



SWISSLINK CARRIER AG
ROBOCALL MITIGATION PROGRAM

January, 2026

Contents

1. Background	3
2. Company Summary	3
3. Principals, Affiliates, Subsidiaries, and Parent Company	3
4. Call Authentication Mechanism	4
5. Know your Customer Protocol	4
5.1 KYC Form Submission	4
5.2 KYC Form Validation Process	5
5.3 Record Keeping	5
5.4 Customer KYC Updates	5
6. Mandatory Blocking Following Commission Notification	6
7. Only Accepting Traffic from Providers in the RMD	6
8. Contractual Provisions to Mitigate Illegal Robocalls	6
9. Proactive Network Monitoring, Call Filtering and Blocking	6
10. Updates to SwissLink's RMD Submission and RMP	7
11. Training and Awareness	7
12. Traceback Process and Best Practices	7

1. Background

Pursuant to the FCC’s Sixth Caller ID Authentication Report and Order and revisions to 47 C.F.R. §§ 64.6303–64.6305, all voice service providers, including foreign providers delivering traffic to the United States, must maintain a Robocall Mitigation Program (RMP) and certify their compliance in the Robocall Mitigation Database (RMD). The FCC requires all voice service providers to certify whether they have implemented STIR/SHAKEN authentication framework and to ensure that all calls they originate, carry, or process are subject to a robocall mitigation program consistent with the Commission’s rules.

Under 47 C.F.R. § 64.6305(a)(2) and § 64.6305(c)(2), a provider’s mitigation plan “shall include reasonable steps to avoid originating, carrying or processing illegal robocall traffic and shall include a commitment 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 originate calls.”

This document outlines SwissLink Carrier AG (“SwissLink”) policies, procedures, and technical safeguards to prevent the origination, carriage, or facilitation of illegal robocalls. SwissLink is committed to robust compliance practices, including strict Know Your Customer (KYC) verification, continuous network monitoring, strong contractual enforcement, and full participation in traceback efforts, in order to protect the US telecommunications ecosystem.

SwissLink responds to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG) within 24 hours and only accepts traffic from providers registered in the RMD. The company promptly investigates and blocks any traffic identified as illegal or suspicious upon notification from the FCC’s Enforcement Bureau or other trusted sources.

SwissLink affirms that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the RMD by the Commission.

2. Company Summary

SwissLink is a Swiss licensed Operator that provides international VoIP connectivity worldwide, with commercial presence in Europe, and Latin America.

SwissLink is a subsidiary of IQSTEL Inc, a NASDAQ listed global telecommunications and technology holding company.

3. Principals, Affiliates, Subsidiaries, and Parent Company

Parent Company: IQSTEL Inc (NASDAQ-listed global telecommunications and technology holding company).

Principals: Juan Carlos Lopez (CEO)

Affiliates:

- Etelix.com USA LLC – Domestic Voice Service Provider
- Whisl Telecom LLC – Domestic Voice Service Provider
- Smartbiz Telecom LLC – Domestic Voice Service Provider
- Qxtel Limited – UK based Voice Service Provider

Subsidiaries: No Subsidiaries

4. Call Authentication Mechanism

While SwissLink, as a foreign carrier, is not required to implement STIR/SHAKEN, it has adopted a robust robocall mitigation framework to ensure that all US bound calls are subject to strict customer verification, continuous traffic monitoring, and proactive mitigation measures.

Traffic received with valid STIR/SHAKEN token is passed unaltered.

5. Know your Customer Protocol

SwissLink has implemented appropriate Know Your Customer (KYC) protocols when onboarding new customers.

As part of its customer onboarding process, SwissLink implements several measures to confirm the identity and relevant business practices of a potential customer before entering into a formal agreement with them. This KYC Protocol outlines the procedures for collecting and verifying customer information to ensure compliance with regulatory standards and mitigate risks associated with new and existing customers. All prospective customers must complete the following KYC protocol:

5.1 KYC Form Submission

Customers are required to complete and submit a KYC Form containing the following information. Failure to comply with KYC requirements may result in delays or rejection of the interconnection request.

a) Business Information

- Type of Business.
- Types of voice services provided.
- Contact information: Main Telephone No, Address, emails.
- Employees contact information: telephone numbers, emails, LinkedIn profile, job position.
- FCC 499 File ID No.

- FCC Registration No (FRN).
- Federal Tax ID No (FEIN) or equivalent.

b) Business Purpose, Activities and Regulatory Compliance: This includes questions such as:

- Do you originate calls?
- Provide RMD registration number
- Do you act as a US point of entry (Gateway provider) for foreign originated traffic?
- Do you have a Subscription Account Number for accessing the National Do Not Call Registry?
- Does your business involve telemarketing to solicit the purchase of goods, services, or charitable contributions?
- Have you implemented STIR/SHAKEN in your network?
- NECAS's Operating Company Number (OCN)

c) Acknowledgment: By submitting the KYC Form and associated documents, clients acknowledge their understanding and agreement to comply with the requirements outlined in this KYC Form.

5.2 KYC Form Validation Process

Upon receipt of the required information in the KYC Form, SwissLink conducts a validation process to ensure the accuracy of the information provided by the Customer. The validation process includes:

- Reviewing the client's website, social media profiles, and LinkedIn profile.
- Verifying the validity of provided phone numbers.
- Confirming the authenticity of FCC 499 Filing and FCC registration numbers (When applicable)
- Checking for registration in the Robocall Mitigation Database (RMD)
- Customer's provided information is cross checked for consistency with the data uploaded in the RMD

If the prospect is not in compliance, SwissLink will decline to move forward.

5.3 Record Keeping

The Company maintains records of all KYC Forms, validation processes, and KYC Protocols for auditing and regulatory purposes.

5.4 Customer KYC Updates

As part of our compliance procedures, SwissLink reviews and updates KYC information for all active customers on a recurring basis.

6. Mandatory Blocking Following Commission Notification

SwissLink will promptly investigate and block illegal traffic upon receiving a notice from the Commission's Enforcement Bureau.

7. Only Accepting Traffic from Providers in the RMD

In accordance with 47 C.F.R § 64.6305(e)(1), SwissLink only accepts calls from Providers listed in the RMD.

8. Contractual Provisions to Mitigate Illegal Robocalls

SwissLink requires the execution of a Master Service Agreement (MSA) together with a Robocall Mitigation Addendum. This addendum contains explicit provisions requiring customers to:

- Comply with all applicable federal, state, and international telecommunications laws and regulations, including the Telephone Consumer Protection Act (TCPA), the TRACED Act, and FCC robocall mitigation rules.
- Prohibit the use of SwissLink services for unlawful, fraudulent, abusive, or deceptive purposes, including but not limited to illegal robocalls, caller ID spoofing, or transmission of traffic that violates federal or international law.
- Fully cooperate with SwissLink in responding to ITG and law enforcement requests within 24 hours, including disclosure of upstream provider information.

The Robocall Mitigation Addendum also grants SwissLink the right to suspend or terminate services immediately and without prior notice if a customer violates these requirements or is reasonably suspected of transmitting illegal robocalls.

9. Proactive Network Monitoring, Call Filtering and Blocking

SwissLink's Network Operations Center (NOC) team continuously monitors traffic across its network. As part of IQSTEL group, SwissLink relies on sister company network capabilities to monitor US terminating traffic, such as short duration calls, and invalid ANIs, blocking traffic from media IPs associated with suspicious or unlawful campaigns and use of Somos Do Not Originate list (DNO).

If SwissLink has reason to suspect illegal robocalling or spoofing, SwissLink identifies the offending party and takes appropriate action in a timely manner.

Calls carrying valid STIR/SHAKEN signatures are passed unaltered.

10. Updates to SwissLink’s RMD Submission and RMP

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(c)(5) & (d)(5), SwissLink will update its submission in the RMD within 10 business days of any change to the applicable information, including its RMP.

11. Training and Awareness

SwissLink provides ongoing training to its Sales and NOC teams on robocall mitigation policies and procedures. Training covers FCC requirements, identification of suspicious traffic patterns, KYC protocols, traceback obligations, and escalation procedures. By ensuring that both commercial and technical staff are properly trained, SwissLink reinforces compliance across all levels of the organization and strengthens its ability to prevent, detect, and respond to illegal robocall activity.

12. Traceback Process and Best Practices

SwissLink diligently follows established protocols to address and respond to traceback requests in full compliance with 47 C.F.R. § 64.6305(a)(2), which requires providers to respond within 24 hours to traceback requests from the FCC, law enforcement, and the industry traceback consortium (ITG).

To meet these obligations, SwissLink participates in the ITG Traceback Process and:

- **24 Hours response:** SwissLink commits to respond fully, within 24 hours, to all traceback requests from the Commission, law enforcement and ITG, and to cooperate with such entities in investigating and stopping illegal robocallers that use its service to originate, carry, or process illegal robocalls, in accordance with applicable laws.
- **Secure Portal & Escalation:** SwissLink uses the ITG’s secure traceback portal to review and confirm traffic records, ensuring consistency and cooperation.
- **Dedicated Point of Contact:** SwissLink has designated a dedicated point of contact for addressing requests from other Voice Service Providers, ITG or any other government entity related to Suspicious Traffic. This person will oversee all matters regarding robocall mitigation action:

Name:	Juan Carlos Lopez
Title:	CEO
Email:	legal@SwissLink-carrier.com

- **Ongoing Coordination:** SwissLink will exchange information regarding suspicious traffic with other VSP and USTelecom.

