

TELEFONICA GLOBAL SOLUTIONS USA– ROBOCALL MITIGATION PLAN

This document describes the robocall mitigation program implemented by TELEFONICA GLOBAL SOLUTIONS USA (“TGS USA” or “Telefonica”) to combat the origination of illegal robocalls.

TGS USA will be carrying out the following robocall mitigation program.

- I. TGS USA commits to fully respond to all traceback requests from the FCC, law enforcement, and the industry traceback consortium within 24 hours of receipt of such request, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.
- II. TGS USA commits that all the voice traffic managed on its network is subject to a robocall mitigation program.
- III. TGS USA will only accept traffic for termination from companies that are in the Robocall Mitigation Database.
- IV. TGS USA screens all applicants for its services to determine if they are suspicious of using illegal robocall methods.
- V. TGS USA includes within its agreements some terms designed to prevent new customers or upstream providers from originating illegal calls. These provisions are also being included in contract renewals.
- VI. TGS USA requires its customers to fill in and sign a Know-Your-Customer form where customers provide information about the nature of their traffic and confirm that they do not originate any fraudulent calls.
- VII. TGS USA has a “know-your-upstream provider” procedure in place designed to mitigate illegal robocalls. This procedure works as follows:
 - TGS USA asks its upstream providers to fill in and sign a “know-your-upstream provider” form. The information gathered through this form is:
 - Company details: physical business location, contact person(s), state or country of incorporation, federal tax ID, etc.
 - Nature of the business: retail/wholesale, type of services provided, traffic profile.
 - FCC registration, licensing details, industry traceback status.
 - Information regarding automated dialing/robocall/telemarketing uses.
 - Customers shall maintain updated this information and notify TGS if there is a change in their answers.

- Forms are stored together with their contractual documents.
- VIII.** TGS USA limits how many calls per second customers can make to preventively mitigate bursty traffic patterns. TGS USA analyses its traffic periodically in order to identify any potential risk of calls related to fraud or robocall systems.
- IX.** TGS USA uses call analytics systems to identify and block illegal traffic. These systems work as described in Annex I.
- X.** TGS USA has implemented STIR/SHAKEN to all egress traffic.

ANNEX I - TELEFÓNICA GLOBAL SOLUTIONS: FIGHT AGAINST FRAUD

TGS USA is part of the TELEFONICA GLOBAL SOLUTIONS group. Telefónica has developed the functionalities into its Fraud management solution called TUKU FMS; to detect and take actions on robocalls origination.

- TUKU FMS is the guardian of Telefónica international network against any potential fraud and spam attacks. It surveys in near real time 24/7.
- Telefónica is increasingly challenged by all types of fraud, due to its geographical diversity, different market scenarios and leading market position.
- To address all existing fraud cases, Telefonica Global Solutions has developed TUKU FMS leveraging in Telefonica Group Experience. Thanks to this fully in-house solution, Telefónica is able to prevent, detect and to take action on fraud in outgoing traffic streams (IRSF, avoids 100% IRSF caused by Wangiri), as well as in the incoming traffic streams (By pass, FAS, hijacking and CLI manipulation). There is no tool in the market supervising frauds on both traffic streams.
- And from a security perspective, TUKU FMS safeguards the network by blocking any spam attacks. Additionally, the new functionality to mitigate the robocalls has been developed to comply with the fight against these types of activities.
- This platform is a web solution, hosted in the Telefónica Cloud, 100% configurable by the customer. It applies Big Data Methodology in the initial identification of traffic, combining relational and non-relational storage. It also offers the possibility of bidirectional APIS.
- Our in-house solution is developed as a service to make it available to other carriers in the industry who suffer from fraud, positioning Telefónica as a real anti-fraud provider. And accordingly, the Telefonica operating companies mentioned in the above overview, are under the umbrella of TGS routing facilities and therefore under TGS mitigation robocall tool.



This work has been recognized by the industry in October 2020. TUKU FMS has been awarded in the "Global Carriers Awards" as the best anti-fraud tool on the market, granting it the "Best Antifraud Innovation" award.

Finally, it should be mentioned that Telefónica Global Solutions is an active member of international forums for the fight against the fraud. Among these is the i3Forum, as well as the GLF (Global Leaders Forum). Telefónica Global Solutions supports, complies with and is committed to the global anti-fraud initiative of the "Code of Conduct".

Security and the fight against fraud remain a **key priority** for our company and clients.

TGS has successfully implemented its own solution in order to mitigate the growing phenomenon of Identity Impersonation known by Robocall.

The implemented procedure is described below:

Detection:

1) TUKU FMS monitors traffic, applying filters by:

- a. Origin of A & B numbers
- b. Duration of calls
- c. Dispersion of number B
- d. simultaneous calls

Action:

2) TUKU-FMS generates automatic alarms according to the defined parameters and proceeds to block the calls.

Additionally, Telefónica Global Solutions collaborates to respond to all traceback requests from the FCC, 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, to the extent permitted by law and regulations in each country origin of the calls.

Finally, our International network has been adapted to pass authentication information to the next provider in the chain unaltered.