

NEK Community Broadband, d/b/a NEKCV, d/b/a NEK Broadband, and d/b/a CVFiber Robocall Mitigation Compliance with TRACED Act

Date	Company Contact
03/01/2026	Christa Shute

This mitigation plan is submitted on behalf of NEK Community Broadband, d/b/a NEKCV, d/b/a NEK Broadband, and d/b/a CVFiber (“NEKCV”). NEKCV is a Communications Union District (CUD), which is a special-purpose municipality organized pursuant to Chapter 82 of Title 30 of the Vermont Statutes Annotated comprised of seventy-two member towns. As a municipality, the organizational structure of a CUD is defined by statute. Governance is comprised of a Governing Board made up of delegates and alternates from the member towns of the district. NEKCV provides broadband and other services within its member towns.

I. Implementation and Extension Status

Status of STIR/SHAKEN Implementation

NEKCV offers its customers Voice Over Internet Protocol (VoIP) services as a reseller of white-labeled services offered by Waitsfield-Fayston Telephone Co., Inc. (“WCTV”). NEKCV does not control the softswitch, number porting or call trunking for the associated calls. Accordingly, NEKCV does not have the facilities necessary to implement STIR/SHAKEN. NEKCV has, however, adopted this robocall mitigation plan to establish procedures intended to limit the potential for the origination, carrying, or processing of unlawful robocalls from its voice services.

II. Robocall Mitigation Plan

Under its arrangements for authentication and verification with its underlying service provider, NEKCV has taken further steps to prevent robocalls from originating from its end user customers.

Know Your Customer

NEKCV utilizes the mitigation technique of “Know Your Customer” and follows the North American Numbering Council (NANC) – Call Authentication Trist Anchor Working Group guidelines and best practices for vetting caller identity [NANC CallerID Best Practices](#).

This includes confirming the identity of NEKCV’s customers – (i) contact person(s); (ii) business location; (iii) state or country of incorporation; (iv) federal tax identification; and (v) the nature of our customer’s businesses.

Robocall Mitigation

NEKCV is a small community-owned provider that maintains a close relationship with its subscribers. 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 us to use targeted in-house analytics to monitor, alert and apprehend suspected robocalling activities.

NEK Community Broadband, d/b/a NEKCV, d/b/a NEK Broadband, and d/b/a CVFiber Robocall Mitigation Compliance with TRACED Act

NEKCV has set a call path level based on its average customer size. The level – referred to as “large volume calling capability” – is subject to change.

NEKCV has a screening for new customers requesting service at or above large volume calling capability levels:

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

Contractual Terms

All customers are subject to the company’s terms of service that prohibit and warn against the use of the services for illegal activities.

NEKCV provides a subscription-based, non-commercial legal robocalling product and educates any subscribers or potential subscribers (such churches, school systems) regarding legal versus illegal robocalling activities to insure they are compliant in their use of the product.

Know Your Upstream Provider

While NEKCV does not currently serve upstream providers, it recognizes that effective May 28, 2024 its underlying service provider must refuse to carry traffic from any provider not listed in the Robocall Mitigation Database.

Call Analytics Systems

WCTV uses call analytics software provided by TransNexus to monitor all outbound voice traffic in real-time to prevent the origination or transit of illegal robocalls. The software provides detailed reporting to identify suspected illegal robocalls. The system alerts WCVT to outbound calls where the calling number has a poor reputation or is invalid, unallocated, or on a Do Not Originate list.

WCTV will immediately ask NEKCV to investigate any unidentified calls to determine if the caller was attempting to originate unlawful robocalls. If NEKCV or WCTV determine that the caller was attempting to originate unlawful robocalls, our policy is to warn them to stop, suspend their service, and/or terminate their account.

Plan Updates

NEK Community Broadband, d/b/a NEKCV, d/b/a NEK Broadband, and d/b/a CVFiber Robocall Mitigation Compliance with TRACED Act

NEKCV will continue to work with WCTV to monitor industry best practices and improve our internal processes to ensure our systems adapt to address the ongoing challenges affecting this industry.

III. Traceback and Enforcement Cooperation

NEKCV, both directly and through its underlying service provider, will actively participate in the traceback community including the FCC, law enforcement, and The Industry Traceback Group (ITG). NEKCV commits to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium and will cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

IV. Additional Certifications

Neither NEKCV nor any entity which shares common ownership, management, directors, or control has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.