

365agents Inc.

Robocall Mitigation Certification and Plan

March 2025

Version 1.0 | FCC Robocall Mitigation Database Filing

Platform Overview

365agents Inc. operates as a voice AI platform that enables businesses to deploy AI-driven voice agents for inbound call handling, escalation routing, appointment reminders, and customer engagement. The platform originates and processes calls over IP networks and provides SIP connectivity to its customers.

PSTN interconnection and numbering resources are provided through 365agents Inc.'s upstream carrier partner, Bandwidth.com. 365agents Inc. does not directly administer NANPA numbering resources. For purposes of this Plan, “originates” refers to VoIP calls initiated through the 365agents platform, and “processes” refers to real-time audio handling and AI-generated voice responses. 365agents Inc. does not function as a traditional intermediate or transit carrier; any PSTN termination is performed through interconnection with Bandwidth.com as its upstream carrier partner.

Certification

In submitting this Robocall Mitigation Plan (RMP) with the FCC, 365agents Inc. states that: **(a)** all calls it originates, carries, or processes 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.

365agents Inc.'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.”

365agents Inc. states that during the past two years, it (and/or any entity for which 365agents Inc. 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.

Platform Architecture and Constrained Call Flow Model

365agents Inc. operates under a structurally constrained outbound calling model specifically designed to minimize illegal robocall risk. The platform is purpose-built for the following call flows:

Inbound-First Architecture

All calls are initiated by end users calling a client-provisioned phone number. The client's number is forwarded to a 365agents platform number for AI agent handling. No unsolicited outbound calls are originated to consumer numbers without prior inbound contact or explicit consumer consent.

Escalation Routing to Known Destinations Only

In the event the AI agent determines an escalation is required, the only permissible outbound action is to route the call to a pre-registered, verified destination number associated with the client account. These destination numbers are registered at onboarding. Ad-hoc outbound dialing to arbitrary numbers is technically restricted at the platform level.

Branded Outbound Calling via FirstOrion

For clients authorized to initiate outbound calls (such as appointment reminders, callbacks, or notifications), 365agents Inc. requires enrollment in the FirstOrion Branded Caller ID program. All outbound calls made under this authorization are delivered with a verified Branded Caller ID displaying the originating business identity. Unbranded outbound calling is not available to 365agents clients. This architecture eliminates the anonymous robocall risk profile common to general-purpose voice AI platforms.

Mitigation Measures

1. Customer Signup and KYC Verification

During signup, 365agents Inc. verifies customer identity using Stripe Identity (Stripe Verify), which validates government-issued identity documents, matches them against business registration data, and cross-references payment instrument ownership. One verified legal entity may be associated with one account. This ensures that only known, verified businesses can access the 365agents platform and provision phone numbers.

Accounts requesting elevated outbound call capacity are subject to additional review and monitoring prior to activation. Phone number provisioning is further restricted by requiring each client to register their inbound number(s) and all permitted escalation destination numbers before outbound call capabilities are activated.

2. Access Control via Cloudflare WAF

All 365agents platform services are protected by Cloudflare's Web Application Firewall (WAF), which is configured to:

- Block requests originating from high-risk or blacklisted IP address ranges.
- Require challenge-response authentication for requests from IP addresses with a moderate risk profile.
- Enforce rate limiting on API endpoints used for call initiation to prevent automated abuse.
- Log and alert on anomalous traffic patterns consistent with bulk or unauthorized call origination attempts.

3. Rate Limiting via Cloudflare Load Balancing

365agents Inc. employs Cloudflare Load Balancing to regulate and throttle outbound call request volume at the network layer:

- Non-enterprise accounts are restricted to a defined maximum number of concurrent outbound calls and daily outbound call limits per account tier.
- Outbound call requests exceeding defined thresholds are queued and reviewed before execution to prevent burst abuse patterns.
- Cloudflare's traffic management layer provides real-time visibility into call origination volume, enabling rapid identification of anomalous spikes that may indicate unauthorized use.
- Outbound calling activity is subject to continuous monitoring for anomalous traffic patterns. 365agents Inc. may restrict, suspend, or terminate accounts exhibiting suspicious activity.

4. Upstream Carrier Compliance via Bandwidth.com

365agents Inc. utilizes Bandwidth.com as its upstream carrier and telephony infrastructure partner. Bandwidth's carrier-grade compliance infrastructure provides:

- Active monitoring of traffic for AUP violations, with Bandwidth authorized to notify 365agents Inc. of detected anomalies or policy breaches.
- STIR/SHAKEN call authentication enforcement on all applicable outbound traffic, ensuring caller ID integrity and reducing spoofing risk.
- Routing rule enforcement consistent with FCC robocall mitigation standards, including blocking of traffic patterns associated with illegal robocall campaigns.
- 365agents Inc. maintains an active compliance relationship with Bandwidth.com and responds to any carrier-initiated AUP notification within 24 hours.

5. Branded Caller ID Enforcement via FirstOrion

All clients authorized for outbound calling must enroll in the FirstOrion Branded Caller ID program prior to making any outbound calls. This program:

- Verifies the business identity associated with each outbound caller ID number.
- Ensures all outbound calls display a verified business name to the called party, providing full transparency and eliminating anonymous robocall characteristics.
- Restricts outbound calling to registered, FirstOrion-verified numbers only. Attempts to originate calls from unregistered numbers are rejected at the platform level.

- Provides an additional compliance layer consistent with FCC goals of consumer transparency in AI-generated and automated voice calls.

6. Analytics and Monitoring

365agents Inc. employs continuous system monitoring across its platform infrastructure, including:

- Real-time alerting on anomalous call volume, unusual origination patterns, or call destinations inconsistent with registered client use cases.
- Automated flagging of accounts that exhibit patterns associated with high-frequency dialing, sequential number harvesting, or calls to non-registered destination numbers.
- Regular vulnerability assessments and security scans of platform infrastructure.
- Audit logging of all call initiation events for post-incident traceback support.

7. Incident Response

365agents Inc. participates in and acts on reports from industry partners including the USTA Industry Traceback Group (ITG). Where applicable, call authentication and related network-level controls are implemented in coordination with upstream carrier partners, including Bandwidth.com.

Reports of Acceptable Use Policy (AUP) violations, including suspected robocalls, are reviewed and responded to within 24 hours, as prescribed by our agreements with upstream carriers. Reports include those generated through automated internal or external analytics, as well as reports from individual users and customers. 365agents Inc.'s contracts with end users and upstream providers include AUP requirements subject to enforcement via automated analytics and manual review.

8. Third-Party Analytics

365agents Inc. does not use third-party analytics vendors for outbound telephony verification. As noted above, Stripe Identity is utilized for customer identity validation and KYC at account creation, and FirstOrion is utilized for branded outbound call verification — both of which are material factors in robocall mitigation.

9. Terms of Service and Acceptable Use

365agents Inc.'s services enable AI-generated voice functionality. Customers are contractually required to comply with all applicable telemarketing, consent, caller identification, and anti-spoofing laws, including those applicable to artificial or prerecorded voices under the TCPA and related regulations.

365agents Inc. may suspend or terminate accounts engaged in unlawful robocall activity and will cooperate with upstream carriers and traceback entities in investigating and mitigating suspected violations. All client agreements explicitly prohibit:

- Initiating unsolicited outbound calls to consumers who have not provided prior express consent.
- Spoofing or misrepresenting caller ID information.
- Using the platform to conduct automated dialing campaigns to numbers not pre-registered with the 365agents platform.
- Any use of AI-generated voice in violation of applicable federal or state law.

10. Training

365agents Inc. has implemented a training program focused on personnel understanding of the Robocall Mitigation Plan, with specific attention to the onboarding of new customers and renewals. Training ensures that all relevant personnel understand the prerequisites for customer activation, how those prerequisites support this Plan, and the regulatory requirements governing illegal robocalls, traceback requests, and AI-generated voice compliance.

Corporate Information and Key Personnel

Legal Entity: 365agents Inc.

Principal Address: 18291 N. Pima Rd, STE 110 #273, Scottsdale, AZ 85255

State of Incorporation: Nevada

Executive Leadership

- Catherine Weir – Executive Leadership & Compliance

Affiliated Entities

- None

Compliance Contact

For inquiries from regulatory bodies, traceback requests, or law enforcement, please contact:

Contact Name: Catherine Weir

Title: Compliance Contact

Business Address: 18291 N. Pima Rd, STE 110 #273, Scottsdale, AZ 85255

Phone: 206-206-1200

Email: cweir@365agents.com

Revision History

Version	Description	Date
1.0	Initial Documentation	March 2025

This document is submitted in connection with 365agents Inc.'s filing in the FCC Robocall Mitigation Database pursuant to the TRACED Act and applicable FCC rules. This certification is accurate and complete to the best of the company's knowledge.