

Robocall Mitigation Plan

Overview

This document constitutes Claro's Robocall Mitigation Plan. Claro is a Brazilian telecommunications company, owned by América Móvil. A Robocall Mitigation Plan will be deemed sufficient by the Federal Communications Commission (FCC), if the voice service provider:

- includes detailed practices that can reasonably be expected to significantly reduce the origination of illegal robocalls,
- complies with the practices it describes, and
- participates in industry traceback efforts.

1 Objective and Scope

The objective is to define Claro's illegal Robocall Mitigation Plan. Claro's commitment is to prevent, as much as reasonably possible, any illegal calls from originating in its network, as well as monitoring incoming calls to its network.

2 Use Policy

Claro has adopted Acceptable Use Policy ("Política de Uso Justo") and / or Anti-Fraud Policy ("Política Antifraude en el Uso de Servicios Ilimitados") and / or Policy to prevent prohibited practices ("Política para prevenir practicas prohibidas") (collectively, "Policies") that describe prohibited practices and the corresponding consequences of engaging in those practices. The Policies are contained within the service contracts that are available on its website to its customers and subscribers. In accordance with the Policies, customers and subscribers may not use the Claro network, products and / or services to engage in, encourage or promote fraud, including, but not limited to, the use of the Claro platform for dialing, robocalls, telemarketing, high volume fax, text messaging, voicemail transmission or any other transmission that may violate any statute or regulation in the countries where the company operates. The Policies specify that customer access to the Claro network, products and / or services may be restricted or suspended for violation of the Policies, always in compliance with the applicable Brazil regulations.

In the service contract that the client signs with Claro, obligations are established for the client not to use it at any time to carry out the prohibited practices defined in the contract or to use the service for fraudulent, criminal or illegal purposes. Only in some specific service contracts of business client it's allowed some types of telemarketing or robocalls but always in compliance with the applicable Brazil regulations. In those cases, the endcustomer / subscriber can opt to be a part of the national Non-Disturb List. Claro network will block

any telemarketing or robocalls to a subscriber registered on that list.

Under the service contract, depending on the object of the contract, a prohibited practice may include several activities, including: (i) using the service as call center lines for telephone contact campaigns and / or for carrying out and sending advertising, alerts, etc., (ii) using the service as a gateway sending bypass type communications; (iii) using the service for spam-type messages.

If it is detected that the customer engages in any prohibited practice, Claro reserves the right to pursue the administrative, civil and / or criminal actions that correspond permitted under the law; including, suspend totally or partially, temporarily or permanently the provision of services, always in compliance with the applicable laws and regulations.

Robocall Mitigation Plan

3 Know your Customer Protocols.

Claro has a vetting process of its clients and subscribers that includes collecting information, such as:

For Residential/Consumer Services: Claro requires customers to provide their full legal name (as reflected on government identification), residential address (confirmed through verifiable means such as a telephone or electricity bill), contact phone number(s) and email address. New or renewing customers are also required to affirmatively acknowledge and accept Claro's terms and conditions associated with use of the service.

For Enterprise Services: Claro conducts appropriate due diligence on new/renewing customers, such as a credit check, and confirmation of the physical business address. Customers are also required to provide a Certificate of Incorporation and/or company tax number, company website, and a valid email address matching the company domain. Claro also considers whether any enterprise customer has been the subject of: (1) any formal written request from a government agency, subpoena, civil investigative demand, or other complaint; or (2) any lawsuit filed by a regulatory agency, or any other law enforcement action by any other state or federal agency (this review could also include any trade or fictitious names/aliases under which the company operates).

4 Review Existing Contractual Terms and Amend as Appropriate.

Claro includes relevant provisions in its contracts with customers and subscribers that can reasonably be expected to significantly reduce the origination of illegal traffic. For example, Claro includes the following types of provisions:

- Payment Terms: Claro payments through verifiable methods, including checks, debit cards, credit cards, electronic bank transfers, etc. Claro expressly prohibits payment through other non-traceable mechanisms such as gift cards, cryptocurrencies, etc. In

accordance with tax law, Claro limits the acceptance of cash payment by the allowed amount.

- Contractual Provisions: Claro service contracts (particularly for enterprise customers) include provisions that: (a) require the lawful use of the service; (b) prohibit number spoofing; (c) require cooperation with law enforcement requests; and (d) enable Claro to suspend service for customers using the services unlawfully.

5 Monitoring

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

Claro has a continuous monitoring and related reporting protocol to analyze network traffic, such as inbound and outbound high-volume traffic in order to identify unusual spikes and suspicious patterns. Claro also validates international traffic through monitoring platforms to identify patterns of irregular activity and, if necessary, engage in mitigation and control.

6 Investigating Suspicious Traffic

Claro has a multidisciplinary group that is dedicated to collaborate in case of a threshold's control is broken and alarm is triggered or in case of a specific request. Claro takes the following steps once it has identified suspicious traffic:

- (a) Once an anomalous behavior is detected, the customer profile is analyzed with personnel trained in the subject.
- (b) If company personnel is unable to determine the legitimacy of the traffic, the client is contacted and a further investigation is carried out.
- (c) If company personnel is still unable to determine the legitimacy of the traffic, the company proceeds to suspend service, always in compliance with the applicable regulations.

Claro collaborates with other carriers expeditiously and in good faith on any investigation of suspicious activity.

Claro cooperates with industry groups to share best practices and fraud scenarios and discuss solutions that are reasonably designed to minimize prevent illegal, abusive or irresponsible behavior, including, illegal robocalls. For instance, Claro collaborates with the Fraud Security Group of the GSMA.

Lastly, Claro is part of the America Móvil group, which is constantly sharing the experiences of each subsidiary with respect to fraudulent activities -- including illegal robocalls -- as well as best practices to quickly detect and prevent such practices. This permits the subsidiaries

to benefit from each other's experiences and solutions.

7 Suspending/Mitigating Illegal Traffic.

When suspicious traffic has been identified and verified with further investigation, the client or subscriber's service may be suspended, according to the local requirements regulations.

As of June 2022, Anatel published some measures to combat the volume of abusive calls, with the determination to block users for 15 (fifteen) days that generated a volume of short calls (incomplete and completed with a duration of up to 3 seconds) greater than the stipulated limits and the obligation to use the number 0303XXXXXXX for telemarketing calls. Such measures were faithfully implemented by CLARO, which contributed to significantly reducing the volume of abusive calls and complaints.

Measures to combat abusive calls have been improved by Anatel since 2022, with the alteration of the concept of short calls (for those not completed or destined for voicemail and, when completed, lasting up to 6 seconds) and the elimination of the mandatory use of the number 0303XXXXXXX for telemarketing calls, in view of new rules for the implementation of mandatory call authentication.

Starting in 2023, Anatel has been encouraging and coordinating a working group with telecommunications providers to implement the STIR SHAKEN call authentication and identification protocol in the country's telecommunications networks. Initially, adoption of the protocol was optional and applied only to corporate clients. From January 2026, all users who make more than 500,000 calls per month must contract the call authentication service from their telecommunications providers, and from October 2028, all calls must be routed by providers in an authenticated manner.

8 Participation in fraud-centric industry organizations.

Currently AMX subsidiaries are members of the Fraud and Security group of the GSMA and the TM-Forum.

9 U.S.-bound Voice Traffic

Claro's traffic originating on its network enters the USA through intermediate operators which are listed on the FCC's Robocall Mitigation Database as having either deployed the STIR-SHAKEN solution or having an appropriate robocall mitigation plan in place.

10 Glossary

FCC U.S. Federal Communications Commission
Claro Brazilian subsidiary of América Móvil

STIR Secure Telephony Identity Revisited. Standardized by IETF and defines a signature to verify the calling number, and specifies how it will be transported in SIP

SHAKEN Signature-based Handling of Asserted information using toKENs. Framework developed by the ATIS/SIP Forum IP-NNI task force to provide STIR implementation profile for service providers, STIR & SHAKEN will be the basis for authenticating calls and facilitating the ability to trust the caller ID information.