

Robocall Mitigation Program Description

Filer: Jobs2me

FRN: 0038341749

Business Address: 6700 Roswell Rd 21-g Atlanta GA 30328

Date: April 27, 2026

Provider Type: Voice Service Provider

1. Introduction and Statement of Commitment

Jobs2me (“the Company”) submits this Robocall Mitigation Program Description pursuant to 47 CFR § 64.6305(d) and the Federal Communications Commission’s (“FCC” or “Commission”) rules governing the Robocall Mitigation Database. The Company is committed to combatting illegal robocalls and to taking reasonable steps to avoid originating illegal robocall traffic on its network.

This program describes the specific measures the Company has implemented to prevent illegal robocalls, identify suspicious traffic, cooperate with traceback requests, and respond to enforcement actions by the FCC, law enforcement, and the industry traceback consortium.

2. Company Overview

Jobs2me is a recruiting software company providing companies the ability to track applicants and move applicants through the hiring pipeline for offices throughout the United States.

The Company serves end-users directly and acts as a wholesale provider. The Company’s network is all IP.

The Company has approximately 1,200 customers and originates approximately 15,000 calls per day on average.

3. STIR/SHAKEN Implementation Status

The Company has fully implemented the STIR/SHAKEN caller identification authentication framework across its entire network. All calls originated by the Company are signed with the appropriate attestation level (A, B, or C) in accordance with 47 CFR § 64.6301. The Company has obtained a Service Provider Code (SPC) token from the Secure Telephone Identity Policy Administrator (STI-PA) and uses an authorized STI-Certification Authority for its signing certificates.

4. Customer Due Diligence (“Know Your Customer”)

The Company applies “Know Your Customer” (KYC) procedures to all new and existing customers to ensure that its services are not used to originate illegal robocall traffic. These procedures include:

- **Identity verification.** Before activating service, the Company collects and verifies the customer's legal business name, business address, FRN (if applicable), tax identification number, and primary contact information.
 - **Beneficial ownership.** For business customers, the Company identifies the beneficial owners and principals of the customer entity.
 - **Use case review.** The Company reviews each customer's intended use of the service (e.g., outbound calling volume, target geographies, calling campaigns) and declines service to applicants whose intended use raises significant compliance concerns.
 - **Watchlist screening.** The Company screens prospective customers against publicly available lists of entities subject to FCC enforcement actions, FTC actions, state attorney general actions, and industry traceback findings.
 - **Periodic re-verification.** The Company periodically re-verifies customer information for existing accounts to detect changes in ownership, use case, or risk profile.
-

5. Acceptable Use Policy and Contractual Provisions

All customer agreements include an Acceptable Use Policy ("AUP") that:

- Expressly prohibits the use of the Company's services to originate, transmit, or facilitate any unlawful call, including but not limited to calls that violate the Telephone Consumer Protection Act (TCPA), the Truth in Caller ID Act, FCC robocall rules, or any state or federal consumer protection law.
 - Prohibits the spoofing of caller ID with intent to defraud, cause harm, or wrongfully obtain anything of value.
 - Requires customers to maintain documented consent for any calls made to consumers as required under applicable law.
 - Authorizes the Company to suspend or terminate service immediately upon evidence of illegal calling activity.
 - Requires customers to cooperate with the Company in any traceback or enforcement investigation.
-

6. Traffic Monitoring and Analytics

The Company monitors call traffic on its network for indicators of illegal robocall activity, including:

- Abnormally high call volumes or short-duration ("dial-and-hang-up") calling patterns
- High rates of unanswered or rejected calls
- Calls with mismatched, invalid, or unallocated calling numbers
- Calls to numbers on the National Do Not Call Registry
- Patterns consistent with neighbor spoofing or number cycling
- Consumer complaints or reports received via Jobs2me complaint channels

The Company uses internal analytics tools and third-party traffic-monitoring services such as Bandwidth to identify and investigate suspicious traffic.

When suspicious traffic is detected, the Company promptly contacts the originating customer for explanation, may impose temporary call-volume caps, and may suspend or terminate services if the customer fails to provide a satisfactory response.

7. Traceback Response Procedures

The Company commits to respond fully and within 24 hours to all traceback requests from the FCC, law enforcement, and the industry traceback consortium (the USTelecom Industry Traceback Group, or “ITG”).

Specifically, the Company:

- Designates a primary point of contact (identified in Section 11 below) responsible for receiving and responding to traceback requests.
 - Maintains call detail records (CDRs) sufficient to identify the source of any call originated, transited, or terminated on its network for at least 12 months.
 - Provides upstream call source information (originating customer, signaling details, timestamps) within 24 hours of receiving a valid traceback request.
 - If the call originated with a customer of the Company, takes appropriate action against that customer in accordance with Section 8 below.
 - Cooperates with the requestor in any follow-up inquiry or investigation.
-

8. Investigation, Enforcement, and Termination

When the Company receives evidence — through traceback, customer complaint, regulatory inquiry, or its own monitoring — that a customer is originating illegal robocall traffic, the Company:

1. Promptly investigates the allegation, including reviewing relevant CDRs, customer documentation, and consent records.
2. Contacts the customer to demand explanation and remediation.
3. Suspends service to the customer if the conduct continues or if the evidence is sufficiently clear and material.
4. Terminates service to the customer for repeat or egregious violations.
5. Documents all such actions and retains documentation for at least 1 year.
6. Reports the customer’s identity to the ITG and to relevant regulators where appropriate.

The Company will not knowingly accept traffic from any customer that has been the subject of an FCC § 64.1200(n)(2) enforcement notice or similar regulatory action without first conducting enhanced due diligence.

9. Cooperation with the FCC, Law Enforcement, and the Industry Traceback Consortium

The Company will cooperate fully with the FCC, law enforcement (including state attorneys general and the U.S. Department of Justice), and the industry traceback consortium in

investigating and stopping illegal robocallers that use the Company's service to originate calls. This cooperation includes:

- Providing call records, customer information, and other relevant evidence in response to lawful requests
 - Participating in industry-wide traceback efforts
 - Reporting suspected illegal robocall activity to appropriate authorities
 - Implementing any additional mitigation measures requested by such entities to the extent technically feasible
-

10. Internal Training and Compliance

The Company maintains internal policies and procedures that ensure operational personnel understand and comply with applicable robocall mitigation rules. Personnel involved in customer onboarding, network operations, and compliance receive both onboarding and annual training on robocall mitigation requirements, traceback procedures, and the Company's internal escalation procedures.

11. Point of Contact for Robocall Mitigation Matters

All traceback requests, regulatory inquiries, and law enforcement requests related to robocall mitigation should be directed to:

Name: Adam Robinette

Title: CEO

Department: Support

Email: Adam@jobs2me.com

Phone: 440-796-6123

Address: 6700 Roswell Rd 21-g Atlanta GA 30328

This contact is available during regular business hours and monitors the listed email address for time-sensitive traceback requests.

12. Recordkeeping and Program Review

The Company retains call detail records, customer due-diligence records, traceback correspondence, and enforcement actions for a period of at least 12 months. The Company reviews this Robocall Mitigation Program at least annually and updates it as necessary to reflect changes in the regulatory environment, the Company's network and operations, and emerging robocall threats.

13. Certification

Jobs2me certifies that the foregoing Robocall Mitigation Program is currently in effect and that the Company has taken and continues to take the steps described above to mitigate the origination of illegal robocall traffic on its network. The Company further certifies that it has not been prohibited from filing in the Robocall Mitigation Database and that any prior certification has not been removed by Commission action.

Signed,

A handwritten signature in black ink, appearing to read 'Adam Robinette', written over a horizontal line.

Adam Robinette

CEO

Jobs2me

Date: April 27, 2026