12 Trends Reshaping Identity Verification in 2026

Q&A session

Please note that the questions have not been edited: they appear exactly as they did in the chat.

Question 1

With deepfake tools becoming so cheap and accessible, how do we realistically keep ahead of attackers? do we need new types of liveness or behavioral checks too?

Answer

With deepfakes getting cheaper and more convincing, traditional liveness alone isn’t enough anymore. The way to stay ahead is to shift from what it looks like to where it came from.

That means combining: provenance checks like device attestation and capture-source verification, strong server-side liveness instead of simple blink tests, and behavioral signals that AI can’t easily fake, like micro-movements and timing patterns.

No single test beats deepfakes but a layered approach, especially provenance + behavior + liveness together, keeps attackers from getting in.

Question 2

We are relying on existing technology to protect against deepfake fraud in video conferencing. Is that not adequate?

Answer

It's adequate but nowadays it's not enough. You need to think about combining different approaches to be sure that you keep attackers from getting in your system and protect you well.

Question 3

Banks are very slow to adopt. Which industries will be the fastest to adopt anti deepfake fraud technology? Big tech like Microsoft meta and Google for their conferencing tools - Teams Gmeet Zoom etc?

Answer

Yes, traditional banks are often slower to adapt, but that's partly because they still have branches and in-person services where IDV can be done for high-value transactions. In contrast, neobanks and online-first fintechs rely entirely on technology, which makes them faster adopters by necessity.

So, I'd say fintechs and neobanks are leaders when it comes to adopting new fraud detection technologies, including those targeting deepfakes.

Big Tech also adopts quickly, but for different reasons — they often develop these technologies themselves and have the ideal environments to test them. However, the direct risks for them aren't always as high as in financial organizations.

That's why I believe fintechs and neobanks will remain the fastest to implement advanced tools for combating deepfake fraud.

Question 4

Do you think reusable identity will actually reduce onboarding friction in regulated banking, or will liability concerns make adoption impossible?

Answer

It will reduce friction but only when governance is clear. Banks need legal clarity on liability: who is responsible when a reused identity fails?

We expect early adoption in:cross-bank KYC sharing networks consortium-managed identity wallets fintech–bank partnerships where trust anchors are established.

Banks won’t outsource risk but they will reuse verified attributes behind the scenes once standards mature.

Question 5

Marketplaces depend on verifying ordinary users quickly and cheaply. How do we handle age checks, identity checks, and fraud without creating too much friction?

Answer

E-commerce, marketplaces can really benefit from risk-based orchestration:

- low-risk users -> light verification
- high-risk behaviors -> escalate gradually
- repeat users -> reusable credentials

Privacy-preserving age verification, device intelligence, and reusable ID attributes let platforms verify responsibly without creating unnecessary drop-offs.

Thank you!

kate.johnson@regulaforensics.com

Regula

Decades of Forensics for Seamless Identity Verification.
Bringing together 33 years of experience in forensics, border control and business, to create industry standards to trust and follow.