



All Access Telecom, Inc. specializes in offering voice services, focusing on US Voice Termination for other domestic carriers. It is important to note that All Access Telecom, Inc. does not operate as a Gateway Provider.

Robocall Mitigation Plan

RMD Number: RMD0001366

FRN Number: 0019397843

OCN: 855K

OBJECTIVE:

In this document, All Access Telecom details the procedures, controls, and measures it has in place to fulfill its commitment to monitoring incoming calls and preventing unauthorized and abusive calls from either originating or passing through its network. These actions align with the guidelines set forth by the FCC for the prevention and mitigation of robocalls.

1. **Prohibited Practices for all Customers**

All Access Telecom, included in all agreements executed with its customers, has a clause that prohibits and prevents certain fraudulent and abusive practices by clients and customers. The agreement also includes, as prevention, All Access Telecom's right to block and/or terminate service and the agreement if any of the prohibited practices occur.

The prohibited practices and termination clauses are an integral part of the provisions of the agreements designed to mitigate and prevent illegal robocalling and as such, at execution customers must sign in acceptance.

All Access Telecom's **Prohibited Practices** List as included in its Agreements are as follows:

- i. Any practice or conduct whose purpose is the re-origination of public switched traffic/re-origination of Telephone Calls.
- ii. Traffic masking through false, modified, or fraudulent identification of Telephone Calls with different origination numbers.
- iii. The termination of Telephone Calls or any other type of public traffic switched to End Users avoiding the routes defined for it and the interconnection rates established for concessionaires and authorized for the termination of said Telephone Calls.
- iv. Any conduct indicated in the terms and conditions of the authorized records and FCC/FTC/States regulations applicable to the contracted Service.
- v. Use of Services for illegal purposes that imply or result in the commission of a crime or any administrative offense.
- vi. Any other act prohibited by applicable laws.

2. **Know Your Customer Protocols**

All Access Telecom has established a thorough process that involves conducting due diligence with its customers. This process encompasses the review and collection of the following information:

- Carrier Must Be a US Entity
- Carrier Must Be FCC Registered
- Carrier Must Have an Active 499 Filer ID
- Carrier Must Be Registered on the RMD Database

- Carrier Must Have Active Website and Email Address with Company Domain Name
- Carrier Must Provide Ownership Information (% Ownership and Contact Information)
- Carrier Must Provide a Minimum of two Trade References with Contact Information
- Carrier Must Have US Bank Account and Provide Bank References
- All Payments from Carrier Must be Remitted from a US Bank Account
- Carrier Must Be Stir & Shaken Compliant

3. **Active Traffic Monitoring**

All Access Telecom's NOC monitors all network traffic to assure service and quality for our customers. This is performed on a 24/7 basis.

SCOPE:

Protect our Vendors and Customers from illegal robocalls and conduct active analysis and utilize detailed reporting tools to detect inbound illegal robocalls and abusive calls from bad actors that attempt to traverse our network:

- a. All Access Telecom is a member of the ITG Group.
- b. All Access Telecom is a SOMOS member and an active SOMOS DNO subscriber.
- c. All Access Telecom is a YouMail subscriber.
- d. All Access Telecom is a RRaptor subscriber.
- e. All Access Telecom's NOC team is trained in traffic analysis and operates on a 24/7 basis.
- f. Part of the technical team's tasks are analyzing the entirety of customer traffic that traverses over our Network to detect and determine possible suspicious or malicious traffic patterns.
- g. All Access Telecom follows internal processes to review suspicious traffic and is escalated through our Engineering and commercial teams, in parallel the customer is contacted during the analysis process.
- h. If suspect traffic is detected, the Team will open a trouble ticket with the source customer and depending on the analysis will block the fraud traffic on our network to prevent it from traversing to our vendors.
- i. If the source customer does not cease their fraudulent/abusive profile, the customer will be blocked and faces potential contract termination per agreed terms.
- j. All Access Telecom collaborates with partners to prevent abusive companies from masking traffic.

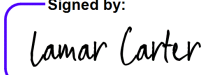
PARTICIPATION:

All Access Telecom is dedicated to adhering to the entirety of federal and state regulatory laws and regulations. We are determined to implement the necessary procedures and take actions aimed at fulfilling our role in the ongoing effort to reduce the prevalence of illegal robocalls and combat fraudulent traffic.

STIR/SHAKEN:

All Access Telecom certifies that it commits to respond 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 originate calls, and that some of the voice traffic that originates on its network is authenticated with STIR/SHAKEN, and the remainder of the voice traffic that originates on its network is subject to a robocall mitigation program. The filer also certifies that the attached searchable PDF details the specific reasonable steps it has taken to avoid originating illegal robocall traffic as part of its robocall mitigation program, and, if applicable, the type of extension or extensions it received under 47 CFR § 64.6304.



Signed by:

1520B3BFB27D40D...

Lamar Carter, CEO

Year - 2026