

ROBOCALL MITIGATION PROGRAM DESCRIPTION

Voice Service Provider | Owned Infrastructure | Inteliquent/Sinch SIP Trunking

Pursuant to 47 CFR § 64.6305(d)(ii)-(iii) and DA 24-73

Company Name	STL Communications DBA Inzo Technologies
Primary Business Address	100 Chesterfield Business Parkway Suite 300 Chesterfield, MO 63005
FRN / OCN	0031422264
Robocall Mitigation Contact	Patrick Shain Director of Engineering and Technology 314-205-7119 pshain@inzotechnologies.com
OCN (if applicable)	257M
Foreign VSP Affiliate?	☐ Yes ☒ No
Parent / Affiliates / Subsidiaries	None
Prior Business Names	None
Document Date	April 20, 2026

1. Purpose and Regulatory Basis

This Robocall Mitigation Program Description is submitted to the Federal Communications Commission (FCC) Robocall Mitigation Database in accordance with 47 CFR § 64.6305(d)(ii)-(iii) and consistent with the filing requirements and guidance set forth in FCC Public Notice DA 24-73 (released January 25, 2024).

[COMPANY LEGAL NAME] (hereinafter "the Company") operates as a Voice Service Provider that owns and operates its voice network infrastructure across two physical host locations. The Company obtains SIP trunking services from Inteliquent (Sinch) for interconnection to the public switched telephone network (PSTN). The Company is currently in active implementation of the STIR/SHAKEN caller ID authentication framework and is subject to a robocall mitigation program obligation covering all originating calls on its network. This document describes with particularity the specific reasonable steps the Company has taken, and continues to take, to avoid originating illegal robocall traffic, and states the Company's commitment to cooperate fully with the FCC, law enforcement, and the industry traceback consortium.

2. Company Overview and Provider Role

The Company provides voice communications services to business end users using resources from the North American Numbering Plan (NANP). All calls originated on the Company's network are subject to this Robocall Mitigation Program. The Company operates exclusively as a Voice Service Provider in the call chain and does not function as a gateway provider or non-gateway intermediate provider as defined under 47 CFR § 64.6300.

The Company owns and operates its voice network infrastructure across two physical hosting locations, providing the platform over which all originating calls are processed. SIP trunking interconnection to the PSTN is provided by Inteliquent (Sinch). Inteliquent currently applies STIR/SHAKEN Attestation C to calls traversing its trunks, indicating that calls have entered the network through Inteliquent but that end-to-end caller ID authentication has not yet been established at the originating provider level. The Company is actively working to achieve full STIR/SHAKEN implementation on its own network, as described in Section 3 below.

3. STIR/SHAKEN Implementation Status and Active Implementation Plan

The Company owns and operates the IP network infrastructure over which it originates calls and is therefore subject to a STIR/SHAKEN implementation obligation under 47 CFR § 64.6301(a). The Company has not yet achieved full STIR/SHAKEN implementation on its originating network and has not been granted a STIR/SHAKEN implementation extension under 47 CFR § 64.6304. Accordingly, the Company certifies that its calls are subject to the robocall mitigation program described in this document, consistent with the obligations applicable to voice service providers that have not fully implemented STIR/SHAKEN.

3.1 Current Authentication Status

The Company's SIP trunking provider, Inteliquent (Sinch), currently applies STIR/SHAKEN Attestation C to calls traversing the Company's trunks. Attestation C signifies that the call entered the network through Inteliquent but that the originating provider's identity and the caller's right to use the presented number have not yet been fully verified at the originating level. While Attestation C represents a partial authentication posture, the Company acknowledges that full Attestation A or B — which require originating-level signing — is the applicable compliance standard and is the objective of the Company's active implementation efforts.

3.2 Active STIR/SHAKEN Implementation Plan

The Company is actively engaged in implementing STIR/SHAKEN on its owned network infrastructure and has retained a third-party provider to assist with this implementation. The following steps are currently underway or planned:

- Engagement of a qualified STIR/SHAKEN implementation vendor/service provider to configure originating-level call signing on the Company's network.

- Coordination with Inteliquent (Sinch) to establish the technical configuration necessary for the Company to apply Attestation A or B signing to calls before they reach the trunk level.
- Procurement or configuration of a STIR/SHAKEN certificate from an authorized Certification Authority (CA) registered with the FCC's STI-PA (Secure Telephone Identity Policy Administrator).
- Internal testing and validation of signed call delivery end-to-end prior to full production rollout.
- Target completion of full STIR/SHAKEN implementation: [INSERT ESTIMATED COMPLETION DATE].

The Company will update its Robocall Mitigation Database filing promptly upon achieving full or partial STIR/SHAKEN implementation on its network, and no later than 10 business days following any material change in implementation status, in accordance with 47 CFR § 64.6305(d)(5).

4. Robocall Mitigation Program — Specific Reasonable Steps

Pursuant to 47 CFR § 64.6305(d)(ii), the Company describes below the specific reasonable steps it has taken as part of its robocall mitigation program. Because the Company has not yet achieved full STIR/SHAKEN implementation, these mitigation measures apply to all calls originating on the Company's network and are designed to significantly reduce the origination of illegal robocall traffic from the Company's owned infrastructure.

4.1 Customer Onboarding and Know-Your-Customer (KYC) Procedures

The Company takes affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal robocall traffic. These measures include:

- Verifying the identity of each new customer prior to provisioning voice services, including collection of legal business name, contact information, and, where applicable, tax identification numbers.
- Reviewing the nature and stated purpose of any high-volume or automated calling use cases before granting access to originating services.
- Requiring customers to execute terms of service that explicitly prohibit the origination of illegal robocalls, spoofed calls, and calls that violate the Telephone Consumer Protection Act (TCPA), Truth in Caller ID Act, or any applicable state law.
- Performing enhanced due diligence on customers that request large blocks of Direct Inward Dial (DID) numbers or exhibit call patterns indicative of automated dialing.

Contractual Provisions with End-Users (as required by DA 24-73, page 4): The Company's standard customer service agreements include provisions that:

- Expressly prohibit the use of the Company's services to originate illegal robocalls, calls with spoofed caller ID, or any calls in violation of the Telephone Consumer Protection Act (TCPA), the Truth in Caller ID Act, or applicable state law.

- Reserve the Company's right to immediately suspend or terminate service upon identification of violations without prior notice.
- Require customers to obtain all required consents and authorizations prior to initiating automated or high-volume calling campaigns.
- Authorize the Company to cooperate with law enforcement and the FCC in investigations involving the customer's traffic.

4.2 Know-Your-Upstream Provider Procedures

The Company's primary upstream SIP trunking provider is Inteliquent (Sinch). The Company has verified that Inteliquent maintains a valid, active filing in the FCC Robocall Mitigation Database. In addition to its relationship with Inteliquent, the Company maintains the following upstream provider procedures:

- Verifying that any upstream voice service provider or intermediate provider from which the Company accepts traffic maintains a valid, active filing in the FCC Robocall Mitigation Database prior to accepting traffic from such provider.
- Refusing to accept calls from any provider not listed in the Robocall Mitigation Database, in accordance with 47 CFR § 64.6305(g).
- Periodically reviewing the Robocall Mitigation Database status of upstream providers — including Inteliquent — and promptly blocking traffic from any provider whose filing has been removed.
- Monitoring the STIR/SHAKEN attestation levels applied by Inteliquent to the Company's originating traffic and coordinating with Inteliquent as the Company works toward achieving Attestation A or B signing at the originating level.

Contractual Provisions with Upstream Providers (as required by DA 24-73, page 4): To the extent the Company has agreements with upstream providers, such agreements include or the Company seeks to include provisions that:

- Require upstream providers to comply with all applicable FCC rules regarding robocall mitigation, STIR/SHAKEN, and caller ID authentication.
- Prohibit upstream providers from knowingly routing illegal robocall campaigns through the Company's network.
- Authorize the Company to immediately cease accepting traffic from an upstream provider found to be in violation of such requirements.

4.3 Call Analytics and Traffic Monitoring

The Company employs call analytics and network monitoring capabilities across its owned voice infrastructure to identify and respond to suspicious or illegal robocall traffic, including:

- Monitoring originating call traffic for anomalous patterns associated with illegal robocall campaigns, including unusual call volume spikes, high short-duration call rates, sequential dialing patterns, and abnormal caller ID usage.
- Leveraging the monitoring and reporting tools available within the Company's hosted voice platform to flag and investigate potential robocall activity in real time.

- Conducting periodic review of call detail records (CDRs) to identify customers exhibiting calling behavior inconsistent with legitimate business use.
- Blocking or suspending origination privileges for customers found to be generating illegal robocall traffic pending investigation and remediation.

Third-Party Call Analytics Vendors (as required by 47 CFR § 64.6305(d)(2)(ii) and DA 24-73):

☒	The Company does not currently use a third-party vendor for call analytics or traffic monitoring for robocall mitigation purposes. All monitoring is conducted using tools native to the Total Voice hosted platform.
☐	The Company uses the following third-party vendor(s) for call analytics to identify and block illegal traffic: [VENDOR NAME(S)]. [Briefly describe the role the vendor plays in the Company's robocall mitigation program.]

4.4 Caller ID Authentication and Spoofing Prevention

The Company takes the following steps to prevent the origination of calls with spoofed or falsified caller ID information:

- Restricting customers to use of caller ID numbers for which they have been authorized or have demonstrated a legitimate right-of-use.
- Implementing technical controls within the Total Voice hosted environment to prevent injection of caller ID information that is not associated with provisioned numbers or verified customer identities.
- Cooperating with downstream providers and law enforcement in investigations involving suspected caller ID spoofing originating from the Company's network.

4.5 Incident Response and Remediation

Upon identification of suspected illegal robocall activity, the Company follows an established incident response process:

- Immediate suspension or rate-limiting of the suspected originating customer's account pending investigation.
- Investigation of the incident using CDR analysis, customer records review, and coordination with the Total Voice platform provider as necessary.
- Termination of service for customers confirmed to have originated illegal robocall traffic, with documentation of the violation.
- Notification to appropriate authorities, including the FCC, law enforcement, or the industry traceback consortium, as warranted.

4.6 Employee and Agent Training

The Company ensures that personnel responsible for customer onboarding, account management, and network operations are trained to recognize indicators of illegal robocall

activity and understand their obligations under applicable FCC rules and the Company's robocall mitigation policies.

5. Traceback Cooperation Commitment

Pursuant to 47 CFR § 64.6305(d)(iii), the Company hereby commits to respond fully and within 24 hours to all traceback requests from the Federal Communications Commission, law enforcement agencies, and the industry traceback consortium (currently USTelecom's Industry Traceback Group), and to cooperate with such entities in investigating and stopping illegal robocallers that use the Company's service to originate calls.

The Company designates the following individual as its primary point of contact for robocall mitigation and traceback requests:

Name	Patrick Shain
Title / Department	Director of Engineering and Technology
Business Address	100 Chesterfield Business Parkway Suite 300 Chesterfield, MO 63005
Telephone Number	314-205-7119
Email Address	pshain@inzotechnologies.com

6. Prior Enforcement Actions Disclosure

Pursuant to 47 CFR § 64.6305(d)(2)(iv) and DA 24-73, the Company is required to disclose whether, at any time in the prior two years, the filing entity (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing related to illegal robocalls, spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

☒	No. The Company has not been the subject of any such action or investigation in the prior two years.
☐	Yes. [DESCRIBE: agency involved, date commenced, current status, findings, and whether final determinations have been issued.]

7. Program Maintenance and Annual Recertification

The Company is committed to maintaining, reviewing, and updating this Robocall Mitigation Program on an ongoing basis to ensure its continued effectiveness. The Company will recertify

its Robocall Mitigation Database filing annually on or before March 1 of each year, as required by 47 CFR § 64.6305(h), and will update its filing within 10 business days of any material change to the information contained herein, in accordance with applicable rules.

The Company will promptly amend this Program Description to reflect any new mitigation measures implemented, changes in STIR/SHAKEN status, changes in the designated robocall mitigation contact, or other material developments.

Submission Format Note: Pursuant to DA 24-73, this Robocall Mitigation Program Description must be uploaded to the FCC Robocall Mitigation Database portal in PDF format. The filing must be in English and signed by an officer in conformity with 47 CFR § 1.16. Updates to any filed information must be submitted within 10 business days of any material change.

8. Officer Certification

I, the undersigned, am an officer of Inzo Technologies and am authorized to execute this certification on the Company's behalf. I hereby certify that the statements made in this Robocall Mitigation Program Description are true, complete, and accurate to the best of my knowledge, information, and belief, and are made in good faith pursuant to 47 CFR § 64.6305 and 47 CFR § 1.16.



Signature

Patrick Shain
Printed Name

Director of Engineering and
Technology
Title

April 20, 2026
Date

This document is submitted to the FCC Robocall Mitigation Database pursuant to 47 CFR § 64.6305(d) and DA 24-73. Filed items within the RMD are subject to Commission review and enforcement action.