



ETELIX.COM USA
ROBOCALL MITIGATION PROGRAM

March, 2026

Contents

1. Background	3
2. Company Summary	4
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:	6
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	7
9. Network Monitoring, Call Filtering and Blocking	7
10. Caller ID & Number Authorization	8
11. Updates to Etelix's RMD Submission and RMP	8
12. Training and Awareness	8
13. Traceback Process and Best Practices	9

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.

Etelix 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 Etelix’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, Etelix’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, Etelix 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. Etelix 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, Etelix 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. These measures are consistent with the requirements in the *Sixth Caller ID Authentication Report and Order* and the [Gateway Provider Report and Order](#).

As illustrated in this plan, Etelix is committed to implementing reasonable and effective mitigation measures consistent with FCC regulations and recognized industry best practices

Finally, Etelix 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

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

Etelix provides International and Domestic Long-Distance voice termination in the ILD Wholesale market through over 200 interconnections with telecommunications carriers, PSTNs, PTTs, Mobile Operators, Mobile Virtual Network Operators (MVNOs), Long Distance Operators and Long-Distance Wholesales Carriers supplying international connectivity and international call transit worldwide.

Etelix 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:

- Qxtel Limited – UK based Voice Service Provider
- SmartBiz Telecom LLC – Domestic Voice Service Provider
- SwissLink Carrier AG – Swiss licensed telecommunications operator
- Etelix Telecom LLC – Domestic Voice Service Provider

Subsidiaries: No Subsidiaries

4. Call Authentication Mechanism

Etelix 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

Etelix implements strict Know Your Customer (KYC) protocols for all customers, regardless of Etelix'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, Etelix 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. Etelix evaluates this information to reasonably assess, based on the information provided by the customer and information available to Etelix, whether the customer's activities appear to be legitimate and consistent with applicable federal and state telecommunications laws and regulations.

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

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?
- 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, Etelix conducts a validation process to ensure the accuracy of the information provided by the Customer. The validation process includes:

- Reviewing the customer's website, social media profiles, and LinkedIn profile.
- Confirming the authenticity of FCC 499 Filing and FCC registration numbers (When applicable).
- Checking for RMD Registration.
- Customer 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 the validation processes for auditing and regulatory purposes.

5.4 Customer KYC Updates:

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

6. Mandatory Blocking Following Commission Notification

Etelix 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), Etelix only accepts calls from Providers listed in the RMD:

- **Domestic Voice Service Providers:** As per 47 C.F.R § 64.6305(e)(1), Etelix solely accepts calls from domestic Voice Service Providers if the provider's filing is listed in the RMD and has not been subject to delisting due to enforcement actions.
- **Foreign Voice Service Providers and Foreign Intermediate Providers:** Etelix only accepts calls from Foreign Voice Service Providers or Foreign Intermediate Providers utilizing North American Numbering Plan upon the provider's inclusion in the RMD and absence of delisting due to enforcement actions.

- **Gateway Providers:** Etelix will only accept calls directly from Gateway Providers if the provider's filing: (a) is listed in the RMD, (b) demonstrates affirmative submission of the filing, and (c) has not undergone delisting due to enforcement actions.

8. Contractual Provisions to Mitigate Illegal Robocalls

Etelix requires customers to execute a Master Service Agreement (MSA) together with a Robocall Mitigation Addendum. This addendum includes explicit provisions that require 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 Etelix 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 Etelix in responding to ITG and law enforcement requests within 24 hours, including disclosure of upstream provider information.
- Maintain accurate and updated KYC information, with a mandatory update upon Etelix's request.

The Robocall Mitigation Addendum also grants Etelix 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. Network Monitoring, Call Filtering and Blocking

Etelix uses a combination of internal monitoring controls and affiliate-supported analytics to detect and mitigate potentially unlawful robocall traffic.

While Etelix's switching platform does not support advanced Do Not Originate (DNO) and analytics-based filtering features, relevant traffic is routed through its affiliate network partners, which operates SIPNAV platform. Through this architecture, Etelix leverages SIPNAV's real-time monitoring and call filtering capabilities, including:

- 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.

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

Etelix 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.

Calls carrying valid STIR/SHAKEN signatures are passed unaltered.

Etelix 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 Etelix'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 Etelix 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 Etelix's RMD Submission and RMP

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(c)(5) & (d)(5), Etelix 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

Etelix 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, Etelix 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

Etelix 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, Etelix participates in the ITG Traceback Process and:

- **24 Hours response:** Etelix 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:** Etelix uses the ITG's secure traceback portal to review and confirm traffic records, ensuring cooperation.
- **Dedicated Point of Contact:** Etelix has designated a dedicated point of contact for addressing requests from other Voice Service Providers (VSP), 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@etelix.com

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