

Robocall Mitigation Policy

Robocall Mitigation Compliance with TRACED Act

Date	On behalf of	Change Summary
December 19, 2024	Mendocino Unified School District dba Mendocino Community Network	Revised Version: 1

Objective: Establish and follow a policy that is compliant with TRACED Act

I. Overview

The FCC requires that all providers certify in the Robocall Mitigation Database their status for compliance with STIR/SHAKEN. Those not yet fully compliant must implement and certify to the implementation of a Robocall Mitigation Plan to ensure that this illegal traffic does not originate on their networks as they work within the industry to become fully compliant.

The Commission requires voice service providers to develop a Robocall Mitigation Plan that:

- Details the reasonable steps taken to avoid originating illegal robocalls;
- Demonstrates a commitment to respond to traceback requests to cooperate with investigating and stopping illegal robocalls; and
- Is filed in the Robocall Mitigation Database.

This Robocall Mitigation Plan is submitted on behalf of the Mendocino Unified School District (MUSD)¹ doing business as the Mendocino Community Network (MCN), a small provider of VoIP services using SIP. MCN serves the rural communities in and around Mendocino, CA.

Mendocino Unified School District (MUSD) d/b/a Mendocino Community Network is a public school district organized and existing under California Education Code § 35000 et seq., and as such, has no parent companies, subsidiaries, or affiliates. As for MUSD's "principals", MUSD is governed by the MUSD Superintendent and an elected MUSD Board of Trustees. For more information see <https://www.mendocinoused.org/>

II. General Prohibition Against Illegal Robocalling

MCN's end user services are subject to restrictions contained in MCN's published legal policies and notices, including, but not limited to, MCN's Acceptable Use Policy, which currently prohibits end users from using its voice service for any illegal use, fraudulent activity, or forgery and

¹ MUSD is a small K-12 district located in Mendocino County on the rural coast of northern California, approximately three and half hours north of San Francisco.

Robocall Mitigation Policy

impersonation activities. Further, all executed MCN service orders subject each MCN end user to its terms of service (“TOS”).

MCN’s existing TOS prohibits activities normally associated with robocalling including, but not limited to:

- Providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call;
- Violating any applicable local, state or federal law; and
- Using the MCN service to engage in or in connection with fraudulent activities.

MCN’s end users are notified that MCN may take action up to suspension or termination of service for violation of the TOS.

III. Know Your Customer

MCN utilizes the mitigation technique of “Know Your Customer.” MCN is a small provider that maintains a close relationship with its customers. Its customers are generally “mom and pop” users and few of its total customer base have enough call paths to generate the high volume of traffic associated with robocalling allowing MCN to use in-house, targeted analytics to monitor, alert, and apprehend suspected robocalling activities.

MCN has set a screening for new and renewing customers requesting service at or above large volume calling capability levels:

- MCN will not deploy large volume calling capability as a residential service or at an address shown in the company records as being residential .
- Businesses requesting large volume calling capability must provide a tax ID and verification as to the nature of the business and justify the requested calling capacity.
- MCN verifies addresses to look for overlapping/multiple deployed voice path subscriptions.
- An MCN representative may visit the premise of the business to verify that the number of users at the location is appropriate for the volume of calling.

MCN’s Acceptable Use Policy and TOS provisions described in Section II of this Plan work to mitigate illegal robocall activity by MCN’s users and over MCN’s voice service.

IV. Know Your Upstream Providers

MCN’s current upstream providers for its VOIP services are: Commio, and Bandwidth. Prior to engaging with each upstream provider, MCN conducts due diligence on each company to ensure

Robocall Mitigation Policy

the company: (1) is current with its regulatory filing obligations; (2) has an excellent reputation within the industry; and (3) has an experienced voice services team.

Commio, and Bandwidth are trusted STIR/SHAKEN implementers that MCN has partnered with to ensure that MCN follows all robocall mitigation requirements. MCN, as part of these partnerships, is required to comply with each company's acceptable use policies and services agreements which include contractual provisions tailored to preventing unlawful robocall activity. These contract provisions include:

- Prohibitions against unlawful robocalls
- Prohibitions against unlawful, unsolicited, continues, and repetitive calls
- Required compliance with the FCC's STIR/SHAKEN rules
- Required compliance with the upstream provider's fraud mitigation requirements including compliance and cooperation with traceback requests
- Identification of unusual call patterns, excessive numbers and/or consistent excessive usage and establishes various disciplinary actions depending on the level of misuse

V. Network Monitoring

As noted earlier, MCN is small and to date relies on "Know Your Customer" as its primary mitigation/monitoring technique.

- **Device Identification:** Ensuring that every device connected to the network is known and authorized. This involves maintaining an inventory of devices, understanding their specifications, and monitoring for any unauthorized or suspicious devices.
- **User Authentication:** Verifying the identity of users accessing the network. This involves implementing secure authentication mechanisms such as username and password, multi-factor authentication, or other access controls to ensure that only authorized individuals can access the network.
- **Behavioral Analysis:** Understanding the typical behavior of users and devices on the network. This involves monitoring network traffic, analyzing patterns, and identifying deviations from normal behavior that could indicate security threats or anomalies.
- **Compliance Monitoring:** Ensuring that the network and its users comply with relevant regulations and policies. This may include monitoring for activities that violate policies, industry standards, or legal requirements.
- **Risk Assessment:** Evaluating the potential risks associated with each user and device on the network. This involves assessing vulnerabilities, potential security threats, and the impact of a security incident on the network.

Robocall Mitigation Policy

VI. Traceback and Enforcement Cooperation

MCN will actively cooperate with the traceback community including the FCC, law enforcement, and The Industry Traceback Group (ITG) to investigate and stop illegal robocalls. MCN will dedicate sufficient resources to provide prompt and complete responses to traceback requests within 24 hours in accordance with CFR Section 64.1200(n).