# ROBOCALL MITIGATION PROGRAM

**Entity Name:** We Pro Inc.

**FRN:** 0039045455

**Primary Business Address:** 5726 Dumfries Dr, Houston, TX 77096

**Primary Contact:** Shmuel Rottman, President

**Email:** sam@wepro.ai

**Telephone:** 214-400-3130

## 1. Company Overview

We Pro Inc. ("Company") operates a cloud-based business management and communications platform supporting business telephone calls, customer service, dispatch operations, and automated answering services.

The Company utilizes Bandwidth as an underlying telecommunications provider for telephone number provisioning, Public Switched Telephone Network (PSTN) connectivity, and applicable carrier-level telecommunications functions.

The Company's platform supports application-level call handling and routing, including through FreeSWITCH.

The Company maintains customer account-level calling controls and prohibits illegal robocalling, unauthorized caller identification, fraudulent communications, and other unlawful calling activities.

## 2. STIR/SHAKEN Authentication

The Company utilizes Bandwidth for carrier-level STIR/SHAKEN authentication functions under its telecommunications service arrangements.

Bandwidth provides the underlying PSTN connectivity and performs applicable call authentication functions. The Company does not independently operate a STIR/SHAKEN certificate signing service.

The Company maintains its own customer-level robocall mitigation procedures, including Caller ID restrictions, customer identification, call recordkeeping, suspicious activity investigation, and outbound calling suspension.

## 3. Customer Identification and Verification

The Company maintains customer registration and account information, including business names, email addresses, and other identifying information collected during onboarding.

Additional business identification, registration documentation, tax identification information, or other verification materials may be requested when required by applicable services, underlying telecommunications providers, or compliance investigations.

Employer Identification Numbers are not universally required for ordinary business customer accounts.

Customer account information is maintained to identify responsible account holders and facilitate investigations of suspected misuse of the Company's communications services.

## 4. Authorized Caller Identification

Customers can originate outbound calls only using telephone numbers assigned to their respective WePro accounts.

The WePro platform does not provide customers with functionality to manually substitute, modify, or spoof originating Caller ID information.

Outbound communications are associated with the telephone numbers assigned to each customer's account.

## 5. Acceptable Use and Prohibited Activities

The Company maintains a published Telecommunications Acceptable Use Policy as part of its website Terms and Conditions.

The policy prohibits illegal robocalls, fraudulent communications, unauthorized Caller ID spoofing, unlawful telemarketing, and other violations of applicable telecommunications laws.

Customers are responsible for complying with applicable requirements under the Telephone Consumer Protection Act (TCPA), the Telemarketing Sales Rule (TSR), Do Not Call regulations, and other relevant federal and state laws.

The Company reserves the right to restrict, suspend, or terminate telecommunications functionality associated with suspected or confirmed unlawful activity or violations of its policies.

## 6. Illegal Robocall Detection and Mitigation

The Company maintains the following operational measures to identify, investigate, and mitigate potentially unlawful calling activity:

**A. Caller ID Restrictions**

Customers are limited to originating calls using telephone numbers assigned to their respective WePro accounts.

**B. Customer Identification**

The Company maintains customer registration and account information that allows calling activity to be associated with the responsible customer.

**C. Call History and Traceability**

The Company's systems maintain call records identifying originating telephone numbers, destination telephone numbers, call timestamps, and associated customer accounts.

These records support the investigation of reported or suspected unlawful communications.

**D. Traffic Monitoring and Investigation**

The Company reviews suspicious calling activity and complaints received from customers, telecommunications providers, or other relevant parties.

The Company utilizes available call records and account-level calling information to investigate potentially unlawful traffic and identify the responsible customer.

**E. Automated Traffic Analytics**

The Company utilizes an internal automated analytics system to monitor unusual outbound calling activity and identify potentially suspicious calling patterns.

Identified activity may be reviewed through customer account records, calling history, and other available operational information.

**F. Outbound Calling Suspension**

Authorized Company administrators can disable outbound calling functionality for individual customer accounts when necessary to investigate or prevent suspected unlawful activity.

**G. Carrier Coordination**

The Company cooperates with its underlying telecommunications providers in investigating suspicious or unlawful calling activity and implementing appropriate mitigation measures.

# 7. Telecommunications Provider Coordination

The Company utilizes Bandwidth for telecommunications connectivity and applicable carrier-level services.

The Company maintains information identifying its telecommunications provider relationships and cooperates with its providers regarding suspected unlawful traffic, traceback investigations, and necessary calling restrictions.

Where appropriate, the Company coordinates with its underlying telecommunications providers to identify affected calls, investigate reported abuse, and prevent further unlawful traffic.

# 8. Traceback Cooperation

Pursuant to 47 CFR § 64.6305(a), the Company commits to responding within 24 hours to traceback requests from the Federal Communications Commission, law enforcement agencies, and the Industry Traceback Consortium.

The Company commits to cooperating with these entities in investigating and stopping illegal calling activity involving its services.

Upon receiving a traceback request, the Company will, as appropriate:

1. Review relevant call records and customer account information.
2. Identify the originating customer account and associated telephone number.
3. Coordinate with the applicable underlying telecommunications provider.
4. Investigate suspected unlawful activity and take appropriate mitigation measures, including disabling outbound calling when warranted.
5. Provide responsive information to the requesting authority in accordance with applicable law.

**Designated Traceback Contact:**

Shmuel Rottman, President

Email: sam@wepro.ai

Phone: 214-400-3130

# 9. Program Maintenance and Recertification

The Company will maintain and periodically review its Robocall Mitigation Program to reflect its actual operations and applicable regulatory requirements.

The Company will update its Robocall Mitigation Database filing within 10 business days following changes requiring an update under 47 CFR § 64.6305.

The Company will complete its required annual Robocall Mitigation Database recertification on or before March 1.

The Company is committed to preventing misuse of its communications platform, cooperating with telecommunications providers and regulatory authorities, and maintaining reasonable safeguards against illegal robocalling and fraudulent communications.

**Authorized Officer:** Shmuel Rottman

**Title:** President