

Robocall Mitigation Plan Personal Computers Plus FCC Registration Number (FRN): 0031491517 Business Address: 573 Ocean Blvd, Hampton, NH 03842 **Telephone:** (603) 929-4272 **Email:** JHouston@PersonalComputersPlus.com

Prepared by Authorized Officer: Jeffrey Houston, Compliance Officer **Date:** February 24, 2026

1. Company Role in the Call Chain

Personal Computers Plus is a **voice service provider** that acts as a reseller of interconnected VoIP services to end-user customers. We originate calls placed by our customers but do not own or control any switching facilities or network infrastructure. All outbound traffic is handed off to our upstream providers for carriage to the PSTN. We serve only small and medium-sized businesses and municipal governments located in the United States.

2. STIR/SHAKEN Implementation Status (Option 3 – No STIR/SHAKEN Implementation)

We have **not implemented STIR/SHAKEN** on any portion of our network and claim exemption from the implementation obligation under the FCC's rules (47 CFR § 64.6304 and related Orders) because we are a small, pure reseller that lacks control over the network infrastructure necessary to implement STIR/SHAKEN (no switching facilities or direct IP network control).

We are entirely dependent on our four upstream providers, who implement and manage STIR/SHAKEN authentication on our behalf for all calls originating from our customers. The upstream providers are:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Each upstream provider is registered in the Robocall Mitigation Database and performs caller-ID authentication using their own STIR/SHAKEN certificates and infrastructure. We contractually require them to authenticate all eligible traffic passed from our customers and monitor their ongoing compliance through regular account reviews and contractual obligations. Because we have no direct access to the authentication infrastructure, full or partial implementation by Personal Computers Plus is not feasible or required.

3. Robocall Mitigation Program – Specific Reasonable Steps to Prevent Origination of Illegal Robocalls

We implement the following affirmative, effective measures focused on customer vetting, contractual controls, monitoring, and rapid response. These steps are reasonable and tailored to our low-risk customer base and reseller model.

A. Affirmative Measures to Prevent New and Renewing Customers from Originating Illegal Robocalls (Know-Your-Customer / Customer Vetting) We maintain an exceptionally strong, relationship-based KYC process:

- Every customer is personally known to us. More than 90% began as our long-term Information Technology clients before adding telephony service.
- All installations and activations require an in-person site visit at the customer's business location, where we meet principals and install hardware.
- We provide ongoing on-site maintenance and repair services, resulting in repeated in-person contact at the customer premises.
- We fully understand the nature of each customer's business (e.g., local retail, professional services, municipal government offices), which involves legitimate, low-volume business communications rather than high-volume outbound dialing.
- New and renewing customers must provide physical business address verification (confirmed in person), primary contact information, and sign a service agreement that expressly prohibits: (i) origination of illegal robocalls, (ii) spoofing, (iii) use of auto-dialers for unsolicited calls in violation of the TCPA or any other law, and (iv) any traffic that would violate FCC rules. Violations trigger immediate investigation and potential termination.
- We do not sell services to resellers, wholesalers, international call originators, or any high-risk entities.

These in-person, relationship-driven controls make it highly unlikely that any customer could originate illegal robocalls without our immediate knowledge and ability to intervene.

B. Call Analytics Systems We do not operate independent call-analytics systems. We rely on the robust, industry-standard analytics platforms of our four upstream providers which actively monitor for illegal robocall patterns, high-volume anomalous traffic, and known bad actors. The upstream providers notify us promptly of any issues involving our customers. We supplement this with our own billing and CDR review for usage anomalies. Upon any alert, we immediately investigate with the customer using our direct relationship.

C. Procedures to Know Upstream Providers We maintain active, written contracts with only the four upstream providers listed in Section 2. We verify their current registration and good standing in the Robocall Mitigation Database at least annually and upon any material change. Traffic is routed exclusively through these known, compliant providers; no other upstream carriers are used.

D. Traceback and Law-Enforcement Cooperation Jeffrey Houston (Compliance Officer) is the designated point of contact for all traceback requests. We commit to responding fully and completely to every traceback request from the Industry Traceback Group, the FCC, or law enforcement **within 24 hours**. Our process includes:

1. Immediate review of customer records and CDRs obtained from upstream providers.
2. Direct contact with the customer (leveraging our in-person relationship).
3. Provision of all available information to the requesting entity.
4. Immediate blocking or disconnection of any customer confirmed to be originating illegal robocalls.

We cooperate fully in any investigation and will terminate service as necessary to stop illegal traffic.

E. Enforcement History Neither Personal Computers Plus nor any affiliated entity has been the subject of any FCC or other law-enforcement action or investigation in the prior two years concerning suspected illegal robocalling, spoofing, or deficiencies in Robocall Mitigation Database filings.

F. Additional Commitments

- We will monitor the Robocall Mitigation Database for any changes affecting our upstream providers and update this plan within 10 business days of any material change in our operations.
- We annually recertify this filing as required.
- This Plan is reviewed internally at least annually for effectiveness.

This Robocall Mitigation Plan is actively followed and constitutes the complete set of reasonable steps we take to prevent the origination of illegal robocalls.

Certification I certify under penalty of perjury that the foregoing is true and correct, that all calls originated by Personal Computers Plus are subject to this robocall mitigation program, and that the information provided in this filing is accurate and complete.

Signed,

Jeffrey Houston

Authorized Compliance Officer

Personal Computers Plus

February 24, 2026