

COMM-CORE

Robocall Mitigation Plan

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

All outbound calls are being signed by Bandwidth.com to fully comply with STIR/SHAKEN.

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>) At the time of this filing, users do not have the ability to create new accounts on their own and require business information to be provided to process onboarding applications.

Know-your-upstream provider

Our Tier 1 providers Bandwidth.com and Commio both provide fraudulent traffic mitigation that block and alert our NOC team.

Call Analytics Processing

COMM-CORE partners with multiple 3rd party systems to identify, alert, and mitigate bad traffic.

1. Our B2B headends that manage traffic to our carriers contain rate limiters on outbound calling. This watches for spikes outside normal traffic, and can temporarily terminate the endpoint and alert our NOC team.
2. VoIPMonitor is our call analytics platform. This system monitors for increases in outbound call activity, calls to foreign countries, high priced LATAs, and quality of the calls.
3. By default, we do not allow international traffic on our platform. Should there be a valid business use case, we will then consider, and subsequently allow access for that end customer.

Caller Authentication and Identification

We use software internally along with software provided by Bandwidth.com to monitor our outbound voice traffic in real time to prevent the origination of illegal robocalls.

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.

- **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.

In addition, we have implemented a Call Abuse Policy and have published the following policy to our web site, terms of use, and have notified our customers of the policy as copied below:

“Any call originated on the Comm-Core network is subject to inspection and investigation if the call is suspected of being fraudulent, abusive, or illegal. Calls meeting any of these criteria will be blocked. If these conditions are repeated, becoming excessive, the subscriber may be disconnected from the Comm-Core network, may be subject to further investigation by the FCC for enforcement of the TRACED Act and the subscriber may be subject to fines and penalties imposed by the FCC or the jurisdictional court.”

Robocall Mitigation Update

COMM-CORE recognizes that continuous improvement is necessary to mitigate robocalls. Should major changes be made to our platform, an update will be filed to the database within 10 working days of the change.