

Crown Networking Consultants, Inc.

Robocall Mitigation Plan

Our headquarters is located at 521 W. Broad Ave., Albany, GA 31701.

We have not been prohibited from filing a certification in the Robocall Mitigation Database.

Crown Networking Consultants, Inc, nor any of our executives or principals have a history of enforcement actions for illegal robocalls, TCPA or TSR violations or related state law violations.

We use the affirmative and effective measures detailed below to prevent the origination or transit of illegal robocalls.

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 within 24 hours 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

Our network does not have the capability to implement STIR/SHAKEN and we rely on our carrier partners; BCM One, Inc. companies: Skyswitch (RMD0002940), SIP.US (RMD0002365), SIPTrunk (nexVortex)(RMD0003284); and Enguity Technology Group (RMD0008025) to sign our calls. Our carrier partners provide TNs to our customers and are fully compliant with STIR/SHAKEN, therefore they certify our customer originations. We have obtained our IPES OCN 261M from NEAC. Enguity will use our OCN through Martini Security (STI-CA) to sign our calls directed to their network.

All the voice traffic that originates on our network is subject to the robocall mitigation program described below.

Robocall Mitigation Program

We use software provided by Skyswitch, SIP.US, SIPTrunk and Enguity 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.
- ☐ **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.
- ☐ **Do Not Call Registry:** We comply with the FTC's rules for the Do Not Call Registry as it pertains to voice and text messaging.
- ☐ **Do Not Originate:** Our carrier partners screen originating calls against a reasonable national Do Not Originate List per the FCC's rules on DNO.

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 Crown Networking Consultants, Inc 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 Crown Networking Consultants, Inc. 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.”