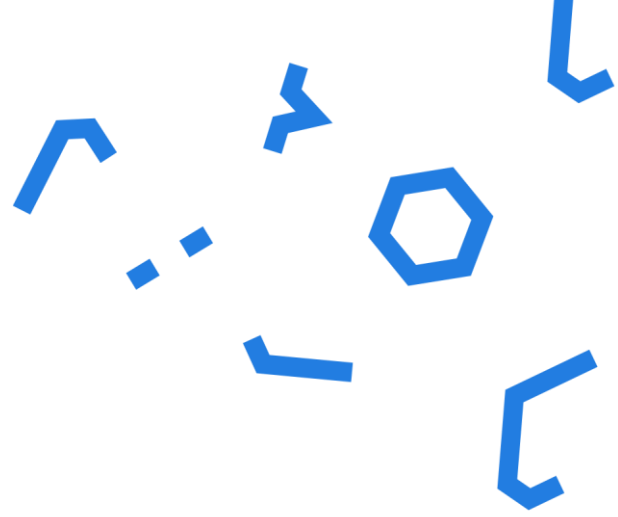




BrightCloud Group Robocall Mitigation Plan

Traceback

We promptly respond to call traceback requests from; the Commission, law enforcement and the traceback consortium and to cooperate with such entities in investigating and stopping any illegal robocallers initiating calls

STIR / SHAKEN

All the voice traffic that originates on our network is subject to our caller-id whitelisting process. Should a customer intend on using a caller-id not purchased from BrightCloud Group, the number must be verified before use. Calls with an unverified number will be dropped.

The Cisco Webex Calling Platform also utilises STIR / SHAKEN, this is where our customer's telephony will be provisioned from.

Mitigation

Our onboarding processes ensure a client agreement, including an acceptable use policy is in place, prior to any services being connected and made live. This identifies the signing parties and identification of the consumers of those services.

BrightCloud Group will block services to a customer if it determines that the customer is using the services for illegal robocalling.

BrightCloud Group monitors its voice traffic in real-time 24 hours a day/7 days week using dedicated tooling monitored

by the Fraud Operations and Network Operations Centre teams. This monitoring is used to identify,

investigate, and address any abnormal traffic patterns or other unusual behaviour on customer accounts. The Fraud Operations team will immediately terminate a customer if the team confirms that a customer has used BrightCloud Group's services to violate laws or to facilitate fraud.