

Robocall Mitigation Plan (revised)

Overview

This document constitutes the Robocall Mitigation Plan for Empresa Nicaragüense de Telecomunicaciones S.A. ("Enitel"). Enitel is a Nicaraguan 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.

A. General/Contact Information

Business name: Empresa Nicaragüense de Telecomunicaciones S.A.

Primary Address: Edificio Eliseo Duarte 3 piso, Claro Villa Fontana, Managua, Nicaragua

Other business name(s) in use: None

All business names previously used: None

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

- The company is a wholly owned subsidiary of América Móvil, a Mexican holding company. The company's affiliates in the United States include LATAM Telecommunications, LLC, Puerto Rico Telephone Company, Inc. d/b/a Claro Puerto Rico, and Claro Enterprise Solutions, L.L.C. As of the date of this filing, the company's officers and directors are Antonio Vega and Edwin García.

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: Ivonne Mayorga Lopez

Title: Carrier International

Department: Regulación e Interconexión

Business Address: Edificio Eliseo Duarte 3 piso, Claro Villa Fontana, Managua, Nicaragua

Telephone number: +505 57218888

Email address: ivonne.mayorga@claro.com.ni

Operating Company Number (OCN): Given its status as a foreign voice service provider, Empresa Nicaragüense de Telecomunicaciones S.A. does not have an OCN.

B. Provider Classification Information

1. Role the provider is playing in the call chain: Empresa Nicaragüense de Telecomunicaciones S.A. is a foreign provider.

Robocall Mitigation Plan (revised)

2. STIR/SHAKEN Implementation Status: Not applicable because Empresa Nicaragüense de Telecomunicaciones S.A. is a foreign provider.

C. Certifications

1. Filing in the Robocalling Mitigation Database:

Empresa Nicaragüense de Telecomunicaciones S.A. certifies its prior certification filed in the Robocall Mitigation Database (“RMD”) has not been removed by FCC action, nor has it been prohibited from filing in the RMD pursuant to a law enforcement action.

2. Enforcement Actions and Investigations:

Empresa Nicaragüense de Telecomunicaciones S.A. is not subject to a Federal Communications Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing. Furthermore, neither Empresa Nicaragüense de Telecomunicaciones S.A. nor any entity with which Empresa Nicaragüense de Telecomunicaciones S.A. 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 Empresa Nicaragüense de Telecomunicaciones S.A. 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, Empresa Nicaragüense de Telecomunicaciones S.A. 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 Empresa Nicaragüense de Telecomunicaciones S.A. 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 Enitel Robocall Mitigation Plan. Enitel’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.

2. Use Policy

Enitel 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

Robocall Mitigation Plan (revised)

para prevenir practicas prohibidas”) (collectively, "Policies") 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 the Enitel network, products and / or services to engage in, encourage or promote, including, but not limited to, the use of the Enitel 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 the Enitel 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 Enitel, 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; (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, Enitel 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. Enitel has a vetting process of its clients and subscribers that includes collecting information, such as:

For Residential/Consumer Services: Enitel 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 Enitel's terms and conditions associated with use of the service.

For Enterprise Services: Enitel 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.

Enitel 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).

Robocall Mitigation Plan (revised)

4. Review Existing Contractual Terms and Amend as Appropriate

Enitel 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, Enitel includes the following types of provisions:

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

5. Monitoring

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

Enitel 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. Enitel 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

Enitel 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.

Enitel 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.

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

Enitel 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, Enitel collaborates with the Fraud Security Group of the GSMA.

Robocall Mitigation Plan (revised)

Lastly, Enitel 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 is immediately suspended, according to the local requirements regulations.

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

Enitel'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. Call Analytics Systems

Enitel 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.

Glossary

FCC	U.S. Federal Communications Commission
Enitel	América Móvil subsidiary
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.