

SMARTBIZ TELECOM, LLC

ROBOCALL MITIGATION PROGRAM

2026 - Revised for VeriSwitch / SIP 603+

Table of Contents

1. Background
2. Company Summary
3. Principals, affiliates, subsidiaries, and parent company
4. Call Authentication Mechanism
5. Know your Customer Protocol
 - 5.1 KYC Form Submission
 - 5.2 KYC Form Validation Process
 - 5.3 Record Keeping
 - 5.4 Customer KYC Updates
6. Mandatory Blocking Following Commission Notification
7. Only Accepting Traffic from Providers in the RMD
8. Contractual Provisions to Mitigate Illegal Robocalls
9. Network Monitoring, Call Filtering and Blocking
10. Caller ID & Number Authorization
11. Updates to SmartBiz's RMD Submission and RMP
12. Training and Awareness
13. Traceback Process and Best Practices
14. Formal Investigations

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.

SmartBiz Telecom, LLC ("SmartBiz") 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 SmartBiz'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, SmartBiz'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, SmartBiz 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. SmartBiz 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, SmartBiz 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, SmartBiz is committed to implementing reasonable and effective mitigation measures consistent with FCC regulations and recognized industry best practices.

Finally, SmartBiz affirms that no prior certification has been removed by Commission action and that it is not prohibited from filing in the RMD, except as otherwise disclosed in Section 14 of this plan.

2. Company Summary

SmartBiz Telecom is a telecommunications company based in Miami, FL, dedicated to the VoIP business for both wholesale and retail markets. Established in 2016 by an experienced team with over 15 years in the international voice business, SmartBiz provides International and Domestic Long-Distance voice termination through numerous interconnections with telecommunications carriers, PSTNs, mobile operators, and other service providers.

SmartBiz 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: Eduardo Borrero (CFO) and José Olivar (CEO)

Affiliates:

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

Subsidiaries: No Subsidiaries

4. Call Authentication Mechanism

SmartBiz 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

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

SmartBiz reserves the right to request additional information, documentation, or certifications at any time when SmartBiz determines it is necessary to satisfy regulatory, compliance, or risk-management requirements. Customer onboarding and the continuation of any business relationship with SmartBiz 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 discontinuation of 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
- Type of traffic
- 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, SmartBiz 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, SmartBiz reviews and updates KYC customer information for all active customers and upstream providers on a recurring basis. KYC refresh is conducted every year, which includes review of regulatory filings and compliance with RMD requirements.

6. Mandatory Blocking Following Commission Notification

SmartBiz will promptly investigate and block illegal traffic upon receiving a notice from the Commission's Enforcement Bureau. Additionally, SmartBiz will adhere to the specified Process for Issuing a Notification of Suspected Illegal Traffic outlined in the Gateway Provider Report and Order to ensure effective resolution of such issues.

7. Only Accepting Traffic from Providers in the RMD

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

- Domestic Voice Service Providers: As per 47 C.F.R. § 64.6305(e)(1), SmartBiz 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: SmartBiz 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: SmartBiz 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

SmartBiz 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 SmartBiz 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 SmartBiz 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 SmartBiz's request.

The Robocall Mitigation Addendum also grants SmartBiz the right to suspend or terminate services immediately and without prior notice if a customer violates these

requirements, fails to comply with KYC requirements, or is reasonably suspected of transmitting illegal robocalls.

9. Network Monitoring, Call Filtering and Blocking

SmartBiz uses VeriSwitch as its switching solution. VeriSwitch provides network-level traffic monitoring, call-control, filtering, and blocking capabilities that support SmartBiz's robocall mitigation program.

SmartBiz uses these capabilities to support 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
- Including YouMail fraud prevention features
- Integrating Somos Do Not Originate (DNO) lists into filtering logic
- Supporting destination number blocking

SmartBiz has confirmed that its VeriSwitch implementation supports the use of SIP code 603+, as defined in ATIS-1000099, for notification of analytics-based call blocking on IP networks, in accordance with 47 C.F.R. § 64.1200(k)(9). Where SmartBiz blocks calls based on reasonable analytics, its network is configured to generate, receive, and transmit the SIP 603+ response as applicable. SmartBiz's Network Operations Center (NOC), supported by VeriSwitch monitoring and call-control capabilities, supervises traffic 24/7, proactively filtering and enforcing controls in alignment with FCC robocall mitigation requirements and industry best practices. SmartBiz has implemented detailed reporting and

alerting systems to detect and investigate suspicious traffic patterns, including anomalous call volumes and relevant SIP response codes, including SIP 603+ blocking responses. When illegal robocalling or spoofing is suspected, SmartBiz promptly identifies the responsible party and takes appropriate action in a timely manner.

Calls carrying valid STIR/SHAKEN signatures are passed unaltered.

SmartBiz 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 SmartBiz's call blocking policies and monitoring systems to ensure uninterrupted access to emergency services, consistent with applicable Commission requirements and 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 SmartBiz 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 SmartBiz's RMD Submission and RMP

SmartBiz will keep its Robocall Mitigation Database filing and this RMP accurate and current and will update its RMD submission within 10 business days of any change to information that the Commission's rules require to be updated.

SmartBiz will also complete the FCC's annual RMD recertification on or before March 1 of each year, certifying in accordance with 47 C.F.R. § 64.6305(h) and 47 C.F.R. § 1.16 that the information submitted to the Robocall Mitigation Database is true and correct. As part of each annual recertification, SmartBiz will review its filing, including the certification selections applicable to each role SmartBiz performs in the call path, and will correct or update information as necessary before recertifying.

12. Training and Awareness

SmartBiz 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, SmartBiz 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

SmartBiz 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, SmartBiz participates in the ITG Traceback Process and:

- **24 Hours response:** SmartBiz 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:** SmartBiz uses the ITG's secure traceback portal to review and confirm traffic records, ensuring cooperation.

- **Dedicated Point of Contact:** SmartBiz 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 Manager Email: noc@SmartBiztel.com

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

14. 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.

SmartBiz Case Disclosure:

SmartBiz and the Florida Attorney General's Office resolved Case No. 1:22-cv-23945 through a Consent Final Judgment on February 13, 2025. The case, which began on December 5, 2022, involved allegations regarding robocall traffic and was settled without trial.

SmartBiz remains fully compliant with FCC regulations and continues to uphold all robocall mitigation requirements. The resolution of this matter demonstrates SmartBiz's commitment to cooperating with regulatory authorities and maintaining the highest standards of compliance in its operations.