

Chaneste S.A. Robocall Mitigation Plan

Updated February 22, 2026

Purpose and Scope

Chaneste S.A. is a voice service provider that originates voice traffic to the public switched telephone network (PSTN) and maintains a robocall mitigation program consistent with 47 CFR § 64.6305.

STIR/SHAKEN Status

As a foreign voice service provider, Chaneste S.A. does not maintain its own SPC token and therefore does not originate STIR/SHAKEN authentication using a Company-issued signing certificate. Because it is incapable of obtaining an SPC token due to Governance Authority policy, it is exempt from the voice service provider call authentication requirements in 47 CFR § 64.6301 until it is capable of obtaining an SPC token, pursuant to 47 CFR § 64.6304(b). Accordingly, the Company relies on its U.S.-based gateway and downstream providers to apply STIR/SHAKEN authentication where required and technically feasible, and it maintains and enforces a robust robocall mitigation program (including KYC, traffic monitoring, prompt investigation, and suspension/termination of suspicious traffic) as described below.

Robocall Mitigation Program

a. KNOW YOUR CUSTOMER PROCEDURES

During onboarding, Chaneste S.A. collects and verifies business identity information, including legal business name, physical address, primary contacts, and payment credentials. Chaneste S.A. validates customers through public business records, contract execution, and payment verification. Chaneste S.A. gathers expected use case and call volume information to help ensure traffic patterns align with normal business usage. Enhanced review is triggered by high-volume or short-duration traffic, marketing/dialer use cases, inconsistent caller ID behavior, or any indicators of potential fraud or misuse.

Additionally, Chaneste S.A. maintains Terms of Service and an Acceptable Use Policy that prohibit illegal robocalls, spoofing/unauthorized caller ID, misuse of numbering resources, and other unlawful or abusive calling activity. Customer agreements reserve Chaneste S.A.'s right to investigate, rate-limit, block, suspend, or terminate service for suspected or confirmed violations and to require supporting documentation when warranted.

b. TRAFFIC MONITORING, ANALYTICS, AND ENFORCEMENT

We use software provided by digitalip voice, Inc. to monitor our outbound voice traffic in real time to prevent the origination of illegal robocalls.

Combining behavioral analytics, caller authentication and verification, our solution features:

Fraud Detection: Detection of high-volume robocalling, spoofing and spam call activity.

Call Blocking Support: Accurate identification enabling you to block fraudulent phone calls as per the TRACED Act (2019)

Business Number Verification: Register legitimate business numbers to prevent unintentional call blocking.

Caller ID Name Service: Easy integration of Caller ID name lookup service, including robocall mitigation with override to include original caller ID even when call is determined fraudulent.

Any call originated on the Chaneste network is subject to inspection and investigation if the call is suspected of being fraudulent, abusive, or illegal. Calls meeting any of these criteria will be blocked. If these conditions are repeated, becoming excessive, the subscriber may be disconnected from the Chaneste network, may be subject to further investigation by the FCC for enforcement of the TRACED Act and the subscriber may be subject to fines and penalties imposed by the FCC or the jurisdictional court.

Traceback

We remain committed to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls. Additionally, Chaneste S.A. reviews and maintains its robocall mitigation program and updates it within 10 business days when filing information, services, traffic patterns, or risk controls change.