

Robocall Mitigation Plan

The Hustle software application is designed for individualized person to person conversations primarily over text with some support for person to person voice capabilities. The application does not currently support “robocalling” functionality or specifically the delivery of automated voice recordings or any one-to-many call functionality over voice networks. All call sessions are initiated by a human agent-user manually selecting a “call” button to place a call to a recipient. Numerous safeguards are in place to ensure the Hustle software application is not abused.

Below are a series of steps Hustle, Inc., the company, has taken to mitigate any instance of a robocall being placed by the Hustle software application:

- The Hustle application does not offer the capability to distribute recorded audio via voice networks.
- The Hustle application limits voice capabilities to one concurrent call per agent user of the customer. There is no capability for one-to-many voice functionality.
- The Hustle application does not provide customers options to programmatically originate call sessions or place calls.
- Any modification of the application by customers, such as the introduction of automated voice recording or one-to-many call capability to place “robocalls”, is expressly forbidden in both contract language and in terms of service
- There are numerous layers of user authentication in place to ensure a malicious actor does not have the requisite permissions to cause harm to message and call recipients
- Each agent user is invited to the platform by an authenticated admin user of the customer. Agent and admin users are both authenticated via a verified unique email and an associated verified phone number.
- There is no option for customers to create their own Hustle Instance within the Hustle software application. All customers are vetted through a rigorous sales and onboarding process, receive an onboarding from a customer success manager, and are ultimately provisioned a Hustle Instance within the Hustle software application by an employee of Hustle. With numerous interventions by Hustle employees, the company is able to vet every customer joining the platform to ensure malicious actors do not gain platform access.
- Regular penetration testing by experienced third parties to ensure the numerous layers of defense introduced for Hustle’s software application remain in-tact and any vulnerabilities exposed for quick redress
- The Hustle application is rate limited in the number of phone calls that can originate from the platform at any given time. These rate limits are in place to accommodate the low levels of person to person i.e. manually-placed voice traffic that originates from the Hustle platform. Volumes exceeding these rate limits will fail and the recipient will not receive the call. Monitoring is in place via tooling like Datadog to identify when various rate limits are approached or exceeded.

- Hustle's communications are registered with relevant bodies and protocols, e.g. STIR/SHAKEN, TCR, Short Code Registry, and send all voice traffic through CPaaS provider Bandwidth, granting deep visibility into the communications generated via the Hustle software application. With this visibility all relevant ecosystem participants assist in the monitoring of communications generated via the Hustle software application.