

Paramaribo, July 21 2022

To: Federal Communications Commission (FCC)

Ref.nr.: DIR-2022/00.201.200

Subject: Fraud, SPAM, Robocall mitigation letter

Dear Sir/madam,

Telesur is a government owned company and the leading telecommunications service provider in land – and mobile voice, broadband and multimedia markets in Suriname.

Telesur with its, high experienced management team, highly skilled engineers and specialists takes irregularities of voice termination, including Robocalls, very seriously.

Telesur has a 24/7 network live monitoring system. Our engineers follow a certain script in case of network performance degradation, network faults, network alarms & concerned notifications from our international partners/carriers.

Our 24/7 monitoring includes a fraud prevention system from Ribbon on which we can monitor, detect, and prevent any potential fraud traffic (including Robocall activities), whether such traffic originates from Telesur network or terminates into Telesur network or transits through Telesur network. We have the capability to create specific fraud detectors modeled to our specific requirements to flag undesired activities within our network. See illustration in Appendix 1.

Telesur continuously improves mitigation steps to cope with potential fraudulent traffic, SPAM and Robocall activities and therefore undertake the following solutions:

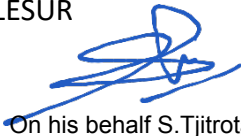
- Detection of callers, generating an unusually large number of calls to a lot of B numbers within a specific time frame;
- Detection of callers generating an unusually large number of short calls to various B numbers within a specific time frame;
- Detection of callers having unusual or incorrect formats and generating a large volume of traffic,
- Application of Blacklists (blocking A-numbers and/or B-numbers);
- Detection of unusual VoIP traffic (SIM Box);
- Detection of CLI Spoofing.

The Fraud control procedure that we have already implement in our program are:

- 24/7 Monitoring: Notification/Detection of unusual/improper high volume of (short) calls within a certain (short) time frame (SPAM/Robocalls/CLI-Spoofing),
- Isolation: Block the "effected" routes or the numbers that generate the calls,
- Inform: In-depth research (technical/Financial/Commercial) and evaluation with all stakeholders,
- Resolve: Final decision from Management how to proceed.

We trust that the above policies are sufficient to comply with the robocall mitigation requirements.

Sincerely,
TELESUR



On his behalf S.Tjitroteno

Mike Antonius MBA
Chief Executive Officer

Appendix 1 Fraud detectors



Create Incident Detectors

Rule Details
The rule details allows for easy identification of a User Defined Rule.

Name:

Description:

Rule Configuration

Incident Type: Time Group:

KPI Set:

Rule Definitions
Rules monitor the generated KPIs and compare values against static thresholds. Set conditions and thresholds for various filters and KPIs. This definition will trigger events when various conditions are met.

Select a Field: Select an Expression: