



WHISL TELECOM
ROBOCALL MITIGATION PROGRAM

March, 2026

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	7
10. Caller ID & Number Authorization	8
11. Updates to Whisl's RMD Submission and RMP	8
12. Training and Awareness	8
13. Traceback Process and Best Practices	8

1. Background

The Federal Communications Commission (“FCC” or “Commission”) requires voice service providers to file certifications and maintain a robocall mitigation program (“RMP”) in the FCC’s Robocall Mitigation Database (“RMD”) pursuant to 47 C.F.R. § 64.6305 and related Commission orders. These requirements are intended to ensure that providers take reasonable and effective steps to mitigate the origination, carriage, or processing of illegal robocalls.

Whisl operates primarily as a non-gateway intermediate provider and, in certain circumstances, as a gateway provider, and in limited instances may also act as a voice service provider. Accordingly, this RMP describes mitigation measures applicable to all of Whisl’s roles and is designed to comply with the Commission’s rules, including the Sixth Caller ID Authentication Report and Order and the Gateway Provider Report and Order.

The Commission has explained that an RMP is sufficient if it includes detailed practices that can reasonably be expected to significantly reduce illegal robocalls and if the provider complies with those practices. Consistent with this guidance, Whisl’s mitigation efforts focus on identifying and addressing potentially unlawful calls that may violate Section 227(b) of the Communications Act or the Truth in Caller ID Act, Section 227(e).

Under current FCC rules, robocall mitigation plans must address compliance with “know your customer” and “know your upstream provider” obligations, as well as the use of analytics or third-party tools to identify or block suspected illegal traffic. Consistent with these requirements, Whisl maintains documented KYC and KYUP procedures to verify the identity of its customers both at onboarding and on an ongoing basis. These measures include due diligence reviews, traffic monitoring and contractual compliance obligations. Whisl also utilizes internal analytics and, where appropriate, third-party tools to monitor traffic patterns and identify potentially unlawful robocall activity.

In its role as a gateway provider, Whisl commits to taking enhanced measures to mitigate illegal robocalls originating from abroad, including applying STIR/SHAKEN authentication to SIP calls carrying U.S. numbers, responding to traceback requests within 24 hours, implementing KYUP procedures, instituting mandatory blocking where required, and blocking calls based on reasonable Do Not Originate lists.

Whisl affirms that no prior certification has been removed by Commission action and that it is not prohibited from filing in the RMD.

2. Company Summary

Whisl is an intermediate provider that focuses its business and operations on the wholesale and business customer segments of the voice services communications market.

Whisl 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

Principals: Omar Luna (CEO)

Affiliates:

- Etelix.com USA – Domestic Voice Service Provider
- Qxtel Limited – UK based Voice Service Provider
- Smartbiz Telecom – Domestic Voice Service Provider
- SwissLink Carrier AG – Swiss Licensed Telecommunications Operator

Subsidiaries: No Subsidiaries

4. Call Authentication Mechanism

Whisl has fully Implemented STIR/SHAKEN (Secure Telephone Identity Revisited/Signature-based Handling of Asserted Information Using Tokens) protocols for all SIP calls that are eligible for authentication carrying U.S. NANP numbers.

5. Know your Customer Protocol

Whisl implements strict Know Your Customer (KYC) protocols for all customers, regardless of Whisl's role in the call chain, including when acting as a non-gateway intermediate provider, a gateway provider, or, in limited instances, a voice service provider. These protocols are designed to support compliance with applicable regulatory requirements and to mitigate the risk of illegal robocalls and other unlawful or abusive traffic.

As part of its onboarding process, Whisl conducts a review of each prospective customer prior to entering into a formal service agreement to assess risk and support ongoing compliance. This review includes the collection and verification of identity, business operations, regulatory status, and intended use of services. Whisl evaluates this information to reasonably assess, based on the information provided by the customer and information available to Whisl, whether the customer's activities appear to be legitimate and consistent with applicable federal and state telecommunications laws and regulations.

Whisl reserves the right to request additional information, documentation, or certifications at any time when Whisl determines it is necessary to satisfy regulatory, compliance, or risk-management requirements. Customer onboarding and the continuation of any business relationship with Whisl

are conditioned on the customer's timely, complete, and ongoing cooperation with these KYC and compliance requirements.

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?
- 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?
- RMD Number
- NECA's Operating Company Number (OCN)

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

5.2 KYC Form Validation Process

Whisl 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.
- 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 of all KYC Forms and validation processes for auditing and regulatory purposes.

5.4 Customer KYC Updates

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

6. Mandatory Blocking Following Commission Notification

In accordance with FCC robocall mitigation rules, Whisl will promptly investigate and block any illegal traffic upon receiving a Notice of Suspected Illegal Traffic from the FCC's Enforcement Bureau.

7. Only Accepting Traffic from Providers in the RMD

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

8. Contractual Provisions to Mitigate Illegal Robocalls

Whisl requires all customers to execute a Master Service Agreement (MSA). The MSA obligates customers to comply with all applicable federal, state, and international laws, regulations, and rules governing telecommunications services, including those related to robocalls, caller ID authentication, and consumer protection.

Whisl strictly prohibits the use of its services for any unlawful, fraudulent, abusive, or deceptive activity, including but not limited to the origination or transmission of illegal robocalls, caller ID spoofing, or traffic that violates applicable regulatory or legal requirements. These prohibitions are further detailed in Whisl's Acceptable Use Policies (AUP), as published on its [website](#).

In accordance with its MSA, AUP, and Terms and Conditions, Whisl reserves the right to suspend, restrict, or terminate services, in whole or in part, immediately and without prior notice, if Whisl determines, in its reasonable discretion, that such action is necessary due to an AUP violation, security incident, suspected or actual fraud, regulatory or legal compliance obligation (including FCC requirements), or to protect the integrity of Whisl's network, its customers, or third parties.

9. Network Monitoring, Call Filtering and Blocking

Whisl's Network Operations Center (NOC) team continuously monitors traffic across its network to identify suspicious patterns, including abnormal volumes, short duration calls, invalid or unassigned ANIs, and excessive call failures. The NOC team investigates flagged activity, escalates incidents internally, and takes immediate action when unlawful traffic is suspected, including suspension or blocking of the offending traffic.

Whisl relies on SIPNAV (replacing prior 46Labs Peeredge systems), a third-party analytics vendor, which provides advanced real time traffic analysis and detection tools. SIPNAV supports Whisl's monitoring and enforcement by:

- Identifying abnormal traffic patterns through CPS/session limits and anomaly detection.
- Analyzing metrics such as answer-seizure ratios, short-duration calls, and invalid ANIs.
- Blocking traffic from media IPs associated with suspicious or unlawful campaigns.
- Using of Somos Do Not Originate (DNO) filter.
- Using RoboGuard to block media IPs reported as being associated to scam calls, FCC or CLEC complaints.

Whisl's Network Operations Center (NOC), supported by SIPNAV platform, supervises traffic 24/7, proactively filtering and enforcing controls in alignment with FCC robocall mitigation requirements and industry best practices.

Whisl utilizes SIP Code 603+ as the standardized response for analytics-based call blocking, ensuring proper signaling, compliance with applicable FCC requirements, and transparency across the network. Legacy SIP response codes (e.g., 603, 607) are not used for analytics-based blocking determinations.

When illegal robocalling or spoofing is suspected, Whisl promptly identifies the responsible party and takes appropriate action in a timely manner.

Calls carrying valid STIR/SHAKEN signatures are passed unaltered.

Whisl affirms that, consistent with FCC rules, it will not block any emergency calls placed to 911 under any circumstances and will make all reasonable efforts to ensure that calls originating from Public Safety Answering Points (PSAPs) and other government emergency numbers are not blocked. These safeguards are integrated into Whisl's call blocking policies and monitoring systems to ensure uninterrupted access to emergency services, in full compliance with 47 C.F.R. §§ 64.1200(k)(9) and related Commission guidance.

10. Caller ID & Number Authorization

End users are permitted to display only those Caller ID numbers that have been legitimately assigned to them by Whisl or its affiliated companies. Any unauthorized manipulation or falsification of Caller ID information is strictly prohibited and will result in immediate service suspension or termination.

11. Updates to Whisl's RMD Submission and RMP

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

12. Training and Awareness

Whisl 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, Whisl reinforces compliance across all levels of the organization and strengthens its ability to prevent, detect, and respond to illegal robocall activity.

13. Traceback Process and Best Practices

Whisl 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, Whisl participates in the ITG Traceback Process and:

- **24 Hours response:** Whisl 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:** Whisl uses the ITG's secure traceback portal to review and confirm traffic records, ensuring cooperation.
- **Dedicated Point of Contact:** Whisl 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:	Manuel Vicuña
Title:	NOC
Email:	noc@whisl.com

- **Ongoing Coordination:** Whisl will exchange information regarding suspicious traffic with other VSP and US Telecom through email, phone calls, etc.