

QXTEL LIMITED
ROBOCALL MITIGATION PROGRAM

August 2025

Contents

1. Background	3
2. Company Summary	3
3. Principals, affiliates, subsidiaries, and parent company	4
4. Call Authentication Mechanism	4
5. Know Your Customer Protocol.....	4
5.1 KYC Form Submission:.....	5
5.2 KYC Form Validation Process:	5
5.3 Record Keeping:.....	6
5.4 Customer KYC Updates:.....	6
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. Network Monitoring, Call Filtering and Blocking	6
10. Updates to QXTEL 's RMD Submission and RMP	7
11. Training and Awareness	7
12. Traceback Process and Best Practices	7
13. Formal Investigations	8

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 QXTEL (“QXTEL”) policies, procedures, and technical safeguards to prevent the origination, carriage, or facilitation of illegal robocalls. QXTEL 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.

QXTEL 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.

QXTEL reserves the right to modify, add, delete, or otherwise alter any of the policies and procedures described in the plan at any time as it deems appropriate to reflect its business, its capabilities, and its needs, including further strengthening its protocol for limiting robocalls.

QXTEL 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

For over 20 years, QXTEL has been a Telecommunications & Technology Services Provider focused on retail & wholesale voice platform providing, wholesale carrier voice, wholesale carrier messaging and carrier technology services related to IoT, Fintech and Business Intelligence Software solutions.

Headquartered in the United Kingdom with its principal place of business and registered address at No.1 Poultry London, United Kingdom, EC2R 8EJ, QXTEL operates in-house built advanced VoIP,

Messaging, and Fintech platforms over its POPs with IP and IPX interconnection capability under OCN 720K.

3. Principals, affiliates, subsidiaries, and parent company

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

Principals: Rami Herzallah (CFO)

Affiliates:

- Etelix.com USA LLC (Domestic Voice Service Provider)
- Whisl Telecom LLC (Domestic Voice Service Provider)
- Smartbiz Telecom LLC (Domestic Voice Service Provider)
- SwissLink Carrier AG (Swiss-licensed telecommunications operator)

Subsidiaries: No Subsidiaries

4. Call Authentication Mechanism

While QXTEL, 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. Calls lacking STIR/SHAKEN authentication are closely monitored and subject to additional scrutiny or blocking if deemed suspicious or non-compliant.

5. Know Your Customer Protocol

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

As part of its customer onboarding process, QXTEL 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 which provides QXTEL with detailed background, business, and regulatory compliance details.

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. The KYC Form must be filled out in its entirety for acceptance.

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?
- RMD 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 been determined by ITG to be a "Non-Cooperative Voice Service Provider
- Do you have a Robocall mitigation plan in place to combat illegal Robocalling, including customer vetting and telephone number validation?
- Have you implemented STIR/SHAKEN in your network?
- NECA'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, QXTEL 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.
- 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.

5.3 Record Keeping:

The Company maintains records for 5 years, of all KYC Forms, for auditing and regulatory purposes.

5.4 Customer KYC Updates:

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

6. Mandatory Blocking Following Commission Notification

QXTEL 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), QXTEL only accepts calls from providers listed in the RMD.

8. Contractual Provisions to Mitigate Illegal Robocalls

QXTEL includes explicit anti-robocall provisions in the Master Service Agreement (MSA) for all new customers. These clauses require customers to comply with applicable FCC regulations, prohibit transmission of unlawful robocall traffic, and allow QXTEL to suspend or terminate services if violations are detected.

In addition, QXTEL is actively implementing mitigation measures with its existing customer base as described in this RMP.

9. Network Monitoring, Call Filtering and Blocking

QXTEL's voice switching platform, Console (a third-party vendor solution), integrates an advanced Automated Anti-Fraud Management System that uses machine learning algorithms to continuously analyze traffic patterns across both customer and supplier routes. The system automatically identifies deviations from established traffic profiles and mitigates potentially fraudulent or problematic traffic, with the ability to flag and block suspicious Calling Party and Called Party numbers. Traffic patterns are analyzed for indicators such as abnormal call volumes, short-duration calls, invalid or unassigned Automatic Number Identifications (ANIs), and excessive call failures.

QXTEL maintains a dedicated Anti-Fraud Team that collaborates closely with the Customer Service and Traffic Management departments to investigate alerts, escalate incidents, and ensure prompt mitigation. The Automated Anti-Fraud Management System operates 24/7, providing real-time detection, notifications, and escalation workflows whenever suspicious or unlawful activity is detected.

QXTEL blocks traffic from invalid numbers by default. QXTEL also blocks traffic that appears to be potentially illegal or is flagged as suspicious under its fraud policy.

10. Updates to QXTEL's RMD Submission and RMP

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

11. Training and Awareness

QXTEL provides ongoing training to its Sales and Network Operations Center (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, QXTEL 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

QXTEL 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, QXTEL participates in the ITG Traceback Process and:

- **24 Hours response:** QXTEL 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:** QXTEL uses the ITG's secure traceback portal to review and confirm traffic records, ensuring cooperation.
- **Dedicated Point of Contact:** QXTEL 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:	Rami Herzallah
--------------	----------------

Title:	Chief Financial Officer
Email:	legal@qxtel.com

- **Ongoing Coordination:** QXTEL will exchange information regarding suspicious traffic with other VSPs and USTelecom through email, phone calls, etc.

QXTEL periodically reviews records of traceback requests to identify customers that are the subject of a pattern of traceback inquiries. QXTEL determines appropriate actions to take on a case-specific basis, which may include directing the customer to remedy the problem and, when escalated may result in the temporary suspension of the customer, or ultimately in the termination of the customer's service.

13. Formal Investigations

Pursuant to 47 C.F.R. § 64.6305(d)(1)(i), all voice service providers filing in the Robocall Mitigation Database are required to disclose whether, within the past two years, they have been the subject of any formal investigation, enforcement action, or regulatory proceeding related to the origination, carriage, or facilitation of illegal robocalls or caller ID spoofing, or for deficiencies in a previously filed robocall mitigation certification or plan.

QXTEL confirms that it has not been the subject of any such formal investigation, enforcement action, or regulatory proceeding within the past two years.