



UC Telecomunicaciones, S. A. P. I. de C. V. Robocall Mitigation Plan

1. Introduction

UC Telecomunicaciones, S. A. P. I. de C. V., is a Mexican company with a concession granted by the *Comisión de Regulación de Telecomunicaciones "CRT"* (formerly, *Instituto Federal de Telecomunicaciones "IFT"*).

This plan outlines the measures implemented to mitigate fraudulent call traffic and ensure compliance with international regulations, including those of the Federal Communications Commission "FCC" for calls terminating in the United States.

2. Description of Operations

- UC Telecomunicaciones operates primarily in Mexico but may route traffic to the United States through authorized compliant carriers.
- Calls to the U.S. are terminated via partners that comply with FCC standards.
- UC Telecomunicaciones does not use its own IP networks for direct U.S. termination, but participates in the transport of traffic.

3. Robocall Mitigation Strategies

UC Telecomunicaciones uses proprietary software and monitoring tools to prevent the origination of illegal robocalls.

3.1 Customer and Partner Validation

- All customers and partners undergo pre-activation screening.
- Legal documentation is reviewed to verify identity, licenses, and permits.
- Ongoing monitoring ensures that unusual or suspicious activity is detected.

3.2 Real-Time Traffic Monitoring

- Analytical tools detect irregular traffic patterns.
- High-risk calls are identified and blocked, including:
 - Calls with unusually short duration
 - Numbers associated with fraud
 - Abnormal call volumes on specific routes

3.3 Traceback Response

- Full cooperation with regulatory authorities (FCC and CRT) to respond to traceback requests.

JSJS JAH AS SMA



- Rapid identification of the source of suspicious calls and suspension of traffic if fraud is confirmed.

3.4 Training and Awareness

- Regular training for operational teams to detect and mitigate fraudulent activity.
- Communication with customers regarding acceptable use policies and consequences of non-compliance.

4. Technical Measures Implementation

4.1 STIR/SHAKEN

- UC Telecomunicaciones does not operate a U.S. IP network that supports STIR/SHAKEN, but ensures cooperation with U.S. carriers implementing the protocol.

4.2 Proactive Call Blocking

- Systems configured to automatically block suspicious calls based on:
 - Blacklists from recognized fraud databases
 - Indicators of illegal or high-risk traffic

5. Know Your Customer

- Customers are assessed to ensure they do not engage in illegal robocalling.
- Continuous monitoring of traffic for patterns of known abuse.
- Immediate action is taken when illegal traffic is detected.

6. Know Your Upstream Provider

- Verification of RMD registration and compliance for all U.S. traffic routes.
- Confirmation of traceback participation for upstream providers.
- Traffic from non-compliant providers may be blocked or suspended.

7. Commitment to Compliance

Registration in the RMD to inform authorities about the mitigation measures in place.

Regular reporting of suspicious activities to the relevant authorities.

gds MAA AS SMA



8. Record Retention

Records related to U.S. traffic are maintained for a minimum of five (5) years, consistent with CRT record retention requirements.

I certify under penalty of perjury that: (i) UC Telecomunicaciones has implemented the mitigation practices described herein; (ii) UC Telecomunicaciones actively monitors and enforces its robocall mitigation program and; (iii) the information provided is true and accurate.

Simon Masri

Simon Masri
Authorized Representative

JMS MHA AS