



**Robocall Mitigation Plan for Continental Divide Electric Cooperative
d/b/a Red Bolt Broadband
(Revised February 2026)**

I. Background

The Federal Communications Commission (“FCC” or “Commission”) required all voice service providers to certify in the Commission’s [Robocall Mitigation Database](#) by June 30, 2021. Providers needed to confirm whether they had implemented STIR/SHAKEN. If a provider was subject to an applicable extension, it had to document and institute a robocall-mitigation plan to combat the origination of illegal robocalls on its networks.¹ The Commission explained that a robocall-mitigation program is sufficient if the plan’s detailed practices can “reasonably be expected to significantly reduce the origination of illegal robocalls.” The provider also must comply with the practices it describes in its filings.

Continental Divide Electric Cooperative (“CDEC”) d/b/a Red Bolt is dedicated to stopping illegal calls from originating on its network, and this document outlines CDEC’s current Robocall Mitigation Plan.

II. Commitment to Traceback Cooperation

CDEC commits to timely cooperating with and responding to Traceback requests from the FCC Enforcement Bureau and ITG (or any successor entity designated by the FCC). CDEC also responds to trace-forward investigations, valid law enforcement and government demands, subpoenas, and other valid legal processes. CDEC will dedicate sufficient resources to provide prompt and complete responses to these requests. CDEC will investigate suspicious activity found by its monitoring systems or reported by consumers or third parties and take appropriate action.

CDEC has established additional internal procedures to fulfill its commitment to cooperate with Traceback requests and take remedial action when needed:

- Troy McDowell, CDEC’s Telecommunications Manager, has been designated the responsible manager and will coordinate the handling of all Traceback requests that are received.
- If a traceback request is received, CDEC will email the customer a list of questions to properly investigate the scope of the request and determine whether the calls are legitimate.
- CDEC will also promptly call the relevant customer to inform them of the Traceback request and that CDEC has sent the customer an email requesting specific information related to the investigation.
- CDEC will separately audit the subject account and suspend or terminate the account if deemed to be sending illegal content.
- CDEC’s goal is to comply with all Traceback requests within 24 hours if commercially reasonable, and sooner when practicable.

¹ See <https://docs.fcc.gov/public/attachments/DA-24-73A1.pdf> (WCB Jan. 25, 2024, Public Notice).

III. CDEC's Know Your Customer ("KYC") Standards

CDEC is an electric cooperative that also resells retail VoIP service to residential and commercial customers in select areas of New Mexico. As part of onboarding, CDEC takes reasonable steps to verify customer identity before signing a written agreement.

During initial prospective-customer screening process, CDEC collects the following customer-identifying information when possible:

- Customer name,
- Customer's physical address, and
- Customer telephone numbers

IV. Telephone Number Authorization and STIR-SHAKEN Capabilities

As an interconnected VoIP reseller, CDEC is not subject to STIR/SKAKEN implementation requirements because it lacks control over the network infrastructure required to implement STIR/SKAKEN directly. However, CDEC understands that its underlying service provider authenticates its customers' traffic under STIR/SKAKEN. Additionally, CDEC customers may only use telephone numbers assigned by CDEC's underlying carrier, ensuring a documented, verified relationship between the end user and the telephone number used to originate calls.

V. Additional Information Required by Sixth Report and Order

The FCC requires all voice service providers to certify in the Commission's RMD, by March 1, 2026, whether they have implemented the STIR/SKAKEN authentication framework, and that all of the calls that it originates, carries, or processes are subject to a robocall mitigation program consistent with the Commission's rules.² The provider's mitigation plan "shall include reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls." 47 C.F.R. § 64.6305(a)(2).³

³ The TRACED Act defines "robocall violation" as "a violation of subsection (b) or (e) of section 227 of the Communications Act of 1934." TRACED Act § 11(d), Pub. L. No. 116-105, 133 Stat. 3274 (2019); id. at § 13(d)(f)(3) (defining a "suspected unlawful robocall" as a "call that the Commission or a voice service provider reasonably believes was made in violation of subsection (b) or (e) of section 227 of the Communications Act of 1934." Thus, CDEC's training and mitigation efforts focus, consistent with the TRACED Act, on potentially unlawful calls that violate either (a) 47 U.S.C. § 227(b) (governing non-emergency calls initiated with a prerecorded or artificial voice or an automatic telephone dialing system, as that term has been interpreted by the Supreme Court in *Facebook, Inc. v. Duguid*, 592 U.S. 395 (2001)) or (b) 47 U.S.C. 227(e), or the Truth in Caller ID Act, which prohibits people from causing "any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value," absent an applicable exemption.

CDEC notes that, by design, its services are provisioned to significantly curtail end users' ability to spoof their telephone numbers or otherwise commit TCPA violations. CDEC's end users are retail customers – both residential and small businesses – who use CDEC's resold VoIP service like traditional POTS service, not for high-volume use cases. Further, CDEC customers can only use caller IDs that they have verified, through the process described above, as their outbound caller ID, such that, absent some hacking event, which would violate CDEC's AUP, CDEC's end users cannot manipulate their caller ID. Thus, by design, CDEC's end users are prevented from using CDEC's services to violate 47 U.S.C. § 227(e).

The FCC's rules contemplate that the provider's plan should describe how it "complies with its obligation to know its customers pursuant to § 64.1200(n)(4), any procedures in place to know its upstream providers, and the analytics system(s) it uses to identify and block illegal traffic, including whether it uses any third-party analytics vendor(s) and the name(s) of such vendor(s)." 47 C.F.R. § 64.6305(d)(1)(ii). The Commission has acknowledged, however, that, "we do not currently require [] providers other than gateway providers to engage in 'know-your-upstream-provider' procedures, [but] if they have put such procedures in place, they must be documented in their robocall mitigation plan," and that "we do not specifically require providers to use call analytics." Sixth Caller ID Authentication Report and Order ¶ 40 & n.155-56. That said, CDEC directs the Commission to its KYC standards detailed above.