

ROBOCALL MITIGATION PLAN

Puerto Rico Telephone Company, Inc.

February 2024



Table of Contents

I. Objective and Scope	1
II. Claro PR's Robocall Mitigation Procedures as an Originating Provider	1
A. Use Policy (Website Terms & Conditions)	1
B. Know your Customer Protocols (Policy CL-030-A)	2
C. Review Existing Contractual Terms and Amend as Appropriate	4
III. Claro PR's Robocall Mitigation Procedures as an Intermediate Provider	5
A. Know your Upstream Provider Protocols	5
B. Review Existing Contractual Terms and Amend as Appropriate	6
IV. Claro PR's Robocall Mitigation Procedures as a Gateway Provider	6
V. Claro PR's General Robocall Mitigation Procedures	7
A. Monitoring	7
B. Investigating Suspicious Traffic.....	7
C. Suspending/Mitigating Illegal Traffic.....	8
D. Participation in Fraud Prevention-Centric Industry Organizations	8
VI. Certifications	8
VII. Glossary	8

Overview

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 traceback efforts. This document describes Puerto Rico Telephone Company, Inc. dba Claro Puerto Rico’s (hereinafter “Claro PR”) practices to reduce and effectively mitigate the origination of non-IP illegal calls and robocalls. These practices, jointly with others, such as STIR/SHAKEN implemented for all IP traffic, are part of the efforts taken by Claro PR to maintain the proper and legal use of its fixed and wireless networks.¹

Claro PR offers a variety of services and plays different roles in the call chain. Specifically, Claro PR provides service as a call originator, an intermediate provider, and a gateway provider. It does not, however, provide service through its SIP network as an intermediate provider or a gateway provider.

Claro PR has policies and procedures in place for the following requirements:

- Implement measures to prevent customers from using our network to originate illegal calls.
- Take steps to mitigate illegal traffic upon receiving written notification of such traffic from the FCC, the ITG, or law enforcement.
- Implement full STIR/SHAKEN.
- Implement robocall mitigation on the sending and receiving side of our network.
- Respond to traceback requests from the FCC, the ITG, as well as civil and criminal law enforcement, and cooperate with them.

I. Objective and Scope

Our main objective is to define Claro PR’s Robocall Mitigation Plan. Our commitment is to ensure the appropriate use of our network, taking actions to prevent its use to originate illegal calls, monitoring incoming calls that our customers receive, as well as cooperating with the appropriate parties to mitigate the risk of illegal calls.

II. Claro PR’s Robocall Mitigation Procedures as an Originating Provider

A. Use Policy (Website Terms & Conditions)

Claro PR has adopted policies, such as the Acceptable Use Policy (“Política de Uso Justo”) and Anti-Fraud Policy, to inform our customers about prohibited practices and illegal acts, as well as the consequences of engaging in them. Those policies are published on our corporate website: www.claropr.com.

Our policies provide that our retail fixed voice services are not for resale. Our customers are prohibited from using the equipment for illegal or improper purposes in a way that may cause

¹ Fixed Network Claro PR’s OCN: 667C; 3201. Mobile Network Claro PR’s OCN: 4823

damage or risk of damage to Claro PR, its employees or facilities, or the public. Our customers are also required to use the service in accordance with the law, and state and federal regulations. For purposes of our fixed voice services policies, improper use includes (a) reselling or rebilling the service; (b) using the service to engage in illicit activities or behavior that adversely affect Claro PR's customers, employees, business or other people, or that interferes with Claro PR's operations, network, reputation or ability to provide quality service; (c) accessing or attempting to access third-party information, accounts or equipment without authorization; (d) transferring or attempting to transfer Claro PR's networks or systems to other entities; and (e) abusive use of the service, as stated in our policies and federal and local laws and regulations. The illegal use of the service or the failure to follow our policies, terms, and conditions will grant Claro PR the right to suspend the service.

Unlimited voice service plans are offered solely for the purpose of allowing the customer to engage in direct voice communication with another person or other persons. Unlimited voice services offerings may not be used for repeated call forwarding, monitoring services, transfer of data, programs or stored material, or any other connections that do not include a direct, uninterrupted dialog between individuals, or similar purposes. If Claro PR, in its sole discretion, concludes that the customer is using any unlimited voice service plan for a purpose other than direct voice communication between persons, Claro PR may suspend the service.

Our broadband voice over internet protocol service ("VoIP") is offered to business and enterprise customers for their use as end-users and for direct voice communication between persons. Customers acknowledge and accept that all other uses (e.g., monitoring services, use of equipment as a modem for Internet service, transmission or broadcast of recorded materials, telemarketing, auto-dialed calls, and call transfers or other similar connections), fraudulent use, or reselling of the service is considered an abusive behavior and/or a misuse of the service. Customers acknowledge and accept that the illegal use of the service may cause its suspension.

B. Know your Customer Protocols (Policy CL-030-A)

Claro PR requires all new subscribers to sign a contract after having completed a vetting process. Our vetting process includes collecting information to verify the new subscriber's identity.

1. For Residential/Individual Retail Services

A residential or individual new subscriber interested in our products and/or services must first complete an identity verification process, which is carried out by one of our sales representatives ("SR"). This identity verification process consists of three steps. Each one of these steps must be fulfilled to get to the next step.

a. First Step: Physical and detailed review of the residential/individual new subscriber

Claro PR's services can only be sold to persons (21 years in Puerto Rico). If the person is under 21 years of age but is emancipated, he or she must submit an Emancipation Certificate or Certificate of Marriage issued by Puerto Rico's Demographic Registry.

Claro PR accepts the following personal identification documents:

1. Driver's license
2. Real ID Card
3. Passport
4. Identification card issued by a state

Any of the above identifications must be accompanied by a utility bill or housing rental agreement. Sales representatives are not authorized to request or accept any other document for purposes of verifying a residential/individual new subscriber's identity. Any exceptions to this rule must be authorized by the Fraud Control Team Manager.

The residential/individual new subscriber's request of service is denied if the photo in the personal identification document does not match the physical appearance, or if the personal identification document seems to be forged or altered. After verifying the residential/individual new subscriber's identity documents, the SR must proceed to the second step.

b. Second Step: Social Security Number Verification

This verification is done using an online tool provided by a credit bureau. Through this tool, the SR verifies that the social security number is valid and confirms whether it belongs to the residential/individual new subscriber. If this verification fails, the request for service must be denied. If approved, the SR must proceed to the next step.

c. Third Step: Questionnaire about Personal Information and Credit Ratings of the Residential/Individual New Subscriber

Claro PR, in coordination with a credit bureau contracted for this purpose, evaluates the information provided by the new subscriber. If such validation is not achieved on the first attempt, the SR will make a second attempt using another questionnaire. If the new subscriber does not pass the third step of the identity verification process, but the SR concludes that the consumer is the person identified by means of the first and second steps, the SR can seek approval with the Commercial Operations Department through Claro PR's special procedures.

2. For Enterprise Services

Any company or government agency interested in purchasing our voice services must first undergo an identity verification process. Claro PR conducts due diligence on new subscribers, such as a credit check, confirmation of the physical business address, company website, and a valid email address matching the company's domain name. Government agencies are not subject to the credit validation process. Our identity verification process is carried out by an SR, and it includes a physical and detailed review of the enterprise identification documents submitted.

The identification documents requested by Claro PR are the following:

1. Certificate of Incorporation (or certification establishing that the enterprise is not incorporated under the Puerto Rico State Law) issued by the Puerto Rico Department of State.
2. IRS document. If the enterprise does not have the document issued by the IRS, one of the following documents can be accepted if it contains the Employer Identification Number, Employer Social Security Number, or Tax ID:
 - a. Municipal Patent;
 - b. Certificate of Contribution;
 - c. Debt Certificate from the Puerto Rico Treasury Department;
 - d. Federal Government Form 8109 (Federal Tax Deposit Coupon); or
 - e. Copy of the tax return filed for the previous year signed and stamped

If the identification documents appear to be forged or altered, the new subscriber's request for service is denied. Claro PR also considers whether any enterprise 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.

C. Review Existing Contractual Terms and Amend as Appropriate

Claro PR's service contracts with end-users include provisions and contractual terms that are expected to significantly reduce the origination of illegal robocalls. Such terms include, but are not limited to, the following:

Payment Terms: Claro PR only accepts payments through verifiable methods, including checks, debit cards, credit cards, electronic bank transfers, etc. Claro PR expressly prohibits payment through other, non-traceable mechanisms such as gift cards (other than Visa, MasterCard or American Express gift cards), bitcoin and cryptocurrencies. Claro PR limits the acceptance of cash payment to residential and individual customers when it is made in person at a Claro PR's location after an identity validation process is completed.

Contractual Provisions: Claro PR's agreements include provisions that require the lawful use of the service, prohibit number spoofing, and enable Claro PR to suspend the service of any customer originating illegal robocalls or otherwise using the service unlawfully. Our agreements also allow us to determine that a use is unreasonable or abusive, which may lead to the suspension or termination of the service. In Claro PR's agreements, we have adopted the concept of "improper use". The use of a service would be deemed improper when : 1) the service is used for non-personal or resale purposes (excluding wholesale customers); 2) when there is no direct and live dialogue between persons; 3) the service is used fraudulently, contrary to local and federal regulatory provisions of the service or for an illegal purpose; 4) if mobile services are used outside of Claro PR's network for two consecutive months exceeding the usage on Claro PR's network; and 5) when the service is misused.

For purposes of our contracts, a customer misuses the service when it: (a) resells or re-bills our service; (b) uses our service or equipment to engage in illegal activities or behave in a way that adversely affects our customers, employees, businesses, or other person(s), or that interferes with our operations, network, reputation, or ability to provide quality service, including, among others, the generation or dissemination of viruses, malware or "denial of service"; (c) sends unsolicited bulk messages or other abusive forms of communication, or unsolicited or any other type of automated massive voice or communications for commercial purposes; and/or (d) collaborates or engage with others in any of the activities mentioned above.

III. Claro PR's Robocall Mitigation Procedures as an Intermediate Provider

Claro PR requires all new subscribers of wholesale services to sign a contract after having completed a vetting process. Our vetting process includes collecting information to verify the new subscriber's identity.

A. Know your Upstream Provider Protocols

Claro PR Wholesale Department verifies the identity of all third-party service providers with which Claro PR exchanges voice traffic as an intermediate provider. These providers include interexchange carriers ("IXCs") and third-party providers of telecommunications services in Puerto Rico.

The identity verification process includes the collection of the following information:

- a. Name of the company
- b. Commercial name as it will appear in the invoice
- c. Place of incorporation
- d. Name of the person signing the contract, as well as title, civil status, home address, and telephone
- e. Postal and physical address
- f. Email and telephone
- g. Tax Identification Number
- h. Type of organization
- i. Copy of the certificate of incorporation
- j. Identity of the person who will sign the Master Agreement
- k. OCN number
- l. CLII code
- m. ACNA Code

In the case of wholesale service providers that provide telecommunications services in Puerto Rico, Claro PR also verifies whether the provider is certified by the Puerto Rico Telecommunications Bureau as a provider of telecommunications services in Puerto Rico.

B. Review Existing Contractual Terms and Amend as Appropriate

Payment Terms: Claro only accepts payments via wire transfer from wholesale customers.

Contractual Provisions: Claro PR's service agreements with other voice service providers for the exchange of local traffic generally include provisions and contractual terms that are expected to significantly reduce the origination of illegal robocalls. Such terms include, but are not limited to, the following:

- Audit provisions allowing Claro to audit books, call detail records, data, reports, and other records, documents, and materials to determine the traffic type and volume of traffic exchanged with Claro accuracy of invoices, and compliance with terms and conditions.
- Provisions requiring providers to cooperate fully with one another to investigate, minimize, and take corrective action in cases of fraud.
- Provisions requiring providers to exchange information required to comply with requirements of law enforcement and national security agencies.
- Provisions allowing Claro to suspend or terminate services when the network or methods of operation of the provider impair or are likely to impair Claro's network.
- Provisions allowing for the termination of the agreement in case of default.
- Provisions requiring consent for the assignment of rights under the agreements.
- Provisions requiring the parties to work cooperatively to minimize fraud associated with any services provided under the agreement.
- In the case of more recent agreements, provisions requiring registration in the Robocall Mitigation Database and warning that noncompliance could lead to blocking of routed calls.

Claro's service agreements with interexchange carriers ("IXCs"), including IXCs that deliver international traffic, also generally include provisions and contractual terms that are expected to significantly reduce the origination of illegal robocalls. Such terms include, but are not limited to, the following:

- Provisions allowing for the termination of the agreement for any reason.
- Provisions requiring the providers to cooperate on all issues related to fraud or misuse of Claro's telecommunications network.
- Provisions requiring consent for the assignment of rights under the agreements (other than in cases of assignments to affiliates).
- Provisions requiring the providers to represent and warrant compliance with applicable laws and regulations.
- In the case of more recent agreements, provisions requiring registration in the Robocall Mitigation Database and warning that noncompliance could lead to blocking of routed calls.

IV. Claro PR's Robocall Mitigation Procedures as a Gateway Provider

The robocall mitigation procedures that apply to Claro as a gateway provider are the same as those that apply in its role as an intermediate provider, as set forth in Part III above. When Claro

originates or terminates traffic as a gateway provider, the robocall mitigation procedures set forth in Part V also apply.

V. Claro PR's General Robocall Mitigation Procedures

A. Monitoring

Claro PR's Network Operation Center ("NOC") constantly monitors the traffic that originates or terminates in its network to assure quality of service and detect anomalous traffic on a 24/7 basis.

Active robocall deterrence measures include monitoring for suspicious traffic, such as high-volume, short-duration, spoofed calls, and/or low termination rates. Our fraud management system monitors all incoming and outgoing long-distance traffic and alerts when defined rules thresholds are exceeded.

In addition, a third-party service (BICS FraudGuard Service) is used to actively monitor the network for suspected illegal robocall traffic. This 24/7 service monitors all the long-distance traffic routed to the USA by one of Claro's main IXCs and prevents fraud incidents in real-time by blocking most of the fraudulent call attempts and alerting against new fraud destinations or suspicious traffic identified through the CDR analysis of other carriers' routed traffic.

Claro is currently evaluating additional tools to monitor traffic exchanged with third-party providers in its capacity as an intermediate provider and a gateway provider.

B. Investigating Suspicious Traffic

As it relates to traffic that originates or terminates in its network, Claro PR has adopted processes and procedures for handling alerts produced by our fraud management systems for our voice services during regular hours, night hours, weekends, and holidays, with the support of the NOC and the Fraud Prevention Department. For any service that exceeds the minute or number of calls parameters defined by type of voice traffic (long domestic distance or international long distance), an alert is generated.

Once an alert is received, we analyze the details of the call records to identify fraudulent and/or illegal use of our network. Alerts are automatically sent via email and text messages to fraud analysts, supervisors, managers, and NOC-front office supervisor, who process the alerts according to the adopted schedules and protocols.

Those alerts generated during working hours (Monday through Friday (8AM to 5PM EST)) are handled by the Fraud Division staff. The alerts produced during night hours, holidays, and weekends are handled by the NOC-Front Office Supervisor and sent to the Fraud Department staff.

If the Fraud Prevention Staff concludes that the network was used for fraudulent activities and/or illegal robocalling or calls, the service will be suspended. Then, the customer is notified by email, text message, or phone call that the service has been suspended.

As a member of the ITG, Claro PR is committed to collaborating with other carriers expeditiously and in good faith on any investigation of suspicious activity. Claro PR has implemented an internal Traceback Procedure to handle traceback requests from this consortium.

Claro PR also cooperates with other industry groups to share best practices and fraud scenarios and discuss solutions that are reasonably designed to minimize and prevent illegal, abusive, or irresponsible behavior, including, illegal robocalls. For instance, Claro PR, as a subsidiary of América Móvil (“AMX”), collaborates with the Fraud Security Group of the GSMA.

Lastly, the AMX group 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 AMX subsidiaries, including Claro PR, to benefit from each other’s experiences and solutions.

C. Suspending/Mitigating Illegal Traffic

When suspicious traffic that originates or terminates in Claro PR’s network has been identified and verified with further investigation, the client or subscriber’s service is immediately suspended, consistent with local and federal regulations, and following Claro PR’s established internal procedures.

D. Participation in Fraud Prevention-Centric Industry Organizations

Claro PR, as a subsidiary of AMX, is a member of the Fraud and Security group of the GSMA and the TM-Forum. In addition, Claro PR has established a process to provide information requested by the ITG to trace the origin of the alleged illegal robocalls originating in or transiting through the Claro PR Network.

VI. Certifications

- Claro PR is not prohibited from filing in the Robocall Mitigation Database.
- Claro PR will respond to traceback requests within 24 hours.
- Claro PR is not subject to a Commission, law enforcement, or regulatory agency action or investigation.
- Neither Claro PR nor any entity with which it shares common ownership, management, directors, or control has been subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient RMD certification or mitigation program description.

VII. Glossary

AMX	América Móvil
CDR	Call Detail Record

FCC	Federal Communications Commission
ITG	Industry Traceback Group
IXC	Interexchange Carrier
RMD	Robocall Mitigation Database
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.