



Peak Data Networks Inc.
Robocall Mitigation Program
as of February 5, 2026

(DISTRIBUTION: This document does not contain any confidential and/or proprietary information. It is authorized for release to the general public.)

Document History

- **2025-02-05:** Initial version.

The initial document incorporates our Robocall Mitigation Program (RMP) as it exists as of the document date. It documents our current RMP policies and practices, including elements that have been in place since prior to being subject to file a RMP. It also documents planned and anticipated enhancements to our program and practices that we expect to implement through the twelve months following the document date.

Provider Profile

- **Provider Information**

- Name: **Peak Data Networks Inc.
(DBA "Peak DataNet")**
- FCC Registration Number: **0031860562**
- Structure: **501(c)(3) charitable non-profit corporation**
- Main Address: **610 Lacey Road Unit 749
Forked River, NJ 08731-8037**
- Main Telephone: **+1 848-858-7325**
- Website: **<https://www.peakdatanet.org>**
- General Email: **general@peakdatanet.org**
- Responsible Officer: **Terri Beideman, Executive Director**
- DC Legal Process Address: **Peak Data Networks Inc.
c/o Registered Agents Inc.
1717 N Street NW Ste 1
Washington, DC 20036-2827**

- **Robocall Mitigation Issues and Inquiries**

- Contact: **Network Operations**
- NOC Telephone: **+1 848-777-4736 (SMS/MMS enabled)**
- NOC Emails: **peakdatanet@noc-mail.net
and/or noc@peakdatanet.org**

Provider Overview

Peak Data Networks Inc. (DBA “Peak DataNet”) is a small 501(c)(3) public charity focused on digital inclusion in New Jersey and beyond by providing affordable, high-quality internet access, digital literacy training, refurbished access devices, and resilient connectivity solutions. As part of our mission, we are developing plans to become an ETC to offer Lifeline-eligible voice and broadband services to low-income households, immigrants, seniors, and small businesses in underserved areas.

Peak Data Networks Inc. currently operates as a non-facilities-based interconnected VoIP provider (self-provider phase) and, during 2026, plans to transition to offering services to end users and limited partners as an originating and intermediate provider in pilot programs.

Our initial pilot programs will consist of carefully selected partners and participants, as we build capabilities and pursue regulatory approvals (e.g. for Lifeline and MVNO operations).

We are also planning and implementing Voice over Internet Protocol (VoIP) services as a pilot programs. These services will primarily be delivered over broadband networks, in partnership with certified carriers and infrastructure providers. We anticipate serving a limited number of subscribers initially (e.g., pilot programs with a maximum of 500-1,000 users), focusing on community impact rather than large-scale commercial operations.

Our network includes IP-based elements but may interface with non-IP legacy systems during initial rollout. As part of our pivot from self-provider to a provider of services to others, we are building duplicate infrastructure, that will eventually replace our existing IP-based systems with resilient, highly-available, carrier-grade technologies.

STIR/SHAKEN Implementation Status

- **Current Status:** Our “self-provider” infrastructure is fully STIR/SHAKEN capable. At this time, we utilize the services of our origination and termination providers for STI-AS and STI-VS.
- **Prior to Offering Services to Third Parties:** Before we offer services to third parties, either as part of our pilot programs or in any other manner, we will implement measures to ensure that all traffic originating on our network is authenticated in accordance with STIR/SHAKEN protocols (with full A-level attestation where feasible). In addition, all traffic that enters our network through our DID providers will be compliant with STIR/SHAKEN.
- **Under Consideration:** We are considering implementing ENUM (IETF RFC 3761) endpoints for selected incoming traffic on an experimental basis. We are a supporter of this technology but are aware of its limitations and its limited adoption. If we do establish ENUM routing and endpoints, some traffic that enters our network through these endpoints may not be compliant with STIR/SHAKEN, as we then do not have control over the upstream provider and their level of compliance with STIR/SHAKEN. Any traffic that enters through these endpoints, and is not STIR/SHAKEN compliant, will be specially tagged by our monitoring systems, enabling enhanced monitoring, and we will also notify end-users with a CNAM prefix, as described in this document.

- **Timeline for Full Implementation:** We commit to achieving full STIR/SHAKEN deployment by December 31, 2026, subject to partnerships with compliant vendors and FCC/BPU approvals for our ETC designation.

Robocall Mitigation Program

Peak DataNet takes reasonable steps to ensure our network does not originate, carry, or process illegal robocall traffic. Our mitigation program is designed with our non-profit mission in mind, emphasizing transparency, community trust, and collaboration with regulators and industry groups. We focus on preventing abuse in our limited-scale services, which target vulnerable populations unlikely to engage in high-volume calling.

Key components of our current RMP include:

- **Know-Your-Customer (KYC) and Customer Onboarding Procedures:** Prior to provisioning voice services, we conduct thorough identity verification for all subscribers. We will be conducting our pilot project KYC in alignment with Lifeline eligibility requirements (e.g., income verification). This includes:
 - Requiring government-issued ID, proof of address, and eligibility documentation.
 - Screening against databases for known bad actors (e.g., FCC's Do-Not-Originate list and industry blacklists).
 - Contractual agreements prohibiting use of our network for illegal robocalls, with immediate termination clauses for violations. While we do not anticipate having any resellers, if we do, we will mandate KYC standards and establish the right of Peak DataNet to audit their compliance with these standards.

Prior to Offering Services to Third Parties, we will be enhancing our RMP with the following additions:

- **Network Monitoring and Analytics:** As part of the buildout of our carrier-grade technology stack, we will be incorporating real-time analytics tools to monitor call patterns for suspicious activity, such as:
 - High-volume short-duration calls (HVSDs).
 - Anomalous international or premium-rate traffic.
 - Caller ID spoofing attempts. Unless we have an end-user with special authorization, such as law enforcement organizations, we will not allow caller ID spoofing on our network and will maintain compliance with the Truth in Caller ID Act (47 U.S.C. § 227(e)). Though spoofed calls will result in an error for the end-user (rather than complete), we will proactively monitor for attempts to spoof caller ID, which will generate automatic alerts as well as end-user notification. In our experience, some caller ID spoofing is unintentional and actually the result of end-user misconfiguration, so we believe that proactive notification to customers will help to ensure they are properly configured. Traffic will be monitored by automated systems in real-time, and anomalous traffic will be reviewed by

authorized personnel at least daily, with logs retained for six (6) months to support tracebacks.

- **Mitigation Actions:**

- **Blocking, Filtering, and Notification:** We will implement caller ID authentication checks and block unsigned or low-attestation calls when possible, adapting our practices to “real world” expectations of traffic desired by end-users. For incoming calls, we will utilize CNAM prefixes to designate calls that have been unsigned or identified as probable spam, probable robocall, or entering our network through ENUM or other public endpoints.
- **Contractual Safeguards:** All vendor and interconnection agreements require robocall mitigation plans and STIR/SHAKEN compliance, with penalties for non-compliance.
- **Under Consideration:** We are considering developing and implementing the capability for end-users to whitelist individual numbers, based on their personal preferences. The whitelist dataset can be used to better fine-tune our automated filtering processes. Any whitelist we develop will include the capability for customers to remove a number from the whitelist, should their preferences change, or in the event that the number is repurposed.

- **Traceback Cooperation:**

- We will register with the Industry Traceback Group (ITG) and commit to responding to traceback requests within 24 hours, providing all relevant call detail records (CDRs), customer info (subject to privacy laws), and mitigation actions taken.
- During 2026, we plan on beginning to participate in industry forums (e.g., ATIS/SIP Forum) to share best practices.

- **Internal Policies and Training:**

- Staff receive annual training on robocall compliance, with designated personnel overseeing mitigation. We will conduct quarterly audits of our program and report findings to our Board of Trustees.

- **External Communications:**

- We plan on maintaining our Robocall Mitigation Program on an ongoing basis, and will be updating this public description, as well as our internal policies, procedures, and documentation regularly, to ensure that we continuously improve our network and policies. If appropriate, we will submit confidential and/or unredacted information through the procedures described by the Commission, in addition to our public disclosure.

Our program is scalable as we expand beyond pilots, with ongoing evaluations to incorporate FCC updates (e.g., enhanced gateway provider rules).

We will update this filing within ten (10) business days of any material change to our operations, contact information, or mitigation practices, as required under the Commission's rules effective February 5, 2026.

CERTIFICATION

Pursuant to the requirements of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act) (47 U.S.C. § 227 *et seq.*), as well as Federal Communications Commission (FCC) regulations to implement the provisions of the Act (47 C.F.R. § 64.1200 *et seq.*), Peak Data Networks, Inc. hereby submits our Robocall Mitigation Program.

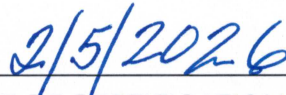
Under penalty of perjury, Peak Data Networks Inc. hereby certifies that:

- We have implemented STIR/SHAKEN on IP portions of our network and apply a robust mitigation program to current traffic, and we plan to expand on this as described herein;
- All calls originating on our network are either signed in accordance with the STIR/SHAKEN protocols and/or subject to our robust mitigation program to prevent illegal robocalls;
- We take reasonable steps to know the traffic we originate and avoid carrying or processing illegal robocall traffic;
- During the two (2) year period preceding this certification, Peak Data Networks Inc. and/or any entity which shares common ownership, management, directors, or control has NOT been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing related to illegal robocalling, spoofing, or a deficient Robocall Mitigation Program filing;
- All information in this submission is true, accurate, and complete to the best of our ability.



PEAK DATA NETWORKS INC.

TERRI BEIDEMAN, EXECUTIVE DIRECTOR



DATE OF CERTIFICATION