

Claro Chile, SpA.

Robocall Mitigation Plan (April 2024)

Overview

This document constitutes Claro Chile SpA's Robocall Mitigation Plan. Claro Chile, SpA. is a Chilean telecommunications company.¹ 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.

A. General/Contact Information

Business name: Claro Chile, SpA.

Primary address: Avenida El Salto 5450. Comuna de Huechuraba, Santiago, Chile. Zip Code: 8580000.

Other business name(s) in use: none.

All business names previously used: Claro Chile, S.A.

Information on the provider's principals, affiliates, subsidiaries, and parent companies:

- Claro Chile, SpA. is a 50:50 joint venture of América Móvil, S.A.B. de C.V. and Liberty Latin America, Ltd. As of the date of this filing, the company's officers and directors are: Alfredo Parot Donoso, Pedro Assael Montaldo, Francisco Guzmán Marín, Patricio Olivares de la Barra, René Caracci Larraguibel, David Carlevarino Weitzel, Jorge Ebensperger Loo, Luz María Antúnez Fernández, Miguel Oyonarte Weldt, Cristián Salgado Padilla, and Juan Vasquez Cordova.

Additional information about Claro Chile, SpA. is available on the company's website at <https://www.clarochile.cl/institucional/informacion-corporativa/>.

Is the provider a foreign provider: Yes

Name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation-related issues:

Name: Eduardo Guzman Florez.

Title: Head of International Roaming and International Long Distance.

Contact Department: Interconnection and International Roaming.

Business Address: Avenida El Salto 5450. Piso 11. Comuna de Huechuraba, Santiago, Chile.

Zip Code: 8580000.

Telephone number: +56990154517.

Email address: eduardo.guzmanflorez@clarovtr.cl.

¹ On October 6, 2022, América Móvil entered into an agreement to combine its Chilean operations with Liberty Latin America, Ltd. ("LLA") to create Claro Chile, SpA, a 50:50 joint venture. As a result of the joint venture, Claro Chile, S.A. ceased to be a wholly owned subsidiary América Móvil.

Claro Chile, SpA.
Robocall Mitigation Plan (April 2024)

Operating Company Number (OCN): Given its status as a foreign voice service provider Claro Chile, SpA. does not have an OCN.

B. Provider Classification Information

1. Role the provider is playing in the call chain: Claro Chile, SpA. is a foreign provider.
2. STIR/SHAKEN Implementation Status: Not applicable because Claro Chile, SpA. is a foreign provider.

C. Certifications

1. Filling in the Robocalling Mitigation Database:

Claro Chile, SpA. certifies its prior certification filed in the Robocall Mitigation Database (“RMD”) has not been removed by FCC action, nor has it been prohibited from filling in the RMD pursuant to a law enforcement action.

2. Enforcement Actions and Investigations:

Claro Chile, SpA. is not subject to an FCC, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing. Furthermore, neither Claro Chile, SpA. nor any entity with which Claro Chile, SpA. shares common ownership, management, directors, or control, has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to Claro Chile, SpA. transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description in the prior two years.

3. Responses to Traceback Requests:

Consistent with the domestic laws and regulations to which it is subject in its country of operation, Claro Chile, SpA. will seek to respond to all traceback request from the FCC, the FCC’s designated traceback consortium, and law enforcement agencies within 24 hours.

ROBOCALL MITIGATION PLAN

The plan below describes how Telcel is meeting its obligation to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls.

1. Objective and Scope

The objective is to define Claro Chile, SpA.’s Robocall Mitigation Plan. Claro Chile, SpA.’s commitment is to prevent, as much as reasonably possible, illegal calls (robocalls) from originating in its network, as well as monitoring incoming calls to its network.

Claro Chile, SpA.

Robocall Mitigation Plan (April 2024)

2. Use Policy

Claro Chile, SpA. has adopted Acceptable Use Policy (“Política de Uso Justo”) that describe prohibited practices and the corresponding consequences of engaging in those practices. The Company makes the Policies available on its website to its customers and subscribers. In accordance with the Policies, customers and subscribers may not use Claro Chile, SpA.’s network, products and/or services to engage in, encourage or promote illegal or abusive behavior including, but not limited to, the use of Claro Chile, SpA.’s platform for dialing, robocalls, telemarketing, high volume fax, text messaging, voicemail transmission or any other transmission that violates any statute or regulation in the countries where the company operates. The Policies specify that customer access to Claro Chile, SpA.’s network, products and/or services may be restricted or suspended for violation of the Policies, always in compliance with the applicable regulations.

In the service contract that the client signs with Claro Chile, SpA. obligations are established for the client to use the contracted service only for their personal use, and not to use it at any time to carry out the prohibited practices defined in the contract.

Under the service contract, a prohibited practice includes 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; and (iv) using the service for fraudulent, criminal, or illegal purposes.

If it is detected that the customer engages in any of the aforementioned prohibited practice, Claro Chile, SpA. 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.

3. Know your Customer Protocols

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

- For Residential/Consumer Services: Claro Chile, SpA. 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 Chile SpA.’s terms and conditions associated with use of the service.
- For Enterprise Services: Claro Chile, SpA. 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

Claro Chile, SpA. Robocall Mitigation Plan (April 2024)

company tax number, company website, and a valid email address matching the company domain.

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

- **Payment Terms:** Claro Chile, SpA. payments through verifiable methods, including checks, debit cards, credit cards, electronic bank transfers, etc. Claro Chile, SpA. prohibits payment through other non-traceable mechanisms such as gift cards, cryptocurrencies, etc. In accordance with tax law, Claro Chile, SpA. limits the acceptance of cash payment by the allowed amount.
- **Contractual Provisions:** Claro Chile, SpA. 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 Chile, SpA. to suspend service for customers originating illegal robocalls, or otherwise using the services unlawfully.

5. Monitoring

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

Claro Chile, SpA. 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. The Company 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 Chile, SpA. has a multidisciplinary group that is dedicated to collaborating in case an alarm is triggered or in case of a specific request.

The Company 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.

Claro Chile, SpA.
Robocall Mitigation Plan (April 2024)

- (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 Chile, SpA. collaborates with other carriers expeditiously and in good faith on any investigation of suspicious activity.

Claro Chile, SpA. 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 Chile, SpA. collaborates with the Fraud Security Group of the GSMA.

7. Suspending/Mitigating Illegal Traffic

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

8. Participation in fraud-centric industry organizations

As previously indicated, Claro Chile, SpA. collaborates with the Fraud Security Group of the GSMA.

9. U.S.-bound Voice Traffic

Claro Chile, SpA.'s traffic originating on its network enters the United States 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. Call Analytics Systems

Claro Chile, SpA. utilizes its own internal resources, systems, and frameworks to analyze its network for suspicious robocall traffic and does not rely on third-party call analytics systems.

11. Glossary

FCC: U.S. Federal Communications Commission.

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.