



Robocall Mitigation Plan.

Prepared by Telecable - Voz y Datos

Document date
September, 2021.

NOTICES

This document is protected under the copyright laws of Costa Rica and other countries as an unpublished work. This document contains information that is proprietary and confidential to TELECABLE S.A. or its technical alliance partners, which shall not be disclosed or duplicated, used or disclosed in whole or in part for any purpose other than to evaluate TELECABLE S.A. Services. Any use or disclosure in whole or in part without the express written permission of TELECABLE S.A. is prohibited.

Content

- 1. Overview4**
- 2. Technical Actions to Prevent Illegal Calls4**
 - 2.1 Considerations in SIP configurations to subscribers 4
 - 2.2 Monitoring and Control 5
- 3. Contractual Policies5**
- 4. Call tracking and details5**
- 5. Considerations6**

1. Overview

This document contains the specifications and actions that Telecable S.A., Costa Rica's telecommunications operator, has taken in its robocall mitigation plan, which includes the best practices for the reduction of robocall origination, commitment to assist with end-to-end tracking and tracing of call events in order to respond to all monitoring requests from the Commission, law enforcement and industry consortium monitoring, cooperation for investigation and arrest of any illegal robocaller who uses its service to originate fraudulent calls.

There is a regulatory responsibility by SUTEL (Costa Rica's telecommunications regulatory agency) to inform and ensure the proper use of services provided to subscribers in terms of contracts for legal compliance and fraud prevention.

For compliance and liability purposes Telecable S.A wishes to register in the FCC databases/registers, with option 3: "No STIR/SHAKEN Implementation - Performing Robocall Mitigation". At the moment, Telecable S.A. does not have a STIR/SHAKEN system in its telephony platforms; however, other techniques are used to avoid identity theft at the numbering level, allowing subscribers to use only assigned and contracted numbering ranges.

2. Technical Actions to Prevent Illegal Calls

2.1 Considerations in SIP configurations to subscribers

Telecable S.A. has 100% of its telephone infrastructure based on SIP, and therefore offers its customers trunk links and conventional telephony subscriptions exclusively with the SIP protocol. Within the provisioning practices, the following configurations are used to authenticate and provide security in order to avoid spoofing in our networks:

- **Use DN for identification** (The directory number in the SIP From header must match the DIDs assigned to the customer, if this does not happen the call is not allowed).
- **IP address match required** (an incoming request (such as INVITE or REGISTER) is correlated with this binding if and only if the IP addresses match)
- **SIP authentication required** (SIP authentication is requested for an existing SIP or pbx device. if it does not meet the authentication factor, the call does not connect).
- **Interoperability with SBC** (Through the security layer of the session border controller it is guaranteed that the calls are not intervened or that the telephone services offered by Telecable S.A are not used by unauthorized users. An effort is made to provide voice services, securely and reliably, to those outside the organization's LAN or WAN network).

2.2 Monitoring and Control

Telecable's NOC monitors international call traffic to ensure service and quality. A control algorithm is available at the international call level that in the event of an unusual peak or unusual number of calls from the same DID in a specific time frame, causes a partial blocking of calls for that caller ID, allowing the customer to be notified of the situation and validating whether or not it is a case of telephone fraud.

Telecable has a 24/7 continuous monitoring protocol and analysis of high volume incoming and outgoing network traffic to identify unusual peaks and suspicious patterns.

3. Contractual Policies

Our customers are committed by contract to use our services for only lawfully purposes, so upon suspicion of illegal use or fraud, we reserve the right to suspend or terminate any customer who we believe is violating or infringing local law, including U.S. federal, state or local laws, rules or regulations. The subscribed contract by the client expressly prohibits customers to impersonate numbers or land international calls in order to avoid long distance charges.

In the case of residential, business or consumer services, Telecable S.A. requires customers to provide their ID, full legal name, residential address (confirmed through verifiable means, such as a telephone or electricity bill), contact telephone number and e-mail address regarding to review the request according to the SUTEL and Data Privacy national regulations. In case of a possible transfer of services, the customer is contractually obliged to provide the new location and contact information that is verifiable through a legal document.

4. Call tracking and details

Telecable S.A. registers at trace level information of the calls of all its customers with a software that allows us to see detailed events at SIP packet level up to 30 days before the date on which the call was made, which allows us in a case of a trace or request to see detailed behavior and information of IP origin and destination. Calls older than 30 days are stored at CDR level.

Telecable S.A. is committed to responding to all tracing requests from regulators, law enforcement and other carriers, and we will cooperate with such entities in the investigation and apprehension of any illegal robocaller who uses our services to originate calls.

5. Considerations

The originating traffic that Telecable S.A. sends for calls to the U.S. is routed through an intermediate carrier that is already in the FCC's robocall mitigation database and has deployed the STIR-SHAKEN solution or has an automatic robocall mitigation plan in place. Telecable S.A. is already investigating a STIR-SHAKEN solution that will allow us to be at the forefront of security and compliance issues.