

Cloud Connect LLC

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. (<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>)

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

We are fully Stir/Shaken compliant and are signing all calls with our Cloud Connect tokens. All the voice traffic that originates on our network is subject to the robocall mitigation program described below.

Robocall Mitigation Program

We use software to monitor our outbound voice traffic in real time to prevent the origination of illegal robocalls.

By combining behavioral analytics, caller authentication and verification, our solution features:

Fraud Detection: Detection of high volume robocalling, spoofing and spam call activity.

Subscriber Notification: Caller ID Name override to warn subscribers of suspicious calls.

Call Blocking Support: Accurate identification enabling you to block fraudulent phone calls as per the TRACED Act (2019)

Business Number Verification: Register legitimate business numbers to prevent unintentional call blocking.

Caller ID Name Service: Easy integration of Caller ID name lookup service, including robocall mitigation with override to include original caller ID even when call is determined fraudulent.

Acceptable Use Policy

-As part of its customer-onboarding process, all of Cloud Connect's customers will contractually agree to various terms and conditions, including a commitment to comply with Cloud Connect's Acceptable Use Policy ("AUP"). Among other things, this AUP prohibits:

Using the Services to engage in any activities that are illegal, abusive, false, fraudulent, deceptive or misleading, or any activity that exploits, banns, or threatens to harm children.

Engaging in any unsolicited advertising, marketing, or other unlawful activities using the Services, including, without limitation, any activities that violate laws applicable to advertising, electronic communications, and telemarketing, including, but not limited to, Section 5 of the FTC Act (15 U.S.C. § 45), the CAN-SPAM Act (15 U.S.C. §§ 7701-7713), the Telemarketing Consumer Fraud and Abuse Prevention Act (15 U.S.C. §§ 6101-6108), the Federal Trade Commission Telemarketing Sales Rule (16 C.F.R. § 310 et seq.), the Telephone Consumer Protection Act (47 U.S.C. §§ 227), the Federal Communications Commission regulations (47 C.F.R. 64.1200 et seq.) and orders implementing the Telephone Consumer Protection Act, and all federal and state Do Not Call and calling-time restriction laws and regulations.

Using Cloud Connect's services in any way that fails to conform to any applicable industry guidelines and standards, including, without limitation, the CTIA Messaging Principles and Best Practices, Short Code Registry Best Practices, and Short Code Monitoring Handbook.

Creating a false identity, forged email address or header, phone number, or otherwise attempting to mislead others as to the identity of the sender or the origin of a message or phone call, including failing to comply with the Truth in Caller ID Act.

Cloud Connect's contracts with its customers stipulate that Cloud Connect is authorized to suspend and/or terminate all Services in the event of an AUP violation.