submitted to it through agency-subscription lists (e.g., IRS Telephone Number Activity reports) to determine whether suspected-fraud calls or customers associated therewith are using the Company's services. Positive results of such analyses trigger fraud mitigation pursuant to this Robocall Mitigation Plan.

Network Control Red Flags and Triggers for Mitigating Illicit Robocalling (Applicable to both IP- and TDM-Originated Traffic Unless Otherwise Indicated)

- Significant volumes of calls to unallocated or unassigned numbers.
- Calls reflecting Caller-ID numbers that generate unusually high call volumes over specific periods.
- Calls reflecting Caller-ID numbers that generate unusually high numbers of short-duration calls over specific periods.
- Calls that, in large volumes, reflect non-standard or improperly formatted Caller-ID.
- Significant volumes of unplanned or non-forecasted calls in bursts irrespective of Caller-ID values.
- High call volumes at times inconsistent with historical trends for the originator's network.

All such Red Flags trigger investigation and, when determined to be appropriate, mitigation. Mitigation steps are dependent on the results of each investigation.