

ROBOCALL MITIGATION ACTION PLAN

I. INTRODUCTION

The present document details TELNOVO's Robocall Mitigation Plan. TELNOVO, as a service provider, has its own Robocall Mitigation Plan In accordance with Federal Communications Commission (FCC) provisions, which consists of the following measures.

II. OBJECT

The present document outlines, TELNOVO's controls and measures in its commitment to monitor incoming calls and prevent illegal calls originating from its network, in accordance with FCC guidelines on preventing and mitigating robocalls.

1 Prohibited Practices for all Customers.

TELNOVO included in all agreements executed with its clients and customers a clause that prohibits and prevents certain actions (practices) by clients and customers. The agreement also includes, as prevention, TELNOVO's right to terminate service and the agreement if any of the prohibited practices occurs.

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

2 TELNOVO's **Prohibited Practices** List as included in its Agreement 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 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 IFT 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.



As stated, the Agreement includes TELNOVO's right to restrict, suspend and even terminate services to violators of the Prohibited Practices Clause.

3 (KYC) Know your Customer Protocols.

TELNOVO has a process that includes due diligence of information of its clients, that reviews and collects the following information:

- Full Legal Name and Articles of Incorporation.
- Legal I.D. of the person contracting services or the legal representative.
- Proper legal authorization for the legal representative to execute the agreement.
- Proof of Address of Client.
- Tax Record information.
- Credit Check. (if needed)
- Company Website (if needed)
- Contact phone number(s) and email address.

III. MONITORING

TELNOVO's network operation center monitors network traffic to assure the service and quality. This is performed on a 24/7 basis.

Monitoring of Traffic is subject to the following criteria:

a. SCOPE:

- Protect at our own Customers/subscribers from robocalls and have the analysis and reporting tools to detect outbound robocalls from bad actors on our Network, always engaged in cooperating with traceback requests.

b. MONITORING.

- TELNOVO's NOC Technical Team is trained on traffic analysis and is operational on a 24/7 basis.
- Part of the NOC Technical Team tasks is analyzing the traffic coursed over our Network with numbers Source /Destination to detect and determine possible suspicious or malicious traffic patterns.
- The Team proactively monitors traffic statistics and in case of Short Duration traffic is detected, the Team proceeds to open a Ticket with Customers involving the Team, plus Commercial and Executive departments of TELNOVO.
- In case it is suspected or determined of being a robocall, traffic should be routed away from TELNOVO's network immediately – and if they continue to route to TELNOVO, TELNOVO will take further actions, as stated in the present Mitigation Plan.

c. PROTECTING THE NETWORK.

As TELNOVO is committed to comply with all regulatory local laws and enforce the procedures and actions to contribute with our part to mitigate the ROBOCALLING, the following protocol is to be observed to prevent Robocalling and suspicious traffic:

- Analyze and report any abnormal increase or spike of traffic incoming to TELNOVO's Network towards USA.
- Analysis of the data provided by TELNOVO's monitoring and analytics tools to determine if the traffic has an organic or legitimate profile.
- Internally traffic suspicious of being Robocalls is escalated to our NOC team, in parallel the customer is contacted during the analysis process.
- If TELNOVO cannot determine if traffic is Robocall but has enough grounds for suspicious activity, blocking, suspension of Service or termination might be enforced, always in compliance with regulatory laws and the present plan.

a. MITIGATING FRAUD CALLS.

The following actions are actively taken to mitigate robocalling:

- Sharing information and collaboration with partners in order to prevent the fraud companies masking traffic.
- Participate actively with security organizations and local regulators.
- Provide all needed information to trace back calls when TELNOVO gets requests for such information.