

This Robocall Mitigation Plan is submitted by Drop Inc [Provider] to establish a “robocall mitigation plan”. This document sets forth the Provider’s current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network. The Provider views these policies and procedures as constituting “reasonable steps” to avoid the origination of illegal robocalls on its network and in addition to following these steps the Provider commits to responding to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG), and to cooperate with such entities in investigating and stopping any illegal robocallers that may use its service to originate calls.

I. STIR-SHAKEN IMPLEMENTATION STATUS

As indicated in the FCC’s Robocall Mitigation Database, the Provider’s status with respect to STIR-SHAKEN implementation is as follows:

- The Provider has implemented the STIR/SHAKEN authentication framework on any all of its network and all calls originating on its network are subject to the policies and procedures set forth in this Robocall Mitigation Plan which are intended to stop anyone from using the Provider’s service to originate illegal robocalls.

II. TRACEBACK REQUESTS

The Provider will cooperate with the FCC, law enforcement and the (ITG) on all traceback requests and investigations. To allow for timely and comprehensive law enforcement response efforts against illegal robocallers, the Provider will dedicate sufficient resources to promptly complete and provide responses to all traceback requests received from the FCC, law enforcement and/or the ITG, and commits to fully responding to any traceback request received within 24 hours after receiving the same.

III. CUSTOMER VETTING PRACTICES

As a means of preventing or minimizing the origination of illegal robocalls through its voice services, the Provider will use best practices in vetting the identity of all of its customers through ID verification provider, Vouched.ID. Provider also only allows US-based customers, who have proved US location and Identification via the Vouched.ID process.

Further, with respect to meeting existing obligations to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls, the Provider:

- Utilizes a manual real person vetting process of every recording, to make sure it’s following TSR requirements. Additionally, Provider tracks any customers that update their messaging in real-time, to then check any new voice files and scripting.

IV. TELEPHONE NUMBER VALIDATION PRACTICES

Telephone Number Validation refers to the confirmation of the customer or end-user right to use a telephone number in connection with their subscribed voice service(s). In accord with industry best practices, the Provider has procedures in place to confirm the calling customer's right to use a telephone number. Provider uses iConectiv's API for real-time phone validation.

V. INTERNATIONAL CALL ORIGINATORS

The Provider is not currently an international voice services provider.

VI. KNOW YOUR UPSTREAM PROVIDER PROCEDURES

Provider utilizes Vouched.ID's (www.vouched.id) software for customer verification via selfie and valid US-based identification, along with tracking of IP Address, Formal Address, Business Name. This information would be provided if any Traceback is received.

VII. ONGOING ROBOCALL MITIGATION PRACTICES

The Provider monitors the usage of its network and examines call detail records (CDRs) on a recurring basis for the purpose of detecting suspicious call activity and/or calling patterns. When network usage patterns consistent with illegal robocalls are detected or the Provider otherwise suspects illegal robocalling is taking place on its network, it immediately seeks to identify the party that is originating, terminating, or routing these calls so that it may take appropriate action. Provider does not allow spoofing of numbers, Customer must purchase a DID/number from one of Provider's carriers, and only then can the number be used in Provider's software. Therefore, spoofing caller IDs is not even possible in Providers software platform.