

Central Texas Telephone Cooperative, Inc.

Robocall Mitigation Plan

This Robocall Mitigation Plan (Plan) is for Central Texas Telephone Cooperative, Inc. d/b/a Central Texas TeleCommunications (CTTC), with headquarters at 1012 Reilly Street, PO Box 627, Goldthwaite, Texas 76844.

CTTC is a rural local exchange carrier that provides voice and broadband service in rural Texas. The service provided by CTTC to its residential and business customers is an analog POTS service capable of originating only one call at a time, whether a local or long distance call, per each POTS service to which a customer subscribes.

CTTC performs the following role in the call chain: a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.

CTTC does not have a history of enforcement actions for illegal robocalls, TCPA or TSR violations, or related state law violations.

CTTC uses the following affirmative, effective measures to prevent the origination or transit of illegal robocalls.

Know Your Customer

CTTC follows, to the best of its ability, the caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers as described by the NANC Call Authentication Trust Anchor Working Group.

CTTC's "Know Your Customer" process includes the collection and review of identifying information to confirm that we have an authenticated relationship with the customer. CTTC investigates new and renewing customers seeking access to high-volume origination services to mitigate the potential of any new or renewing customer originating illegal robocalls.

CTTC's General Tariff addresses unlawful or fraudulent use of services. Specifically, the General Tariff states that CTTC may refuse the installation or continuance of service if the customer plans to or uses the service in an unlawful way. It also states that a customer must obtain a permit from the Public Utilities Commission of Texas if the customer plans to use CTTC services in conjunction with any type of device that is capable of making calls for collection or solicitation. If we find a customer initiating suspicious robocalls, we warn them to stop. If such traffic continues, then we terminate their service.

Know Your Upstream Provider

We have a vetting and review process for upstream providers, that is, providers that send us voice traffic that we terminate or transit to other providers. We confirm that the upstream provider has a certification in the Robocall Mitigation Database. We will not accept voice traffic from an unregistered provider. We require that upstream providers have a reasonable robocall mitigation plan, including a

vetting process for their customers and upstream providers, and use call analytics to identify suspicious traffic.

We establish an understanding of the upstream provider's role in the call path for the traffic they will send to us, for example, whether they are acting as an originating voice service provider, a foreign intermediate provider, or a U.S.-based intermediate provider. We use this information to understand whether we will be obligated to authenticate unsigned traffic that we receive from them. The only inbound voice traffic that CTTC receives over SIP trunks comes from Sinch, which is fully STIR/SHAKEN compliant. While CTTC expects that all incoming traffic from Sinch will be signed traffic, any unsigned traffic that CTTC might receive from Sinch can be identified and investigated with Sinch related to any robocall complaints.

Our contractual provisions with upstream providers prohibit them from sending us any traffic that is illegal. If we find that an upstream provider is sending us suspicious robocalls, we warn them to stop. If such traffic continues, then we terminate their service.

Traceback

CTTC will respond within 24 hours to all traceback requests, and will cooperate with the Federal Communications Commission, law enforcement, and the industry traceback consortium. We will cooperate fully with such entities in investigation and stopping any illegal robocallers that use our service to originate, carry, or process illegal robocalls. CTTC's use of the Cordell VQM software provides a quick and viable way for CTTC to respond to any traceback request that may be received.

Robocall Mitigation Program

CTTC validates, when possible, that a customer has a legitimate right to use its asserted calling numbers using a cloud-based identity hub database. We also use this information to support the attestation level we assign to calls that we originate for that customer. Further, CTTC has in place policies designed to detect and prevent fraudulent traffic on its network.

CTTC currently uses Cordell's Voice Quality Measurement (VQM) software in conjunction with call history servers to monitor all outbound voice traffic in real-time to prevent the origination and transit of illegal robocalls. This software monitors and screens for excessive calls that are originated from CTTC's network. The software provides call record information that helps identify suspicious calling patterns, which can be reviewed to determine if illegal robocalls are occurring. The Cordell software also sets a threshold which will place a customer's telephone number in an excessive calls report if the call volume reaches the set threshold within a twenty-four-hour period. These thresholds can be adjusted to determine suspicious activity on the network. The excessive calls report is reviewed daily to determine if any numbers listed on the report have dialing patterns consistent with robocalling. This review is done in conjunction with the VQM software which provides the call records for the previous day. We perform the same mitigation steps for all outbound calls.

CTTC subscribers will also benefit from CTTC's use of Ribbon Call Trust and Fraudulent Call Services, which provides CTTC with the ability to block originating or terminating calls that either appear to be illegal robocalls or are determined to be illegal robocalls via the identity hub.

We immediately investigate any identified suspicious calls to determine if the caller or upstream provider was attempting to originate or transit unlawful robocalls. If we determine that the traffic was likely unlawful, then we warn them to stop sending such traffic. If they continue to send traffic that appears to be unlawful, then we terminate their service.

STIR/SHAKEN

CTTC is exempt from STIR/SHAKEN implementation requirements for some calls, pursuant to 47 C.F.R. §64.6304(f), because these calls rely on non-IP technology, but CTTC complies with the requirements of 47 C.F.R. §64.6303(a)(2). CTTC has registered with the Secure Telephone Identity-Policy Administrator using OCN 2052. CTTC uses the STIR/SHAKEN certificate issued by the Ribbon Certification Authority (STI-CA) for calls that we initiate. We have implemented a STIR/SHAKEN solution supplied by Ribbon.