

ROBOCALL MITIGATION PLAN

AIRCALL.IO

Aircall.io, Inc. (“Aircall”) submits the following Robocall Mitigation Plan, in compliance with 47 CFR § 64.6305(f), describing: (1) the specific reasonable steps Aircall has taken to prevent new and existing customers from originating illegal robocall traffic; (2) its 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 any illegal robocallers that use its service to originate calls; and (3) Aircall’s process for updating its robocall mitigation program.

Reasonable Steps To Avoid Originating Illegal Robocalls As Part Of The Robocall Mitigation Program, Know Your Customer Practices, and Description of Analytics to Block Illegal Traffic

Aircall has implemented meaningful protections to avoid originating illegal robocalls as part of its robocall mitigation program. For example, Aircall has established and implemented comprehensive Know Your Customer (“KYC”) policies for any new and existing subscribers. The objective of the KYC policy is to prevent Aircall from being used, intentionally or unintentionally, for spoofed or illegal traffic. As part of Aircall’s KYC procedures, each new and renewing customer must go through a check of their rights and abilities to use Aircall’s services. The customer provide the following to pass this vetting process: (1) a working website (with Terms & Conditions); (2) a physical business location; (3) a corporate email address; (4) a working phone number; and (5) a valid payment method, and, optionally, (6) a LinkedIn page. In order to verify all customers’ identities, Aircall requires that its customers provide accurate and detailed information to Aircall, any other relevant service provider, and/or third party in order to port a number into an account. Customers are also required to provide further proof of identity and address to validate an Aircall number, where applicable by law.

At the outset of initiating Aircall’s services, customers must agree to Aircall’s Terms & Conditions, which are designed to combat robocalls before service is deployed. Customers agree that they are responsible for all communications transmitted via their account and Aircall reserves the right to terminate any and all services if Aircall believes, in its sole discretion, that the customer has breached any obligation of the Terms & Conditions. The Terms & Conditions expressly forbid the customer and require the customer to expressly agree that they shall not use Aircall’s services in a manner that would violate any applicable laws, rules or regulations, including those laws, rules or regulations governing telemarketing, unsolicited calls, and limitations on the use of automated or prerecorded calling technology, including the Telephone Consumer Protection Act, the Federal Trade Commission’s Telemarketing Sales Rule, and applicable state laws. Aircall also reserves the right to impose limits on any customers’ usage of its services or to terminate its services, notwithstanding a customer’s purchase of an unlimited minute plan, if Aircall believes, in its sole reasonable discretion, that such usage, including the total number of calls made and/or minutes used by a customer is not consistent with normal, fair, and reasonable use of Aircall’s services.

Once services are initiated, Aircall engages in active fraud monitoring on its own network and, as a VoIP provider that relies on underlying providers for PSTN connectivity, works with its underlying service providers to combat robocalls. Aircall considers the following types of voice calling and text messaging as fraudulent traffic: (1) All traffic deemed invalid per Commission rules; (2) traffic sent with the intent to steal or harm; and (3) traffic sent with the intent to harm through impersonating or masquerading identities. Aircall reserves the right to protect itself, its networks, and the public, by stopping fraudulent traffic from traversing its networks. Aircall's customers who send traffic that the telecommunications industry, government authorities, and Aircall consider to be fraudulent, are at risk of having their traffic blocked—either by Aircall or any downstream service provider. The following specific types of illegal activities also violate Aircall's Permissible-Use Policies: (1) unlawful robocalls; (2) domestic toll fraud; (3) international toll fraud/IRSF; (4) communication that is illegal, exploitative, abusive, harmful, unwanted, deceptive, inappropriate, or objectionable including content or communications which Aircall determines (i) is false or inaccurate; (ii) is hateful or encourages hatred or violence against individuals or groups or encourages terrorism or violent extremism; (iii) could endanger public safety, (iv) describes, features or promotes graphic violence and gore, or (v) the sale or promotion of prohibited substances or goods (5) phishing scams (IRS, SSA, vacations, student loans, etc.); and (6) text messaging SPAM. Further, through reports generated by Call Detail Records and pattern trends, fraud information sharing through industry organizations, and third-party notifications and complaints, Aircall is able to identify and combat potential unlawful robocalling.

Aircall also employs powerful analytics to identify and prevent the origination of illegal traffic, including monitoring traffic volumes and the identification of high cost destinations globally. If traffic is directed towards unusual or suspicious areas, Aircall carefully monitors it and promptly alerts and collaborates with customers. Suspicious calls that terminate in such areas are flagged. In parallel, Aircall collaborates closely with its underlying service providers to identify and escalate any suspicious activity. Both internal and external alerts are meticulously analyzed within a specified time frame by the Fraud team. When it is confirmed that calls are fraudulent, Aircall works diligently to shut down these unlawful calls as soon as possible, including the possibility of terminating the customer account associated with the activity

Commitment To Responding To Traceback Requests & Internal Efforts To Effectuate Tracebacks To Combat Robocalls

Aircall is committed to responding within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperating with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

Aircall also has in place internal traceback procedures. Carriers and service providers are encouraged to send any request for fraud investigation or tracebacks to Fraud team fraud@aircall.io. Once such a request has been received, the Aircall fraud team will open an internal case and gather information associated to the number, including the customer or company name, address, and any information about the business and telephony usage. Simultaneously, an Aircall Customer Success Manager will contact the customer to get more input about the situation. Aircall will relay all relevant information back to the carrier or service provider. In the case of proven fraud (or even spam or scam calls), Aircall will immediately block the number originating the calls or text and, depending on the findings about the customer, also block the whole customer and terminate its account. In some situations, when Aircall suspects it has identified unlawful

calling, in addition to taking the steps identified above, it also may contact the party sending Aircall the calls (i.e., Aircall's carrier/provider customer), and request that they work to investigate their customers (e.g., to identify the party sending them the calls, determine whether the calls are unlawful, and then to eliminate the source of the calling).

Plan Update Process

Aircall ensures that its plan is up to date and will apply all required changes to be compliant with Commission requirements.

This Robocall Mitigation Plan describes the specific measures that Aircall has implemented to as of March 2, 2026. Aircall continually evaluates the efficacy of its measures to combat bad actors and takes appropriate steps to improve these measures when needed.