

382 Communications Corporation

Robocall Mitigation Program – Updated February 3, 2026

Primary Address:

382 Communications
770 Legacy Place, 2nd Floor
Dedham, MA 02026

Robocall Mitigation Program Introduction:

Consistent with the applicable rules and regulations of the Federal Communications Commission (“FCC”), 382 Communications Corporation submits this certification and the following Robocall Mitigation Program (“RMP”). 382’s Robocall Mitigation Program details the policies and practices that it has established that are intended to combat and eliminate unlawful robocalls from originating on, terminating to, or routing through 382’s voice network where it is operating as a Voice Service Provider, Gateway Provider, or Intermediate Provider. These policies and practices are divided into categories described in detail below which include, among other things, contractual safeguards, know your customer policies, cooperation with traceback requests and law enforcement, as well as technical safeguards.

Company Summary:

382 provides global VoIP solutions to commercial customers and depending on the services being provided, 382’s role in the call chain includes being a Voice Service Provider, Gateway Provider, or Non-Gateway Intermediate Provider with a STIR/SHAKEN obligation.

Filing of RMP and Implementation of STIR/SHAKEN:

In submitting this RMP with the FCC, 382 states that: (a) all the calls it originates, carries or process on its network are subject to this RMP, (b) its prior certification has not been removed by Commission action and (c) it has not been prohibited from filing in the Robocall Mitigation Database (“RMD”) by the Commission.

382 has fully implemented the STIR/SHAKEN and submitted its certification that: (a) all calls it carries or processes on its network are authenticated with STIR/SHAKEN consistent with 47 C.F.R §64.6301(a)(1) and (2) and 64.6302(b). 382’s RMP, which has been uploaded into the RMD, reflects the “reasonable steps to mitigate illegal robocall traffic” and “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 illegal robocallers that use its service to originate, carry, or process illegal robocalls.”

382 states that during the past two years, it (and/or any entity for which 382 shares common ownership, management, directors, or control) has not been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient RMD certification or mitigation program description.

Robocall Mitigation Program:

This RMP applies to 382’s calling platforms and provides information on 382’s policies and procedures on the following topics that are discussed below which “details the specific reasonable steps it has taken to avoid carrying or processing illegal robocall traffic”:

- 1) Implementing Knowing Your Customer Protocols
- 2) Requiring Contractual Provisions to Mitigate Illegal Robocalls

- 3) Requiring manual Interop prior to onboarding & Only Accepting Traffic from Providers that Have Affirmatively Filed in the RMD
- 4) Automatically Blocking Calls on a Do-Not-Originate List
- 5) Authenticating Voice Traffic
- 6) Analyzing and Monitoring Network Traffic Routing Through 382's Network
- 7) Operating Company Number
- 8) Investigating Suspicious Calling Patterns
- 9) Ensuring Foreign Providers are not using 382's Network to Carry or Process High - Volume illegal Traffic onto the U.S. Network
- 10) Responding to Commission, Law Enforcement and ITG Traceback Requests
- 11) Designating an Employee Responsible for Addressing Robocall Mitigation Related Issues
- 12) Updating 382's RMD Submission and RMD Plan
- 13) Training
- 14) Information Regarding Principals, Affiliates, Subsidiaries & Parent Companies

1. Implementing Knowing Your Customer Protocols

The FCC requires a voice service provider to take “affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic.”

382 has implemented Know Your Customer compliance team that sets the protocols when onboarding new or renewing commercial and wholesale customers. As part of its KYC protocols, 382 requires any commercial/wholesale customer to provide sufficient information to ensure its legitimacy. All potential and existing customers are required to complete a comprehensive customer profile that includes, among other things, the customer's legal information, contact person, state or country of incorporation, USF filer ID and exemption information, Robocall Mitigation Database number, FCC registration number, and the nature and description of the customer's business. If the company is a Voice Service Provider, Foreign Service Provider, Intermediate Provider and /or Gateway Provider, 382 confirms that the company's listing in the FCC's RMD and has not been delisted pursuant to an enforcement action before accepting traffic from such entities.

2. Requiring Contractual Provisions to Mitigate Illegal Robocalls

382 requires all potential and renewing commercial/wholesale customers to maintain valid and appropriate certifications, and in all Master Service Agreements, 382 specifically prohibits the transmission of all automated, mass dialing, broadcast calls, blaster calls, and calls initiated by automated dialing equipment designed to play a pre-recorded message, and any other calls not in compliance with the FCC, FTC or any regulatory authority. 382 requires that all commercial/wholesale customers certify and represent that they will not remove, alter, or otherwise manipulate ANI, CPN or other origination party information.

382's standard Master Service Agreement includes a termination clause for violations of federal, state, and local laws, rules, and regulations applicable to the use of 382's services. 382 retains

contractual rights, in all carrier agreements and without notice, liability or penalty to block any prohibited traffic and/or suspend services in 382's sole and absolute discretion. 382 further retains the right to terminate the MSA and all services provided upon written notice for any material breach. Illegal robocalls are treated as a material breach under the MSA.

3. Requiring Manual Interop Prior to Onboarding & Only Accepting Traffic from Providers that Have Affirmatively Filed in the RMD:

To help ensure the legitimacy of all potential 382 customers, 382 requires a manual interop and test with a live 382 technician prior to on-boarding. 382 does not automate this process and forces manual interaction with prospective commercial/wholesale customers prior to allowing traffic to pass on our network. In addition, 382's Know Your Customer policy and procedures involve verification of the potential customer in the RMD to see if the Providers filing appears in the RMD. 382 only accepts calls directly from a domestic Voice Service Provider if that Voice Service Provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action. 382 only accepts calls directly from a Foreign Voice Service Provider or Foreign Intermediate Provider that uses the North American Numbering Plan resources that pertain to the United States in the caller ID field to send voice traffic to residential or business subscribers in the United States, only if that foreign provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action. 382 only accepts calls from a Gateway Provider only if that Gateway Provider's filing appears in the RMD and shows that the Gateway Provider has affirmatively submitted the filing and has not been delisted pursuant to an enforcement action.

4. Automatically Blocking Calls on a Do-Not-Originate List:

382 blocks any calls purporting to originate from a number on a reasonable Do-Not-Originate ("DNO") list. This DNO includes numbers for which the subscriber to which the number is assigned has requested that calls purporting to originate from that number be blocked because the number is used for inbound calls only, North American Numbering Plan ("NANP") numbers that are not valid, Valid NANP Numbers that are not allocated to a provider by the NANP Administrator, Valid NANP numbers that are allocated to a provider by the NANP Administrator, but unused, so long as the provider blocking the calls is the allocate of the number and confirms that the number is unused or has obtained verification from the allocate that the number is unused at the time of blocking.

5. Authentication Voice Traffic:

Pursuant to 47 C.F.R §64.301(a), when operating as a Voice Service Provider, 382 does the following (1) authenticates and verifies caller identification information for all SIP calls that exclusively transit its own network; (2) authenticates caller identification information for all SIP calls it originates and that it will exchange with another Voice Service Provider or Intermediate Provider and, to the extent technically feasible, transmit that call with authenticated caller identification information to the next Voice Service Provider or Intermediate Provider in the call path; and (3) verifies caller identification information for all SIP calls it receives from another Voice Service

Provider or Intermediate Provider which it will terminate and for which the caller identification information has been authenticated.

Pursuant to 47 C.F.R. § 64.6302(b) and (c), when operating as a Gateway or Intermediate Provider, 382 authenticates caller identification information for all calls it receives that use North American Numbering Plan resources that pertain to the United States in the caller ID field and for which the caller identification information has not been authenticated and which will exchange with another provider as a SIP call.

Pursuant to 47 C.F.R. § 64.6302(d), when operating as a Non-Gateway Intermediate Provider, 382 authenticates caller identification information for all calls it receives directly from an originating provider and for which the caller identification has not been authenticated and which it will exchange with another provider as a SIP call.

6. Analyzing and Monitoring Network Traffic Through 382's Network:

Consistent with the State Attorneys General/Service Provider Anti-Robocall principals, 382 investigates suspicious calls and calling patterns. 382 has developed proprietary means and methods assisting with the identification of illegal robocall and unlawful Caller ID spoofing. 382 uses programmatic methods to help identify and block offensive traffic. Upon receiving call traffic that originates on, terminates to, or routes through 382 voice Network, 382 monitors the voice traffic and every call undergoes multiple levels of analysis, which may include calls that are unanswered or very short duration, to ensure illegal robocalling and unlawful Caller ID spoofing is mitigated. This analysis occurs not only with regard to real-time behavioral patterns but also rolling historical behavioral patterns for predetermined observation windows that may range from minutes to hours to days. This analysis yields a binary decision on whether the traffic trying to enter our network is highly likely to be illegal robocalling and/or unlawful Caller ID spoofing traffic.

7. Operating Company Numbers:

382 Networks Inc.: 815G

8. Investigating Suspicious Calling Patterns:

382 is committed to ensuring its network is not utilized for unlawful robocalls from originating on, terminating to, or routing through 382's voice network. When analyzing monitoring call traffic, if 382 discovers call patterns that are consistent with illegal robocalling, 382, after further investigation, takes appropriate action to address such behaviors. Depending upon the conduct and the information and explanation provided by the customer, corrective measures may include (a) suspension, (b) termination, (c) warnings to the customer and a thorough understanding of what the customer will do to correct the behavior, (d) reporting the customer to authorities, (e) such other actions as deemed appropriate in the discretion of 382 and consistent with law, regulations, and the governing contracts. If in the alternative, the calls are determined to be legitimate, 382 will memorialize its findings in writing as needed.

9. Ensuring Foreign Providers are not using 382's Network to Carry or Process High - Volume illegal Traffic onto the U.S. Network:

Pursuant to 47 C.F.R § 64.1200(n)(5), 382 takes reasonable and effective steps discussed under sections 1-7, above, to ensure that “any originating provider or intermediate provider, foreign or domestic, from which it directly receives traffic is not using the provider to carry or process a high volume of illegal traffic onto the U.S. network.”

10. Responding to Commission, Law Enforcement and ITG Traceback Requests:

In accordance with the FCC’s regulation 47 C.F.R. § 64.1200(n)(1), 382 will respond to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium (“ITG”) within 24 hours and will cooperate with such entities in investing and stopping any illegal robocallers that attempt to use 382s’s network and services to originate, carry or process calls.

11. Designating an Employee Responsible for Addressing Robocall Mitigation Related Issues:

To further ensure 382’s network is not utilized for the origination, termination, carrying, processing, or routing of unwanted and illegal robocalls, 382 provides the following name, title, business address, telephone number, and email address of the individual within 382 that leads 382’s team that handles robocall mitigation-related issues as well as responds to traceback inquiries from the FCC, ITG, and law enforcement agencies:

Contact Name:	Dan Koch
Contact Title:	CEO
Contact Business Address:	770 Legacy Place, 2 nd Floor, Dedham, MA 02026
Contact Telephone:	617-639-9001
Contact Email:	dan@382com.com

12. Updating 382’s RMD Submission and RMD Plan:

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(d)(5), (e)(5) and (f)(5). 382 will update its submission in the RMD within 10 Business Days of any change to the applicable information it must provide and update in the RMD.

13. Training:

382 has implemented a training program that focuses on personnel and their understanding of the Robocall Mitigation Plan. Specifically focusing on the onboarding of new customers/renewals and how to ensure that account personnel understand the prerequisites for any new customer/renewal and how it relates back to the RMP. In addition, the training focuses on instructing technical support personnel on illegal robocall concerns, trace back requests, the latest regulatory requirements and industry concerns. Finally, to ensure all personnel are aware of the policies and procedures necessary to implement the RMP, all questions are referred to the contact identified in section 11 above.

14. Information Regarding Principals, Affiliates, Subsidiaries & Parent Companies:

Pursuant paragraph 46 of the Sixth Caller ID Authentication Report and Order, 382 is required to provide information regarding our principals, affiliates, subsidiaries, and parent companies in sufficient detail to facilitate the Commission's ability to determine whether 382 has been prohibited from filing in the Robocall Mitigation Database.

382 Communications. Sate of Organization: Nevada

Subsidiary: The Iserv Company LLC. State of organization: Michigan

Subsidiary: JAS Networks Inc. State of organization: Michigan

The below reflects the corporate roles of 382 Communications and its subsidiaries:

President: Daniel Koch

Officers:

James Palisano Director

Scott Campbell Director

John Skinner Director

Richard Koch Director

Joy Voke Director