



TELEWBCOLOMBIA SAS

Robocall Mitigation Plan (RMP)

This document outlines the steps and commitments undertaken by: TELEWBCOLOMBIA SAS to support the STIR/SHAKEN authentication framework and demonstrates our dedication and proactive commitment to prevent and block illegal or abusive call traffic on our network.

Implementation of STIR/SHAKEN

TELEWBCOLOMBIA SAS is committed to implementing STIR/SHAKEN and includes the deployment of the necessary protocols and technologies to verify the legitimacy of caller ID information and prevent fraudulent use of caller ID.

We will make sure to securely transmit an originator's information and as a voice service provider and Gateway we know the caller and their relationship to the phone number they are using along with the call itself, allowing the destination voice service provider to verify the information on their end.

Steps to prevent illegal or abusive robocall traffic.

We have implemented comprehensive measures to prevent and mitigate illegal robocall traffic, ensuring the security and authenticity of calls on our network.

These measures are associated with our users' specific authorization processes and improve security while preventing fraudulent activity.

- We do not offer an anonymous login option on our network, which also improves user accountability.
- We do not allow our customers to submit a Caller ID that is different from the assigned DID Number (DID).
- In order to register or enable a service for each of our clients, we ask for real and verifiable information such as:
 1. Name of the contact person responsible for the account.
 2. State or country of incorporation of the client.
 3. Description of the nature of the client's business.
 4. The customer's taxpayer identification number or equivalent.
 5. Address for legal and invoicing purposes.

Call Analysis / Proactive Network Monitoring.

We continuously monitor call patterns and traffic on our network to detect and prevent illegal robocall activity. This proactive monitoring allows us to quickly identify and respond to potential threats.

For example, our monitoring systems are able to evaluate traffic based on various criteria, including data related to short-term calls, response rates - rejections, invalid caller ID ANI, and anomalous volumes of 404, 503, and other call failure codes.

If illegal or abusive traffic is detected, the originator or customer is notified so that they can immediately suspend the traffic, otherwise the user or customer is blocked.



Follow-Up Response Commitment.

TELEWEBCOLOMBIA SAS hereby commits to the following with respect to tracking requests:

We are committed to responding fully and within 24 hours to all tracking requests from the Federal Communications Commission (FCC), law enforcement agencies, and the industry tracking consortium.

We will cooperate with these entities to investigate and stop any illegal robocalls that use our service to make or process calls.

Cordialmente,

A handwritten signature in black ink, appearing to read "Lina Medina Leon". Below the signature, the text "CC 24.159.461." is written in a smaller, handwritten font.



LINA MARIA MEDINA LEON
Gerente General

E-mail: contacto@telewebcolombia.com
www.telewebcolombia.com