

Central Texas Communications, Inc.

Robocall Mitigation Plan

This Robocall Mitigation Plan (Plan) is for Central Texas Communications, Inc. (CTC), with headquarters at 1012 Reilly Street, PO Box 627, Goldthwaite, Texas 76844.

CTC is a long distance carrier that resells the long distance services of Sinch America, Inc. (Sinch) to customers of CTC's parent company, Central Texas Telephone Cooperative, Inc. (CTTC), 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. For any CTTC subscriber that has chosen CTC as its long distance provider, the long distance calls of such subscribers are routed from the CTTC switch over SIP trunks to CTC and then over SIP trunks to Sinch. CTC only provides outgoing long distance service to CTTC subscribers.

CTC performs the following roles in the call chain: a voice service provider with a STIR/SHAKEN implementation obligation serving end-users and a non-gateway intermediate provider with a STIR/SHAKEN obligation. CTC has recently made modifications to its network, such that it is now fully an IP network and fully STIR/SHAKEN compliant.

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

CTC uses the following affirmative, effective measures to prevent the origination or transit of illegal robocalls. As a reseller of Sinch's long distance services, CTC also relies on the procedures, policies, and safeguards implemented by Sinch to ensure that CTC's customers are sufficiently protected against robocall activities.

Know Your Customer

CTC 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.

CTC's "Know Your Customer" process includes the collection and review of identifying information to confirm that we have an authenticated relationship with the customer. Because CTC's customers are all customers of CTC's parent, Central Texas Telephone Cooperative, CTC relies on CTTC's investigation of new and renewing customers seeking access to high-volume origination services to mitigate the potential of any new or renewing customer originating illegal robocalls.

CTC's contractual provisions with customers prohibit them from initiating illegal robocalls. Specifically, CTC has in place enforceable terms of use and/or an acceptable use policy that prohibit the use of the service for illegal or fraudulent purposes. 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 transit to other providers. CTC only receives voice traffic from one upstream provider, specifically its parent company CTTC.

We confirm that the one upstream provider from which we receive voice traffic has a certification in the Robocall Mitigation Database. We will not accept voice traffic from an unregistered provider.

We require that our only upstream provider has 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. Because CTC only receives voice traffic from one upstream provider, its parent CTTC, and because CTTC sends such voice traffic to CTC over SIP trunks with Stir Shaken certificate, CTC does not ever receive unsigned SIP traffic from an upstream provider. CTC's business arrangements with CTTC prevent CTTC from sending us any traffic that is illegal.

If we were to find that an upstream provider is sending us suspicious robocalls, we would warn them to stop. If such traffic were to continue, then we would terminate their service.

Traceback

CTC will respond within 24 hours to all traceback requests from the Commission, law enforcement, and the registered 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. CTC's use of the Cordell VQM software provides a quick and viable way for CTC to respond to any traceback request that may be received.

Robocall Mitigation Program

CTC relies on its parent CTTC to validate, when possible, that a customer has a legitimate right to use its asserted calling numbers using a cloud-based identity hub database. We use this information to support the attestation level we assign to calls that we transit from CTTC subscribers to Sinch. CTC also has in place policies designed to detect and prevent fraudulent traffic on its network. CTC, through its parent 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.

CTC uses call analytics software provided by Cordell to CTC's parent company. Specifically CTC uses Cordell's Voice Quality Measurement (VQM) software, in conjunction with CTC's call history servers to monitor all outbound voice traffic in real-time to prevent the origination or transit of illegal robocalls.

The Cordell software monitors and screens for excessive calls that are originated from CTC'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 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.

CTC subscribers will also benefit from its parent company's (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

CTC has registered with the Secure Telephone Identity-Policy Administrator via its parent company CTTC, using its own OCN 2750 and its parent company's OCN 2052. CTC uses the STIR/SHAKEN certificate issued to its parent company CTTC by the Ribbon Certification Authority (STI-CA) when we maintain, carry, and process calls originated and authenticated by CTTC. We have implemented a STIR/SHAKEN solution supplied by Ribbon.