

Robocall Mitigation Plan

Company: Cloud Communication Platform LLC **FCC Registration Number (FRN):** 0038134912 **Date:** March 20, 2026

1. Overview and Commitment to Compliance

Cloud Communication Platform LLC (CCP) is committed to protecting the integrity of the U.S. telecommunications network. CCP actively implements comprehensive, multi-layered strategies to prevent the origination of illegal robocalls and unauthorized messaging campaigns on its network. This Robocall Mitigation Plan outlines the strict "Know Your Customer" protocols, automated network monitoring systems, and traceback cooperation procedures enforced by CCP.

2. Know Your Customer (KYC) and Client Vetting Procedures

CCP employs a rigorous Know Your Customer (KYC) process to ensure that only verified, legitimate U.S. businesses utilize our communications infrastructure. Our onboarding process combines automated security protocols with rigorous manual review by our internal compliance team.

- **Identity and Corporate Verification:** All prospective clients are required to submit official Employer Identification Number (EIN) documentation, comprehensive contact information for their primary point of contact, and a valid corporate email address. Our compliance team conducts a manual review of every application to verify the legitimacy of the business entity and confirm the presence of an authentic, operational corporate website.
- **Geographic and Address Authentication:** CCP exclusively serves U.S.-based entities. We utilize Stripe as a third-party verification provider to authenticate physical U.S. business addresses. We do not accept P.O. boxes. To successfully register, the client's submitted physical address must identically match the billing address associated with their payment method. Furthermore, our security systems actively block any registration or payment attempts originating from Virtual Private Networks (VPNs) or international IP addresses.
- **Payment Verification and Fraud Prevention:** To mitigate the risk of fraudulent accounts, CCP actively subscribes to Stripe fraud alerts. We strictly prohibit the use of prepaid credit cards, as they present a high risk for fraudulent transactions.
- **Use-Case Evaluation and High-Risk Prohibition:** During onboarding, clients must complete a dynamic questionnaire detailing their specific use case, expected traffic volume, and messaging nature. CCP strictly prohibits high-risk industries from utilizing our platform, a policy clearly stated on our public website. If our onboarding wizard or

manual compliance review identifies a prospective client as operating within a high-risk industry, the account application is immediately rejected.

- **Strict Prohibition of Auto-Dialers:** The CCP platform architecture is designed to prevent automated, high-volume dialing. We strictly monitor and enforce a policy requiring a manual action by the user for every single contact initiated. Auto-dialers are entirely incompatible with and strictly prohibited on our network.

3. Network Monitoring and Automated Call Analytics

CCP utilizes a combination of automated network monitoring tools and dedicated human oversight to analyze outbound traffic and prevent the origination of illegal communications. Our monitoring strategy is designed to identify and block suspicious activity in real time.

- **Continuous Traffic Analysis:** CCP continuously monitors outbound traffic volumes and patterns across our network. Our systems are calibrated to detect anomalies that may indicate fraudulent activity, such as sudden, massive spikes in message volume from a single user or abnormal call duration metrics.
- **Proprietary Content Firewall:** To enforce our strict prohibition on high-risk industry traffic, CCP operates an internal, automated content firewall. This firewall analyzes all outbound messaging traffic before it is transmitted to the public network.
- **Keyword and URL Flagging:** The CCP firewall is programmed with an extensive, regularly updated database of keywords and keyword variations associated with prohibited and high-risk industries. Furthermore, the system is designed to identify and scrutinize all URLs included in outbound messages.
- **Automated Blocking and Quarantine:** Any outbound message containing a flagged keyword or an unrecognized URL is automatically and immediately blocked by the firewall. The traffic is not transmitted. Instead, it is routed to a secure quarantine queue for further investigation.
- **Mandatory Manual Compliance Review:** Quarantined traffic remains blocked until it undergoes a rigorous manual review by the CCP internal compliance team. A human analyst must evaluate the flagged content, verify the sender's identity, and confirm the campaign's legitimacy. Traffic is only released and allowed to proceed if the compliance team grants explicit, manual approval.
- **Account Suspension Protocols:** If the compliance team determines that the flagged traffic violates our acceptable use policies or indicates an attempt to originate illegal communications, CCP will take immediate action to permanently block the traffic and suspend the offending user's account.

4. Traceback Cooperation and Incident Response

CCP is fully committed to cooperating with all authorized entities to investigate and mitigate illegal robocall traffic. CCP views traceback cooperation as a critical component of its regulatory obligations.

- **Commitment to the 24-Hour Response Mandate:** CCP formally commits to responding fully and promptly to all traceback requests from the Federal Communications Commission (FCC), civil and criminal law enforcement agencies, and the registered industry traceback consortium (the Industry Traceback Group, or ITG). CCP dedicates sufficient internal resources to guarantee that a comprehensive response to any authorized traceback request is provided within twenty-four (24) hours of receipt.
- **Dedicated Traceback Personnel:** CCP maintains a designated compliance team acting as the primary point of contact for all traceback inquiries and informal requests regarding suspicious traffic. This ensures that all requests are immediately routed to personnel authorized and trained to access the necessary network data.
- **Call Detail Record (CDR) Retention:** To facilitate rapid and accurate traceback investigations, CCP retains comprehensive Call Detail Records (CDRs) for all traffic originating on, terminating on, or transiting through our network. These records include origination and destination numbers, timestamps, call durations, and IP addresses, ensuring that the necessary data is available when a traceback request is initiated.
- **Upstream/Downstream Cooperation:** As part of our commitment to the ITG and the FCC, CCP includes mandatory traceback cooperation clauses in our Terms of Service and interconnection agreements. If a traceback investigation reveals that suspicious traffic entered our network from an upstream partner or originated from a specific downstream user, CCP will promptly identify that source to the requesting authority.
- **Incident Mitigation:** If CCP is notified via a traceback request or internal monitoring that a customer is originating illegal or suspicious traffic, CCP will take immediate mitigating action. This includes suspending the offending account, blocking the associated traffic, and sharing the findings of our internal investigation with the ITG and relevant law enforcement to prevent the bad actor from migrating to another provider.