

## Robocall Mitigation Plan (RMP)

*For the Robocall Mitigation Database (RMD)*

---

The following outlines [ **PBX Interactive | PBXi | iPBEX** ]'s ongoing robocall mitigation efforts on our platform / network.

### Call Blocker (cloud app)

- On the [iPBEX Dashboard](#) > Calls (CDR) tab, end users can **simply** click on a displayed **Caller ID Number** to enable call blocking using **(4) account-wide blocking methods**:
  - Instant Hangup
  - Transfer to Voicemail
  - Play “number not in service” message
  - Play “not accepting call message”

### Call Trapper (cloud app)

- On the [iPBEX Dashboard](#) > PBX Manager > DID Numbers tab, end users can easily click on any of their DID Numbers and to **Call Trapper**, our automated SPAM / Robocall blocker.
- **Call Trapper**
  - Performs an **instant risk assessment** to determine if the caller is either **known** or **suspected** spam; based on reports of scams, fraud, telemarketing and other annoyances, using various sources, and perform a “**Trap Action.**”
  - **Trap Actions**:
    - **Known Spam**: Call Trapper intercepts the incoming call and plays a “*Number not in service*” message, then hangs up.
    - **Suspected Spam**: Call Trapper intercepts the incoming call, and **challenges** the caller via a **Phone Captcha** – which prompts the caller to enter a random digit sequence. Callers failing the phone captcha, will be upgraded to **Known Spam**.

### Call Behavior Monitoring / Know Your Customer (internal)

- As a fully managed VoIP provider, we **normally** have direct control over end-user **VoIP PBX equipment** and VoIP Phones.
- Basic know your customer (KYC), procedures are in place to determine the nature of business / typical-use for calls originating on our platform (see page 2 for KYC explained).
- Outgoing Caller ID numbers are verified for authorized end-user use, usually based on existing phone bills from other carriers.
- CDR alerts are configured to detect and alert on abnormal calling patterns, such as duration, and invalid Caller ID numbers.
- For clients using our **FAX Broadcast** app, outgoing Caller ID is verified for authorized client use and is hard coded on the Fax broadcast extension.
- Rate limiting / throttling and simultaneous call limits are also enabled to thwart excessive abuse on the broadcasting platform.

## **Vetting of New and Existing Customers (KYC, explained):**

As a fully managed Cloud PBX / VoIP provider, we maintain direct administrative control over the communication equipment used by our customers. We implement the following streamlined KYC protocol for our business end-users:

- **Identity & Physical Verification:** We require all customers to provide a valid Employer Identification Number (EIN) and a physical business address. We manually verify the business's active status via the relevant Secretary of State registry and confirm the physical storefront or office location through public records (e.g., Google Maps).
- **Provisioning Control:** Because we host and manage the customer's PBX infrastructure, we directly control and verify all outbound Caller ID settings. We do not permit customers to self-provision or "spoof" numbers; all numbers are assigned by us or verified via a Letter of Authorization (LOA) before being active on our platform.
- **Direct Use-Case Review:** We onboard customers only after a manual review of their intended business use. We do not provide service to high-volume dialers or telemarketing firms. Our service is exclusively for standard commercial business operations.
- **Contractual Enforcement:** All service agreements include 'Zero Tolerance' clauses for illegal robocalling. We commit to responding to all Industry Traceback Group (ITG) requests within 24 hours, and our direct control over the Cloud PBX allows us to immediately suspend any specific user or trunk identified as a source of illegal traffic.