

# Robocall Mitigation Plan for Parwan Electronics Corporation (PEC)

Revised November 22, 2024

Parwan Electronics Corporation  
1230 Highway 34  
Aberdeen, New Jersey 07747 – USA  
Tel: 1-732-290-2900  
email: [atschand@voicesaver.com](mailto:atschand@voicesaver.com)  
[www.voicesaver.com](http://www.voicesaver.com)

**Company Information:**

- **Company Name:** Parwan Electronics Corporation  
**Address:** 1230 Highway 34, Aberdeen, New Jersey 07747, USA  
**Phone:** 1-732-290-2900  
**Email:** [atschand@voicesaver.com](mailto:atschand@voicesaver.com)  
**Website:** [www.voicesaver.com](http://www.voicesaver.com)  
Incorporated in 1984.

**Principals:**

- Suraj Tschand ([suraj@voicesaver.com](mailto:suraj@voicesaver.com))  
President & CEO  
1-732-290-1900 x 3100
- Ajay Tschand ([atschand@voicesaver.com](mailto:atschand@voicesaver.com))  
CTO  
1-732-290-1900 x 3225
- Vinay Tschand ([vinay@voicesaver.com](mailto:vinay@voicesaver.com))  
COO  
1-732-290-1900 x 3224

**Affiliates:**

- None

**Subsidiaries:**

- None

**Parent Company:**

- None

This Robocall Mitigation Plan is submitted by Parwan Electronics Corporation (PEC) pursuant to the provisions of 47 C.F.R. § 64.6305, adopted by the Federal Communications Commission (FCC), which require all “voice service providers” to establish a “robocall mitigation plan.” This document sets forth PEC’s current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network. PEC views these policies and procedures as constituting “reasonable steps” to avoid the origination of illegal robocalls on its network and, in addition to following these steps, PEC commits to responding to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG), and to cooperate with such entities in investigating and stopping any illegal robocallers that may use its service to originate calls.

## **1 - Steps Taken to Avoid Originating Illegal Robocall Traffic:**

### **A. Know Your Customer (KYC) Policy:**

- Parwan Electronics Corporation has a robust KYC policy to prevent services from being used to originate illegal traffic. We extensively investigate potential business customers seeking access to high-volume origination services by collecting information such as their physical business location, contact person(s), state or country of incorporation, federal tax ID, and the general nature of their business.

### **B. Contractual Provisions:**

- All business customers are required to sign contracts that contain provisions allowing for termination in the event high-volume origination services are abused. Parwan Electronics Corporation enforces these provisions as necessary.

### **C. Monitoring and Analytics:**

- We continuously monitor call patterns and employ advanced analytics systems to identify and block illegal robocall traffic. This includes real-time detection and mitigation measures.

### **D. STIR/SHAKEN Implementation:**

- As of February 21, 2024, all voice traffic that originates or terminates on our network is authenticated or verified with STIR/SHAKEN. We work with partner carriers to ensure STIR/SHAKEN authentication and verification for voice traffic on the IP portions of our network that support SIP calls.

## **E. Telephone Number Validation Practices**

At Parwan Electronics Corporation (PEC), we prioritize the integrity of our network by ensuring that all telephone numbers used by our customers are valid and authorized for their use. As part of our commitment to industry best practices, we have implemented robust procedures to validate the right of our customers and end-users to use specific telephone numbers in connection with their subscribed voice services.

For single-line voice service subscribers, whether connected via TDM (Time Division Multiplexing) or IP (Internet Protocol), PEC ensures that our switching equipment only accepts calls originating from the assigned number. For subscribers using multi-line telephone systems, PEC performs additional validation by screening all originating calls. Only calls that originate from numbers specifically assigned to the subscriber are permitted to be connected. These processes ensure that the originating telephone number is accurately validated, providing both an automated and secure method of number validation that prevents unauthorized usage of telephone numbers within PEC's network.

## **2. Compliance with Know Your Customer (KYC) / Providers Obligations:**

To comply with our obligation know our customers and/or upstream providers, PEC implements comprehensive due diligence processes. This involves several key steps:

- A. **Customer Verification:** We conduct thorough verification of our customers' identities and business operations. This includes collecting and verifying information such as business names, addresses, registration details, and ownership structures. Utilizing Know Your Customer (KYC) procedures, which involve checking against government databases and industry blacklists, ensures that our customers are legitimate and not involved in fraudulent activities.
- B. **Upstream Provider Vetting:** We also vet our upstream providers to ensure they are reputable and compliant with industry regulations. This involves obtaining and reviewing the upstream provider's robocall mitigation practices, certifications, and compliance records. Ensuring upstream providers adhere to similar standards helps prevent illegal robocalls from entering our network. PEC also limits the number of upstream providers used and uses only reputable companies with traceable histories.

- C. **Ongoing Monitoring:** Continuous monitoring of customer and upstream provider activities is essential. We use advanced analytics and monitoring tools to detect suspicious call patterns or behaviors that could indicate illegal robocall activity. Regular audits and reviews of customer and provider records help maintain compliance and identify any potential risks.
- D. **Traceback Cooperation:** We are committed to cooperating with traceback requests from authorities such as the FCC, law enforcement, and the Industry Traceback Group (ITG). This involves maintaining detailed call records and being able to quickly provide information to trace the origin of suspected illegal robocalls.
- E. **Compliance and Training:** Implementing robust compliance programs and training for our staff ensures that everyone involved understands the importance of these obligations and the specific procedures to follow. This includes regular updates on regulatory changes and best practices for mitigating robocall risks.

By implementing these measures, PEC effectively complies with its obligation to know its customers and upstream providers, thereby reducing the risk of illegal robocall traffic on its networks.

### 3. Analytics Systems Used to Identify & Block Illegal Traffic

PEC utilizes a multi-layered approach to identify and block illegal robocall traffic on its network. The primary analytics system we use (based on Cisco, TelcoBridges & 3CX technology) integrates both artificial intelligence (AI) and machine learning (ML) algorithms to analyze calling patterns, behavior, and historical data. These systems are continuously trained to recognize and flag unusual call volumes, high-speed dialing patterns, and other indicators typically associated with robocalls. PEC also uses in-house software to block any calls that follow abuse patterns identified by several characteristics we have identified over time.

Our system also integrates real-time call data analytics, which includes verifying the integrity of Caller ID information through SHAKEN/STIR protocols. This ensures that any suspicious calls with invalid or mismatched Caller ID information are flagged immediately. By applying these advanced technologies, PEC can continuously improve its detection capabilities, ensuring that most of the illegal traffic is blocked before reaching end users.

Furthermore, PEC employs a feedback loop system, where blocked calls are reviewed by a dedicated team to refine and update the blocking algorithms. This ensures that our systems stay responsive to new robocall tactics and prevent false positives. As part of our

compliance with industry standards and best practices, PEC also participates in industry traceback efforts to assist in identifying the origins of illegal robocalls and further strengthens our blocking mechanisms."

This response outlines how the provider's system uses advanced analytics to detect and prevent illegal robocalls, ensuring the mitigation plan complies with FCC regulations and industry guidelines.

#### **4. Third-Party Analytics Vendors**

To mitigate robocalls, PEC employs a combination of in-house technology alongside solutions from several third-party vendors:

**A. ProSBC by TelcoBridges**

TelcoBridges provides ProSBC, a session border controller (SBC) designed to secure VoIP networks. It helps with call quality management, fraud prevention, and robocall detection.

**Contact Information:**

TelcoBridges Inc.

138 De La Barre, Boucherville, Quebec, Canada J4B 2X7

Phone: +1-450-655-8993

Fax: +1-450-655-9511

Email: [info@telcobridges.com](mailto:info@telcobridges.com)

- B.** 3CX provides its enterprise phone systems and is a communications platform that offers a range of call management features, including robocall detection, call blocking, and voice security tools. It integrates seamlessly with other systems to detect and filter fraudulent calls.

**Contact Information:**

3CX Ltd.

14 Tower Road, Suite 203, Mooresville, NC 28117, USA

Phone: +1-866-493-0797

Email: [sales@3cx.com](mailto:sales@3cx.com)

- C.** Cisco's solutions for call security include network-level protections and robust fraud prevention features, addressing robocalls through both its hardware and software products. Cisco's advanced analytics and machine learning tools help in identifying and blocking robocalls in real-time. PEC utilizes Cisco's CUBE

technology in combination with PEC's VoiceSaver software to mitigate robocalls.

**Contact Information:**

Cisco Systems, Inc.

170 West Tasman Dr., San Jose, CA 95134-1706, USA

Phone: +1-800-553-6387

Website: [www.cisco.com](http://www.cisco.com) .