

Policy Statement. MIAMI TELECOM fully supports the efforts by the various Federal, State, and local regulatory agencies to protect consumers and help rid the USA of the scourge of illegal robocalling and calls that violate TCPA rules by implementing the following policies and procedures summarized here and detailed below.

- **KYC.** Force strict and thorough Know Your Customer (KYC) protocols and practices to help prevent bad actors from becoming MIAMI TELECOM customers and perpetuating their fraud on the MIAMI TELECOM Network.
- **KYCT.** Traffic is not allowed to ramp-up from a new customer until we have analyzed such traffic to make sure it's following robocalling, telemarketing and TCPS rules & regulations.
- **Provisioning.** All new customers and existing customers participating in short duration robocalls will be set-up with separate trunk groups and monitored much more closely than conversational customers.
- **Stir/Shaken.** All calls that come to us unsigned will be filtered by MIAMI TELECOM Filtering Systems, and either (1) signed and passed through our network, or (2) returned to the customer to route advance in their LCR, or (3) stopped the call(s) from being completed or route advanced.
- **ITG Compliance.** MIAMI TELECOM will fully cooperate with the Industry Traceback Group (ITG) promptly on all traceback requests to help identify bad actors.
- **TCPA & Telemarketing Sales Rule Compliance.** MIAMI TELECOM will not willfully assist customers in violating the Telephone Consumer Protection Act (TCPA) and other laws designed to protect consumers from unwanted and/or illegal robocalls.
- **FILTERING.** MIAMI TELECOM uses anti-robocall filtering system which check the calling party's phone number and called party's phone number for suspected fraud using several third-party databases. It will be configured on a customer-by-customer basis to increase filter sensitivity commensurate with KYC policy.
- **Monitoring.** Using filtering systems, calls are monitored to identify calling patterns consistent with fraud for follow-on action to eliminate it from our network without regard for potential revenue loss.
- **Repeat Offenders.** Customers who continue to be responsible for tracebacks and do not take corrective action to address fraudulent call patterns will be terminated using the Company's Three Strikes Rule.
- **Law Enforcement Notification.** Notification will be sent to the appropriate law enforcement authorities on Customers who are purposely sending illegal robocalls.

1. Definitions: For purposes of these policies, procedures and protocols, the following definitions shall apply.

- a. **"Aggregator"** shall mean an FCC licensed long distance telecom carrier with a 499 Filer ID and a RMD FRN number who sells USA termination on a wholesale basis to others such as long-distance carrier.
- b. **"ANI"** means the originating phone number of a call.
- c. **"Conversational Traffic"** shall mean long distance traffic that averages 60-seconds or longer.
- d. **"Caller ID Spoofing"** means when a caller deliberately falsifies the phone number transmitted to the caller ID number shown on a person's phone display to disguise their identity, oftentimes to defraud consumers.
- e. **"DNC"** means the Do Not Call list consumers use to register their phone numbers to avoid sales and marketing related calls that are unwanted.
- f. **"DNIS"** means the called to party on a call.

- g. **“DNO List”** means calls originating from a list of known phone numbers that are for inbound calling only which are spoofed by bad actors to fool customers into believing they are getting calls from the company who owns such a phone number.

- h. **“Enterprise Call / Contact Center”** means a foreign or USA based call or contact center that is not engaged in selling USA terminating minutes to carriers, resellers, or aggregators.
- i. **“FRN number”** means the registration number assigned to a carrier, reseller, or aggregator by the RMD.
- j. **“KYC”** shall mean Know Your Customer and the process for doing so to screen out bad actors before they send illegal traffic over our network.
- k. **“KYCT”** shall mean Know Your Customer’s Traffic and the process for doing so for the purpose of analyzing traffic for illegal calls before allowing full customer production traffic to commence on our network.
- l. **“Pre-production & Test Traffic”** means the initial customer traffic and limited small volume production traffic sent over the MIAMI TELECOM Network for purposes of analyzing such traffic for potential fraud and violation of various laws.
- m. **“Production Traffic”** means Customer traffic being sent to the MIAMI TELECOM Network that represents normal daily traffic volumes the Company can expect to receive.
- n. **“RMD”** shall mean the FCC’s Robocall Mitigation Database.
- o. **“Short Duration Traffic”** shall mean long distance traffic that averages less than 12-seconds in length.
- p. **“Filtering Systems”** means software systems that help to identify numerous types of suspicious and illegal calling activity by dipping different and ever-changing databases which identify calls with a high probability of fraud or outright fraud.
- q. **“Reseller”** means a licensed USA carrier, with an FCC 499 Filer ID and an RMD FRN number who offers USA termination to call or contact centers in the USA or abroad but who does not offer service to other carriers, resellers or aggregators.
- r. **“TCPA”** means the Telephone Consumer Protection Act which specifies rules for sending calls to US consumers which must be followed by callers and carriers allowing calls to traverse their networks.
- s. **“The MIAMI TELECOM Network”** shall mean the Company’s switching platform and underlying carries it uses to terminate traffic to the USA and internationally.
- t. **“TSR”** means Telemarketing Sales Rule which specifies rules for sending calls to US consumers which must be followed by callers and carriers allowing calls to traverse their networks.

2. Traceback Investigation Compliance Policy:

a. **Full Cooperation.** MIAMI TELECOM will comply with all Traceback investigations initiated by the industry.

i. **Department Name:** Voice Operations Traceback Group (ITG) and will provide all information requested.

ii. **Contact Person Names:** Charles Sharp

3. **KYC Compliance:** by blocking suspected illegal robocalling by carefully vetting each new prospective customer to eliminate bad actors, upfront, before they have a chance to pass illegal robocalls and other illegal calls that would violate TCPA rules before allowing their traffic to traverse the MIAMI TELECOM network. All prospective new customers first must fill out and sign MIAMI TELECOM's KYC form, which will be vetted, verified, and approved prior to such potential customer being presented with a Company contract, provisioning form, and being allowed access to the MIAMI TELECOM Network. The following table specifies the KYC requirements for onboarding new customers depending upon whether the customer is a USA or foreign based carrier, and whether it is a wholesale Reseller/Aggregator or Enterprise Call Contact Center. Customers not meeting these requirements will not be onboarded unless approved in writing by MIAMI TELECOM senior management.

MIAMI TELECOM KNOW YOUR CUSTOMER POLICY CHECKLIST		USA BASED		FOREIGN BASED	
ITEM NO.	KYC REQUIREMENT by NEW CUSTOMER TYPE	WHOLESALE CUSTOMER	ENTERPRISE CALL CENTER	WHOLESALE CUSTOMER	ENTERPRISE CALL CENTER
1	Check if KYC form is complete and filled out correctly.	?	?	?	?
	Search Applicant name & owner on Google.				
2	Confirm Applicant website is functional, and links are active.	?	?	?	?
3	Confirm Applicant's website logo is not cloned by using 3 rd . party website www.images.google.com	?	?	?	?
4	Confirms Applicant's website domain age using 3 rd party. software www.whois.com	?	?	?	?
5	Confirm Applicant's switch or auto-dialer IP Address using 3 rd party website for blacklist designation. www.abuseipdb.com/check/207.246.84.98	?	?	?	?
6	Confirm Applicant's company address using 3 rd party service.	?	?	?	?

	by Google Maps				
7	Confirm and verify Applicant's FCC 499 Filer ID, Company name and contact information using 3 rd party website. https://apps.fcc.gov/cgb/form499/499a.cfm	?	N/A	?	N/A
8	For US Applicants o to the Secretary of State website Date of customer's company formation. Companies less than 6- months old rejected.	?	?	N/A	N/A
9	Verify USA Applicant's Federal Tax ID using 3 rd party website. www.tinverify.com	?	?	N/A	N/A
10	Verify foreign Applicant's information by using 3 rd party website www.trulioo.com	N/A	N/A	?	?
11	Verify Applicant's Robocall Mitigation Database registration using 3 rd party website for existence and completeness. https://fccprod.servicenowservices.com/rmd?id=rmd_listings	?	N/A	?	N/A
12	Verify Applicant's FCC Registration Number using 3 rd party website. https://fccprod.servicenowservices.com/rmd?id=rmd_listings	?	N/A	?	N/A
13	Verify Applicant's Stir/Shaken implementation by using 3 rd party website. https://fccprod.servicenowservices.com/rmd?id=rmd_listings	?	N/A	?	N/A
14	Search Applicant's contact name in Google with keyword as "FCC" or "FTC" to find any complaints, investigations, or lawsuits and disposition thereof.	?	?	?	?
15	Search Applicant's company name in Google with keyword as "FCC" or "FTC" to find any complaints, investigations, or lawsuits and disposition thereof.	?	?	?	?
16	Check Applicant's ANIs to be used for calling using 3 rd party. website www.youmail.com	N/A	?	N/A	?

17	Check Applicant's CDRs for spoofed ANIs to be used for calling using 3 rd party website www.youmail.com	N/A	?	N/A	?
18	Check Applicant's provided carrier references to verify Applicant company and contact names and traceback history	?	?	?	?
19	Determine Applicant's IP address Geo Location using 3 rd party website www.ipinfo.io for use of foreign IP address.	N/A	?	N/A	?

4. **Know Your Customer's Traffic (KYCT) for New Customers.** For all new customers, and as part of the Company's KYC Policy, and as an added method for vetting customers, upfront, before full production traffic is processed over the MIAMI TELECOM Network, the Company's Traffic Analysis team will monitor customer test and pre-production traffic for suspicious calling patterns consistent with illegal robocalling and also for calls that are in violation of Federal and State laws for telemarketing and for consumer protection. Customers whose traffic is shown to be in violation of such laws, will be prohibited from sending production traffic, and may be prohibited from sending further test and/or pre- production traffic before such new customer is allowed to send full production traffic.
5. To mitigate the potential for illegal traffic entering the MIAMI TELECOM network by new customers who have somehow been able to get past our KYC scrutiny, the following steps will be taken as part of our KYCT protocols.
 - a. **Traffic Separation** Separate trunk groups will be set-up for each customer according to each of the twelve traffic types below. This is due to the fraud monitoring protocols required for each type.

Traffic Origination	Traffic Types	
	Traffic Type	Product
USA	Wholesale Reseller	Short Duration
		Conversational
	Wholesale Aggregator	Short Duration
		Conversational
	Enterprise / Call Center	Short Duration
		Conversational
Foreign	Wholesale Reseller	Short Duration
		Conversational
	Wholesale Aggregator	Short Duration
		Conversational
	Enterprise / Call Center	Short Duration
		Conversational

- b. **Limited Capacity.** Port Capacity shall be limited initially until MIAMI TELECOM has been able to analyze new customer's traffic to make sure it follows robocall mitigation and TPCA rules depending upon the customer type and associated risk.

Traffic Types	USA	
---------------	-----	--

Traffic Type	Product	Originating	Foreign Originating
Wholesale Reseller	Short Duration	500	100
	Conversational	1,000	200
Wholesale Aggregator	Short Duration	500	100
	Conversational	1,000	200
Enterprise / Call Center	Short Duration	500	100
	Conversational	1,000	200

- c. **Filters**. All filters will be set to the highest levels, initially, despite potential revenue loss, until our KYC protocols prove they can be modified. Foreign originating traffic is giving the highest level of scrutiny to help stop illegal robocalls from entering the USA.

NEW CUSTOMER FILTER SETTINGS		USA ORIGINATING IPs			FOREIGN ORIGINATING IPs		
ITEM NO.	ANI FILTER SETTINGS BY CUSTOMER TYPE	WHOLESALE CUSTOMER		ENTERPRIS E CALL CENTER	WHOLESALE CUSTOMER		ENTERPRIS E CALL CENTER
		SHORT DURATION	CONVER-SATIONA L		SHORT DURATION	CONVER-SATIONAL	
1	Spam/Unwanted Threshold	****	****	****	****	****	****
2	TCPA Violation Certainty	?	?	?	?	?	?
3	Fraud Certainty	?	?	?	?	?	?
4	Neighbor Spoofing: Thousand Block	****	****	****	****	****	****
5	Neighbor Spoofing: NPA-NXX Prefix	****	****	****	****	****	****
6	Neighbor Spoof: OCN/LATA/Rate Ctr	****	****	****	****	****	****
7	Neighbor Spoofing: Thousand Block	****	****	****	****	****	****
8	Local Do Not Originate	?	?	?	?	?	?
9	Toll-Free Do Not Originate	?	?	?	?	?	?
10	Wireless	****	****	?	****	****	?
11	Does Not Originate (P-C)	****	****	****	****	****	****
12	Toll-Free Do Not Originate	****	****	****	****	****	****

Note: ****Will be used for suspected abuse or related to Tracebacks as needed.

ITEM NO.	DNIS FILTER SETTINGS BY CUSTOMER TYPE	WHOLESALE CUSTOMER		ENTERPRIS E CALL CENTER	WHOLESALE CUSTOMER		ENTERPRIS E CALL CENTER
		SHORT DURATION	CONVER-SATIONA L		SHORT DURATION	CONVER-SATIONAL	
1	Wireless	N/A	N/A	****	N/A	N/A	****
2	Do Not Call (DNC)	?	?	?	?	?	?
3	404 Filter	?	?	?	?	?	?

Note: DNC filter can be turned off for Call Centers showing proof of opt-in or evidence of an existing business relationship.

6. **New Customer Stir/Shaken Configuration** - New trunk groups are required to have the following settings depending upon Customer Type and whether Customer is based in the USA or internationally. This is required due to the different levels of monitoring attention and call filtering levels to help mitigate illegal robocalling traffic on the MIAMI TELECOM Network and to attest for such calls to help the industry identify bad actors.

NEW CUSTOMER CONFIGURATION RULES		USA ORIGINATING IPs			FOREIGN ORIGINATING IPs		
ITEM NO.	STIR/SHAKEN REQUIREMENT BY NEW CUSTOMER TYPE & DID PROVIDER	WHOLESALE CUSTOMER		ENTERPRISE CALL CENTER	WHOLESALE CUSTOMER		ENTERPRISE CALL CENTER
		SHORT DURATION	CONVERSATIONAL		SHORT DURATION	CONVERSATIONAL	
1	Separate Trunk Groups for Short Duration Traffic, Conversational Traffic and also for Reseller and Aggregator Traffic.	?	?	Designated as SD	?	?	Designated as SD
2	Stir/Shaken Attestation Level for MIAMI TELECOM provided DIDs:	*A Level Attestation	*A Level Attestation	A Level Attestation	**A Level Attestation	**A Level Attestation	A Level
3	Stir/Shaken Attestation Level for 3rd party DIDs for calls that came in <u>unsigned</u> :	C Level Attestation	C Level Attestation	***B Level Attestation	C Level Attestation	C Level Attestation	***B Level Attestation
4	Stir/Shaken Attestation Level for 3rd party DIDs for calls that came as <u>signed</u> :	Calls not signed by MIAMI TELECOM	Calls not signed by MIAMI TELECOM	Calls not signed by MIAMI TELECOM	Calls not signed by MIAMI TELECOM	Calls not signed by MIAMI TELECOM	Calls not signed by MIAMI TELECOM

Note: * Requires calls to be signed by Reseller, otherwise customer does not qualify for MIAMI TELECOM provided DIDs. ** For Resellers selling directly to call centers only--not Aggregators--otherwise MIAMI TELECOM DIDs cannot be provided. *** Customers providing Proof of Ownership or Letter of Authorization from 3rd party DID provider will allow A-level attestation.

7. Traceback Reactive Compliance Policy & Procedures.

- a. **Prompt Response to ITG.** MIAMI TELECOM's Traceback Group shall strive to complete its investigation within 4-hours of receipt of such Traceback request and return the results within 24-hours back to the ITG.
- b. **Follow-on Actions:**
- i. Traceback will be forwarded to the MIAMI TELECOM account manager for follow-up with the Customer.
 - ii. MIAMI TELECOM account manager will take action as defined below to mitigate the traffic source.
 - iii. Response communications between MIAMI TELECOM & Customer will be documented
- c. **Existing Accounts** that are more than three months old are limited to a "Three Strikes" Traceback policy.

EXISTING ACCOUNT POLICY & PROCEDURES ON TRACEBACKS			
STRIKE	TIME PERIOD	SUSPENSION	CUSTOMER REMEDY(S)
1	Within 3-months of start date	Immediate and for 7-days after customer remedy compliance	Customer must agree to specific disclosure of information and corrective action
2	Within 30-days of 1st traceback	Immediate and for 15-days after customer remedy compliance	Customer must sign MIAMI TELECOM Compliance Statement of Corrective Action & pay \$250 fine
3	Within 30-days of 2nd traceback	Permanent	None available

- d. **New Accounts** that are less than 3-months old are limited to a "Three Strikes & You're Out" Traceback & TCPA Violation policy as follows:

NEW ACCOUNT POLICY & PROCEDURES ON TRACEBACKS			
STRIKE	TIME PERIOD	SUSPENSION	CUSTOMER REMEDY(S)
1	Within 30-days of start date	Immediate and for 15-days after customer remedy compliance	Customer must agree to specific disclosure of information and corrective action & pay \$250 fine
2	Within 30-days of 1st traceback	Immediate and for 30-days after customer remedy compliance	Customer must sign MIAMI TELECOM Compliance Statement of Corrective Action & pay \$250 fine
3	Within 30-days of	Permanent	None available

	2nd traceback		
--	---------------	--	--

8. Existing Customer Traceback Compliance Corrective Action Policy:

- a. Customer agrees to provide a screenshot of Traceback Group's notice showing offending underlying customer name. If such an underlying customer is also a direct customer of MIAMI TELECOM, the same Three Strike Policy & Procedures are invoked.
- b. Customer agrees, in writing, to remove offending underlying customer's traffic from being routed to

MIAMI TELECOM.

- c. Customer may be required to groom its traffic to further mitigate the potential for tracebacks.
- d. Customer shall pay fines as set forth above per incidence of Traceback.
- e. For second offense customers, they will be required to sign a Compliance Statement of Corrective Action.

9. Proactive Illegal Robocall Mitigation Policy & Procedures:

- a. Account traffic is subject to ongoing regular random inspection. Calls found with fraud or calls in violation of TCPA & Telemarketing Sale Rules laws are reported to Customer for correction or possible suspension for non-compliance.
- b. First communication to customers for non-compliant calls will ask for corrections and verification of such corrections that have been made.

Illegal Robocall Mitigation & TCPA Rules Policy continued...

- c. Subsequent calls are subject to a \$250 fine and potential service interruption in the event of frequent offenses and/or perception by MIAMI TELECOM that customers' intentions are not genuine.
- d. Customers found to have a recent traceback reported by another carrier besides MIAMI TELECOM are put into the Company's Three Strikes Policy & Procedures.
- e. Email blasts will be sent to customers periodically as needed to keep customers up to date on current or changing TCPA & Illegal Robocall Mitigation rules and best practices.

10. Proactive Telemarketing Sales Rule & TCPA Compliance Protocols. Customer traffic is subject to filtering and analysis by MIAMI TELECOM's Filtering Systems for the following illegal or suspicious activities.

- a. Spoofed ANI calls using invalid or manipulated ANI
- b. Short duration calls using automated dialing machines using a mobile phone ANI.
- c. Short Duration calls sent to customers on the national know Do Not Call list.
- d. Customer traffic is filtered to identify and potentially block calls from ANIs with bad reputations with high probability of being fraudulent.
- e. Calls originating from Toll Free numbers are monitored and blocked for short duration traffic

11. DID Ordering Qualifications: Given that tracking of a DID's/ANI's reputation is a key part of identifying illegal robocalling and bad actors, and given's MIAMI TELECOM's desire to not circumvent such monitoring systems by allowing customers to acquire a fresh DID that will take time to establish a bad reputation, DIDs will only be issued to vetted enterprise call center customers and resellers—not to aggregators for use in robocalling. MIAMI TELECOM will not offer such DID services to its wholesale carrier customers who are aggregators who do not know their underlying customers directly. MIAMI TELECOM will sign for such an authorized customer with the highest attestation level A.

12. Reporting to Authorities: Customers who have shown themselves to be knowingly ignoring or violating Federal and State laws will be reported to the necessary Federal, State, or local government agency responsible for enforcement of such laws.