

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN (RMP)

Corporacion Digitel C.A. (Digitel), a foreign voice service provider, submits this filing for the Commission's Robocall Mitigation Database established pursuant to the Second Report and Order in the *Call Authentication Trust Anchor* proceeding.¹ This filing describes Digitel's policies and procedures to prevent and mitigate illegal robocalls using North American Numbering Plan (NANP) numbers that pertain to the United States. Digitel reserves the right to modify, add, delete or otherwise alter any of the policies and procedures described in this filing at any time as it deems appropriate to reflect its business, its capabilities, and its needs.

Company Background

Digitel is a Mobile Network Operator (MNO) based out of Venezuela that provides a variety of telecommunications services in Venezuela. Digitel, does not allow its subscribers to use nor does it plan to allow its subscribers, other than the allowed by its roaming services, to use North American Numbering Plan (NANP) numbers that pertain to the United States to send voice traffic to residential and business subscribers in the United States.

STIR/SHAKEN Implementation

As a foreign service provider, Digitel is not subject to 47 C.F.R. § 64.6301, *et seq.*, including the requirement in §64.6301(a) to implement the STIR/SHAKEN call authentication framework. Digitel has not implemented STIR/SHAKEN for its calls. However, due to the nature of its services and its relationships with carriers worldwide that send it traffic for completion, Digitel is not a significant source of illegal robocalls destined to the United States. Even though Digitel does not assign nor use NANP numbering to its subscribers, it has implemented a robocall mitigation plan as described below.

Robocall Mitigation Plan

This Robocall Mitigation Plan describes the specific measures that Digitel has implemented to detect and prevent illegal robocalls on its network as of June 30, 2021. The measures described below explain how Digitel mitigates and addresses the risk that it will originate or act as an intermediate carrier for illegal robocall traffic. Digitel will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described. Should it determine that changes are appropriate, its practices may differ from those described below.

Measures to Prevent or Avoid Exchanging Illegal Robocalls

- **Customer Premises.** Digitel performs identity validation on new and renewed customers, and, if it is a company, the incorporation documents.

¹ *Call Authentication Trust Anchor*, WC Docket Nos. 17-97, Second Report and Order, FCC 20-136 (rel. Oct. 1, 2020).

- **Network Monitoring.** Digitel monitors its network for fraudulent or suspicious traffic, including traffic that may be associated with illegal robocalling activity. In the event potential fraud is detected, Digitel will take action to mitigate the potential fraud, including temporary or permanent blocking of traffic and efforts to identify the source of the traffic.
- Digitel blocks traffic from invalid NANP numbers by default. Digitel also will block traffic that appears to be illegal or is flagged as suspicious under its fraud policy. Digitel will take appropriate action with its customers upon identification of suspicious patterns of calls, including unusual volumes, and has the authority to suspend or terminate service if necessary.

Responding to Traceback Requests

- Digitel commits to responding, to the extent permitted under applicable law, with valid traceback requests from the Commission, law enforcement or the Industry Traceback Group (ITG).

Cooperation with State and Federal Regulators

Digitel will cooperate, to the extent permitted under applicable law, with valid requests from the Commission, or law enforcement to identify and stop any illegal robocallers that use Digitel services to originate calls. Specifically, consistent with applicable law, Digitel will:

- Respond to valid law enforcement requests;
- Provide relevant non-proprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities; and
- Implement mandated robocall mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls.