

Robocall Mitigation Program (RMP)

Company Name: Bitonic Technology Labs Inc. d/b/a Yellow.ai

Filing Type: Voice Service Provider

Service Description: Enterprise Voice AI and Conversational Automation Platform

1. Overview and Purpose

This document outlines the Robocall Mitigation Program (RMP) for Yellow.ai in compliance with Federal Communications Commission (FCC) regulations, including 47 CFR § 64.6305. Yellow.ai provides enterprise-grade Conversational AI solutions. We do not provide general-purpose telecommunications services to the public. This program details our proactive measures to prevent our network and AI infrastructure from being used to originate illegal robocalls or spoofed traffic.

2. Client Vetting and Screening Processes

Yellow.ai operates exclusively in the B2B sector. We do not offer self-service, unverified voice accounts to the general public. To ensure our platform is utilized solely by legitimate enterprises, we enforce a strict Know Your Customer (KYC) onboarding process:

- **Enterprise Verification:** All prospective clients must undergo a commercial vetting process, which includes verifying their corporate identity, physical business address, and verifiable web presence.
- **Contractual Onboarding:** Voice services are only provisioned after the execution of a formal master service agreement (MSA) that includes our Acceptable Use Policy (AUP).
- **Number Authorization:** For clients utilizing their own branded or existing telephone numbers, Yellow.ai requires proof of ownership or a Letter of Authorization (LOA) before allowing those numbers to be used as the Caller ID on our platform.

3. Traffic Profile and Acceptable Use

Yellow.ai strictly prohibits the use of our platform for telemarketing, mass marketing, or cold-calling campaigns. Our outbound traffic profile is strictly limited to the following permitted use cases:

- **Transactional Service Calls:** Outbound calls initiated to a client's *existing* customers strictly for service-oriented purposes, such as appointment confirmations, delivery updates, or customer support follow-ups.
- **Inbound Escalation & Routing:** A significant portion of our outbound traffic consists of "outbound legs" triggered by an inbound call. When a consumer calls a Yellow.ai conversational AI agent and requests human assistance, our platform initiates an outbound SIP/PSTN leg to transfer the caller to the enterprise client's Contact Center as a

Service (CCaaS) platform or internal agent queue.

4. Traffic Monitoring Procedures and Prevention

To proactively prevent unwanted or illegal traffic, Yellow.ai employs continuous network and platform-level monitoring:

- **Volume and Rate Limiting:** We enforce strict Calls Per Second (CPS) and concurrent call limits tailored to each enterprise client's specific, approved use case (e.g., service notifications or agent escalations).
- **Call Detail Record (CDR) Analysis:** We monitor outbound CDRs for anomalous patterns indicative of illegal robocalling, such as sudden, unapproved spikes in outbound call volume, abnormally short call durations, or extremely low Answer Seizure Ratios (ASR).
- **Automated Prevention:** If traffic deviates significantly from a client's approved conversational baseline, our systems are designed to flag the account for immediate administrative review, and we reserve the right to throttle or suspend outbound calling capabilities pending an investigation.

5. Complaint Handling and Traceback Response

Yellow.ai is committed to full cooperation with regulatory bodies and the telecommunications industry to identify and stop bad actors:

- **Traceback Commitment:** Yellow.ai strictly commits to responding fully and comprehensively to all traceback requests from the FCC, law enforcement, and the official Industry Traceback Group (ITG) within 24 hours of receipt.
- **Internal Investigation:** Upon receiving a traceback request or a complaint regarding unwanted traffic, Yellow.ai will immediately identify the enterprise client responsible for the originating traffic.
- **Enforcement Action:** If an investigation reveals that a client has violated our AUP by initiating illegal robocalls, telemarketing, or unauthorized spoofing, Yellow.ai will take immediate corrective action, up to and including the permanent termination of the client's voice services and platform access.