

Kit Carson Electric Cooperative, LLC
Robocall Mitigation Certification and Plan

Kit Carson Electric Cooperative, LLC (Kit Carson or Company) submits this robocall mitigation certification and attached Robocall Mitigation Plan pursuant to section 64.6305 of the Federal Communications Commission's (Commission's or FCC's) rules.

STIR/SHAKEN

Kit Carson is a voice service provider with a STIR/SHAKEN obligation serving end-users.

Kit Carson has "complete" STIR/SHAKEN implementation via its underlying voice service providers Twilio Inc. (Twilio) and Bandwidth Inc. (Bandwidth), who have fully implemented the STIR/SHAKEN authentication framework on their networks.

Enforcement

All voice traffic that originates on our network is subject to the attached Robocall Mitigation Plan.

Kit Carson and/or any entity for which the filing entity shares common ownership, management, directors, or control have never been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program.

Kit Carson has not been prohibited by the Commission from filing in the Robocall Mitigation Database.

Traceback

Kit Carson commits to cooperate with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any robocallers that use our service to originate unlawful robocalls. Kit Carson will respond fully within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and cooperate with such entities in investigating and stopping any robocallers that use its service to carry, process, or originate robocalls.

Identifying and Other Information

Kit Carson, LLC of 118 Cruz Alta Road, Taos, NM 87571

Other business names used by the provider: Kit Carson Internet

All business names previously used by the provider: Kit Carson Telecom, KCI, KCT

Kit Carson is not a foreign voice service provider.

Operating Company Number ("OCN"): None

Parent Company: Kit Carson Electric Cooperative Inc.

Principals, Affiliates, Subsidiaries: None

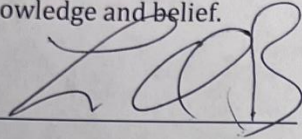
Person within company responsible for addressing robocall mitigation-related issues:

Laura Valerio, IT Manager

IT Department

(Phone): 575-758-4838; (E-mail): lvalerio@kitcarson.com

I, Officer Luis Reyes, CEO for Kit Carson Electric Cooperative Inc., submits this certification on behalf of the Company, which has implemented the STIR/SHAKEN authentication framework as indicated in the Robocall Mitigation Database. Pursuant to section 1.16 of the FCC's rules, I certify, under penalty of perjury that the information and statements contained herein are true and correct to the best of my knowledge and belief.



sign/date

4/30/24

Robocall Mitigation Program

Kit Carson, LLC has implemented specific reasonable steps to mitigate the risk of carrying or processing illegal robocalls on behalf of its customers. Kit Carson reserves the right to modify and/or supplement its robocall mitigation plan to adapt to risks and to improve the overall effectiveness of its program.

Traffic Analysis and Monitoring. Kit Carson relies on the traffic analysis and monitoring processes of its wholesale voice providers.

Bandwidth utilizes internal systems to monitor and analyze call patterns for signs of robocall activity, including voice recognition, real-time “robo-scoring”, and opt-in or opt-out tools that are designed to avoid the delivery and receipt of illegal robocalls. Bandwidth has a team of operational experts who have implemented technical and operational processes and procedures to monitor, detect and analyze the use of its services and traffic on its network. Bandwidth has developed and deployed a “Call Blocking Tool” that incorporates industry best practices into its core network to identify and block invalid, unallocated and otherwise obviously illegal telephone numbers.

Twilio uses automated detection methods, manual reviews and a combination of manual and automated enforcements to stop and prevent unwanted and fraudulent calls. Twilio monitors its network for spikes in calls to high-risk routes and uses machine learning models to detect voice fraud. Twilio developed a machine learning powered system called Tollmaster that automatically detects and alerts its Operations team of possibly fraudulent voice calls. It also triggers automated enforcement actions such as account suspension or call blocking. The system provides interfaces for the Operations team to manually review and investigate alerts and mitigate traffic via customer outreach and manual enforcement. Twilio leverages YouMail's “Watch” service, which actively monitors US phone numbers for illegal robocall activity and provides downloadable details that include evidence of illegal robocalls made with that number.

Additionally, all Kit Carson customers must also agree to abide by our Acceptable Use Policy (AUP). Our AUP prohibits the use of our services for unlawful purposes and illegal activity including activities that violate federal or state regulations and laws or the legal rights of others. If a customer is found to have violated our AUP, the Company will take action commensurate with the severity of the customer’s offense, including, but not limited to, providing the customer with a warning, suspending or terminating the customer’s service, and/or reporting the misconduct to the appropriate authorities.

Know-Your-Customer (KYC). Our end user customers also subscribe to our electric utility services. Our customers are members of the local community in which we operate. Therefore, we know our customers and do not consider our network at high risk of originating illegal robocalls. As part of our standard operating procedures, we conduct due diligence on new and renewing voice customers by collecting personal identifiable information. For business customers, we collect information concerning the company’s name, address, physical location, contact information, and Federal Tax ID, where appropriate. With respect to residential customers, we verify customers’ name and address, physical service location, and contact information.

Additionally, both Bandwidth and Twilio have adopted Know-Your-Customer processes.

In its Robocall Mitigation Database filing, Bandwidth states that it has a stringent on-boarding screening process designed to proactively identify and prevent those that may engage in illegal robocalling. Bandwidth states that its operations personnel stay closely aligned with its customers.

Twilio states that it extensively investigates customers seeking access to high-volume origination services. Twilio built a KYC platform, Trust Hub, to ingest a variety of information about such customers, including the customer's legal business name, physical address, business type, business industry, business registration number, business regions of operation, website URL, social media profiles, and authorized representatives. Twilio verifies the information provided against public records and private databases and assesses KYC for fraud detection using common signals (e.g., email, phone number, IP addresses). Where customers may not want to provide such robust information, Twilio heavily restricts the number of active concurrent calls that a customer can make. Twilio's customers must adhere to the terms of Twilio's AUP to operate on its platform. Twilio reserves the right to suspend or terminate service for any customer that is using Twilio's platform to generate illegal robocalls.

Know-Your-Upstream Provider. Kit Carson relies on the Know-Your-Upstream Provider processes of its wholesale providers.

Bandwidth requires that all of its upstream service providers customers maintain valid registrations in the FCC's Robocall Mitigation Database, Bandwidth requires service-specific contractual requirements in which customers agree to cooperate with the ITG and agree to follow all applicable laws against illegal robocalling, fraud and abuse.

Twilio states that it has processes in place intended to ensure that its immediate upstream providers are not using Twilio's network to carry or process illegal traffic. In cases where Twilio serves as the intermediate provider, the originating provider has implemented STIR/SHAKEN and received its own signing token. Twilio collects information from such providers, the same as it does for any of its customers, including their physical business location, contact person, state of incorporation, tax identification number, and business model. These providers are also Twilio's customers and are contractually bound by Twilio's AUP, which prohibits the use of Twilio's services to transmit illegal communications and requires cooperation with illegal robocall tracebacks and registration in the Robocall Mitigation Database.

Traceback. Kit Carson will respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and cooperate with such entities in investigating and stopping any robocallers that use our network to originate robocalls.