



Robocall Mitigation Plan

This robocall mitigation plan is for Cochrane Cooperative Telephone Company ("CCT"), Operating Company Number (OCN) 0866, with headquarters at 103 West 5th Street, Cochrane, WI 54622. The primary contact for the robocall mitigation plan is:

Name:	Shawn Squires
Title:	Chief Executive Officer
Phone Number:	608.248.2323
Email:	s.squires@cochranetel.com

STIR/SHAKEN

CCT serves fewer than 100,000 voice subscriber lines and qualifies for the small-provider extension framework referenced in FCC rules implementing STIR/SHAKEN obligations under 47 CFR § 64.6305(a)(2). Where CCT is not yet able to implement STIR/SHAKEN across all originating traffic, we operate an appropriate robocall mitigation program for those portions of the network consistent with 47 CFR § 64.6304(a)(1).

At present, CCT's STIR/SHAKEN partner (TransNexus) does not accept all originating traffic, and CCT lacks the necessary facilities to authenticate all calls. We therefore qualify for an additional extension under 47 CFR § 64.6304(d). CCT will evaluate technical and vendor options on a rolling basis and will update its RMD filing as progress is made.

CCT utilizes a third-party hosted switch from Alianza, Inc. for a portion of its voice services. Alianza has certified in the FCC's RMD that it has implemented STIR/SHAKEN and is listed by the Secure Telephone Identity governance ecosystem (STI-PA) as an authorized provider. For calls originating on Alianza's network on CCT's behalf, CCT is using its own certificate and making its own attestation decisions in accordance with 47 CFR § 64.6301(b). Alianza authenticates calls in compliance with 47 CFR § 64.6301. CCT relies on Alianza's policies, analytics, and safeguards for those hosted segments while retaining ultimate responsibility for FCC compliance and for the mitigation actions described herein.

Robocall Mitigation Database (RMD) Filing

CCT is not prohibited by the Commission from filing in the RMD. CCT understands that all providers in the call path must maintain an active RMD filing, that downstream providers may not accept traffic from unlisted entities, and that CCT must block traffic received directly from any provider not listed in the RMD. CCT will promptly update its filing to reflect any material changes to this Plan, to STIR/SHAKEN implementation, or to upstream/downstream provider relationships.

Know Your Customer

CCT employs risk-based "Know Your Customer" procedures consistent with caller ID authentication best practices, including collecting entity-identifying information (legal name, business status, service address, contact data) for new and existing customers to establish an authenticated relationship and



assess operational legitimacy. Customer agreements prohibit illegal robocalls, and CCT may restrict or terminate service for violations.

We follow 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.

This process includes the collection and review of entity-identifying information to confirm that we have an authenticated relationship with the customer. We use this authenticated information to determine whether the customer is subject to any enforcement actions that restrict the type of calling that they may do, for example, if they have been banned from initiating telemarketing calls.

Our provisions with customers prohibit them from initiating illegal robocalls. If any customer is found in violation, the end user's service may be terminated.

Robocall Mitigation Program Monitoring & Controls

CCT monitors originating traffic, including Call Detail Records and analytics outputs, to detect suspicious patterns and takes reasonable steps to avoid originating illegal robocalls, consistent with 47 CFR § 64.6305. CCT analyzes traffic and flags activity for enhanced review when one or more of the following signals are present:

- High-volume traffic inconsistent with the customer's profile or service type.
- Large, bursty call attempts in short intervals.
- Short/very short duration calls or low average call duration.
- Low answer or completion ratios.

Sequential or neighbor-spoofing patterns (including potential international-origin spoofing trends emphasized in ongoing FCC proceedings).

When suspicious traffic is identified, CCT promptly investigates to determine whether the caller or upstream source is attempting to originate or transit unlawful robocalls. CCT documents investigations and outcomes for internal compliance and potential agency requests.

For calls originated on Alianza's hosted platform, Alianza provides real-time analytics, reputation insights, and alerts (e.g., invalid/unallocated caller IDs, Do-Not-Originate (DNO) matches, FCC consumer-complaint reputation signals, anomalous short-duration spikes). Alianza's detection helps CCT identify and stop illegal robocalls. When Alianza or CCT determines likely unlawful activity, CCT will require immediate remediation by the customer and may suspend or terminate service. CCT retains responsibility for enforcement and RMD accuracy.

Know Your Upstream Provider

CCT knows all carriers from which it receives traffic, confirms they are listed in the RMD, and has reviewed their published mitigation plans to understand their monitoring and mitigation methods. CCT will not accept traffic from any unregistered provider and will reassess relationships if a partner is removed from the RMD.



Traceback

CCT designates the contact below as its single point of contact for traceback requests. CCT commits to respond fully and within 24 hours to all traceback requests and to cooperate with the FCC, law enforcement, and the registered industry traceback consortium to investigate and stop illegal robocallers using its services, in accordance with 47 CFR § 64.6305(a)(2). As such, CCT states that the traceback request single point of contact shall be:

Name:	Shawn Squires
Title:	Chief Executive Officer
Phone Number:	608.248.2323
Email:	s.squires@cochranetel.com

Enforcement History

CCT is not the subject of any formal Commission, law enforcement, or regulatory action or investigation with an accompanying finding of actual or suspected wrongdoing related to transmitting, encouraging, assisting, or facilitating illegal robocalls/spoofing, or a deficient RMD certification or mitigation program description.

Recordkeeping and Plan Maintenance

CCT maintains records to demonstrate compliance with this Plan, including Know Your Customer/Know Your Provider documentation, analytics alerts, investigations, customer notices, and mitigation actions taken. CCT reviews this Plan at least annually and updates it as needed to reflect rule changes (including the 2025 third-party authentication guardrails) and operational improvements, and will update its RMD filing promptly upon any material changes.