

Robocall Mitigation Plan

Know Your Customer

We follow the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group.

Customers are limited to low call volumes at initial sign up. Customers who wish to receive higher call volumes are run through more stringent vetting procedures. This includes collecting detailed organizational information, tax ID, and use case.

Traceback

We respond to all traceback requests from the Commission, law enforcement, and the registered traceback consortium and cooperate with such entities in investigating and stopping any illegal robocallers that use our service to originate calls.

STIR/SHAKEN Extensions

We comply with all conditions set forth in the FCC's orders, rules, and policies regarding the implementation of the STIR/SHAKEN framework for providers, including the First Call Authentication Report and Order and Second Call Authentication Report and Order.

Robocall Mitigation Program

We do not allow unknown 3rd party calls to transit our network. All calls originating from our network can be traced back to a known customer. We have implemented monitoring to watch various metrics that will trigger alerting us to possible robocalls originating from our network. We then reach out to the customer to inquire about the alert, or may decide to pause services until we can speak with the customer.

Third Party Vendors

We do not utilize third party vendors for analytics or mitigation purposes.