aurigin.ai

Reduced KYC fraud

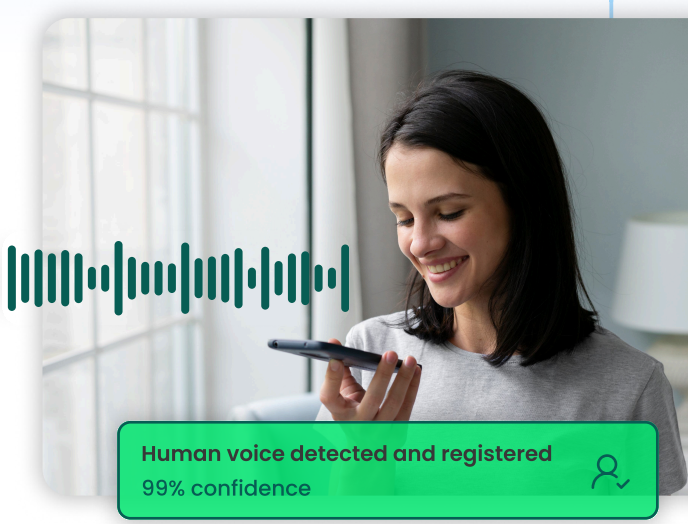
Blocking synthetic identities with real-time voice liveness detection

Understanding the threat

Fraudsters use **fake documents and deepfake videos** to slip through remote KYC. Once an account is opened under a false identity, it becomes **a mule account for fraud**. **Voice liveness checks block these synthetic profiles** at onboarding, while **registering a verified voiceprint securing all future authentication**.

In 2024, an Indonesian bank uncovered over 1,100 deepfake attempts to bypass its digital KYC loan process using AI-generated face swaps, fuelling deepfake fraud losses there to US$138.5 million over just three months.

Source: Forbes



Key challenges

- AI-generated documents and videos easily **bypass today's identity checks**
- Regulators expect stronger **proof of who is really behind the device**
- Identity uncertainty **slows onboarding and increases manual reviews**
- **Disconnected KYC, fraud, and call-center teams** miss synthetic identities later on

30% of fraud is found at account onboarding

4x more fraud in digital vs in-person onboardings

10x cheaper to run digital KYC processes

Solution

Aurigin.ai makes **remote onboarding secure again** by detecting deepfakes in real time, **verifying real customers with voice liveness,** and creating a trusted voiceprint for **seamless future authentication**.

- **Strong assurance:** real-time voice liveness checks for higher first-time right rates
- **Unified identity:** voiceprint reused across KYC, call centers, and TAN resets
- **Frictionless:** automatic voiceprint enrolment to enable future authentication
- **Flexible deployment:** API, or on-premise for full data control and privacy

98% accuracy | **40+ languages** | **<50ms latency**

EY swisscom 1291 GROUP venturelab VERIFYLABS.AI TRUSTED INFORMATION ALLIANCE

Aurigin.ai AG

info@aurigin.ai

www.aurigin.ai