Regula

The New Shape of Identity Threats

From AI-Driven Fraud to Machine Actors

Regula Global Research Report | 2026

Table of Contents

“

Identity verification was designed for a world where every interaction involved a real person. That assumption no longer holds. Today, organizations are not only verifying identities — they are determining whether an interaction itself is genuine, and whether the actor behind it is human or machine.

This report helps decision-makers understand how identity threats are evolving, where visibility breaks down, and what it takes to maintain trust in systems increasingly exposed to AI-driven activity.

Henry Patishman,
Executive VP of Identity Verification solutions,
Regula

Methodology

- 850 decision-makers in fraud detection and financial crime

- 7 markets:

UK

US

UAE

Germany

Mexico

Brazil

Singapore

- Industries include:
  - Banking
  - Government
  - Financial Services
  - Crypto
  - Telecommunications
  - Gaming/Gambling

- Results are accurate to ±3.4% at 95% confidence

- Fieldwork conducted by Sapio Research, March 2026

Regula

Key Findings

98% of organizations are concerned about identity-related threats — risk is now universal across sectors.

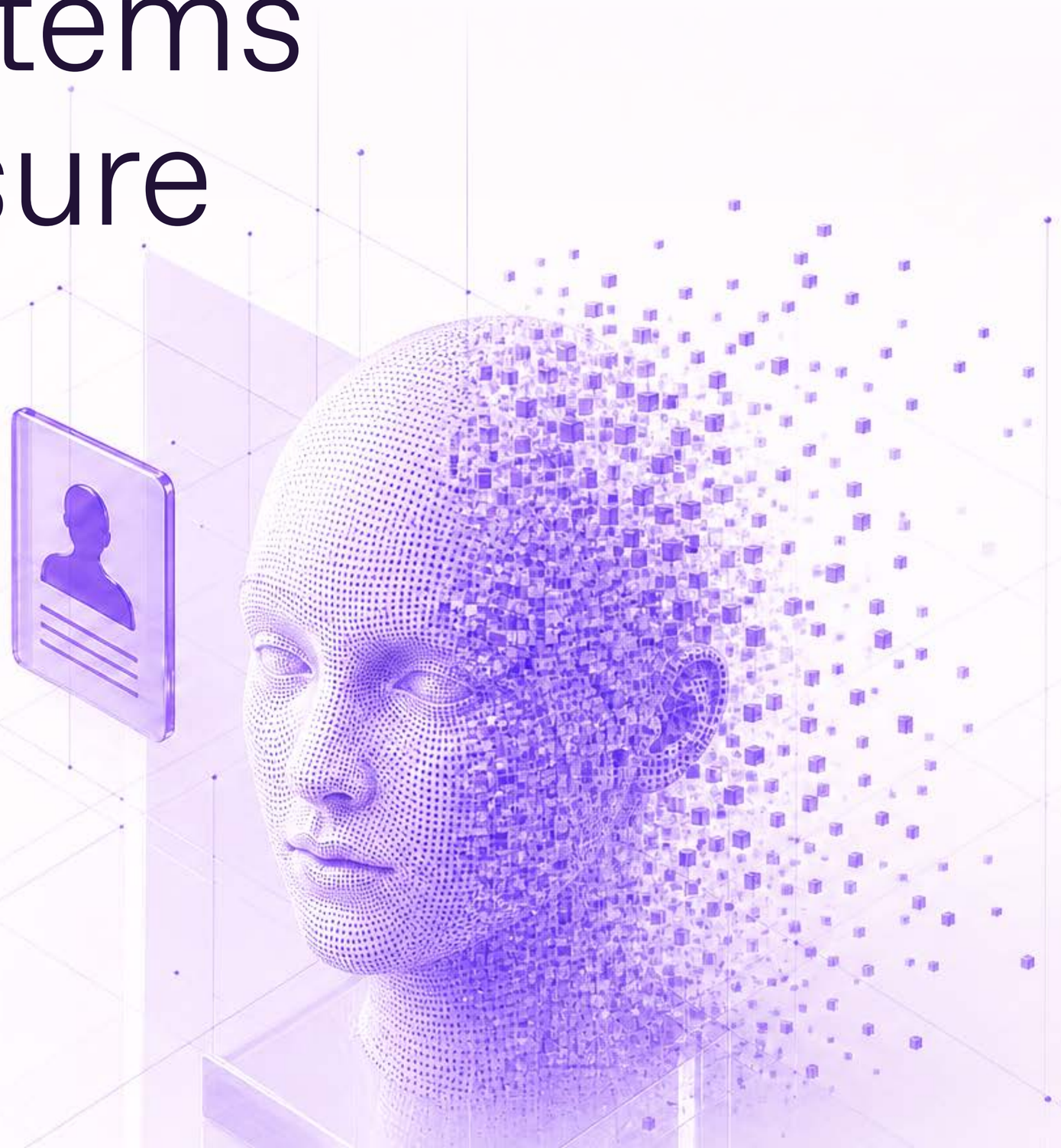
87% report AI-assisted or automated actors already attempting to pass their identity processes in the past 12 months.

69% say AI-assisted tools are common in their identity flows — but many lack visibility into how they're actually being used.

35% flag deepfake or AI-generated impersonation as a major concern, putting it near parity with document fraud.

26% already cite AI agents acting on behalf of users as a threat — a signal that machine-operated identity is moving into the mainstream.

The Shift: Identity Systems Under Pressure



Identity Threat Landscape Is Changing

Identity verification was built to confirm that a real person is behind a transaction, account opening, or access request. That model is under pressure.

Organizations must now answer three questions at once: Is this interaction genuine? Is the actor human, a bot, or AI-assisted? And can the identity signals — documents, selfies, voice, behavior — actually be trusted?

The data shows that automated and AI-assisted actors are already inside live identity flows — and most organizations are still catching up.

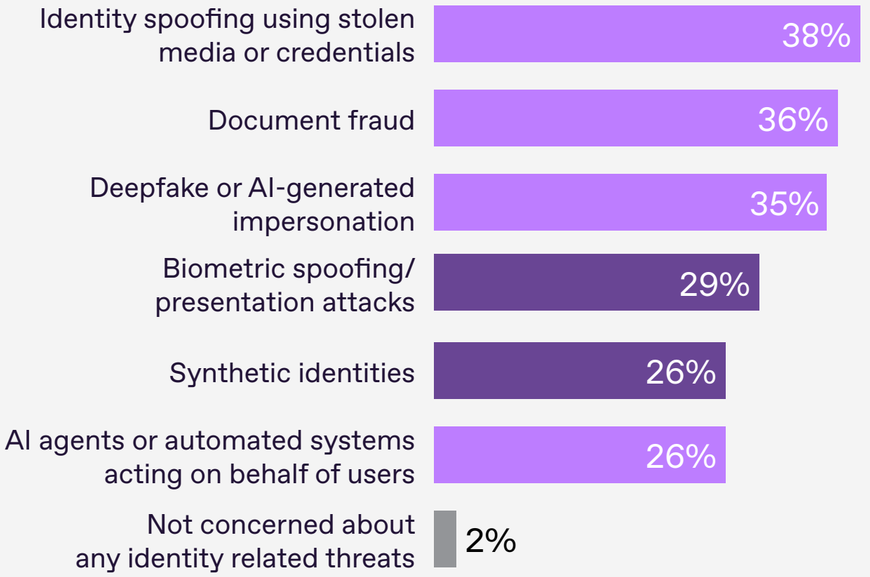
Identity Fraud Risk Is Now Nearly Universal

98%

of organizations are concerned about identity-related threats.

Identity fraud is no longer a banking problem. Telecoms, government services, gaming platforms, and financial services are all exposed.

Every sector is in the line of fire. What separates them is how ready they are when attacks hit.



Ways attackers attempt to pass identity checks: top concern

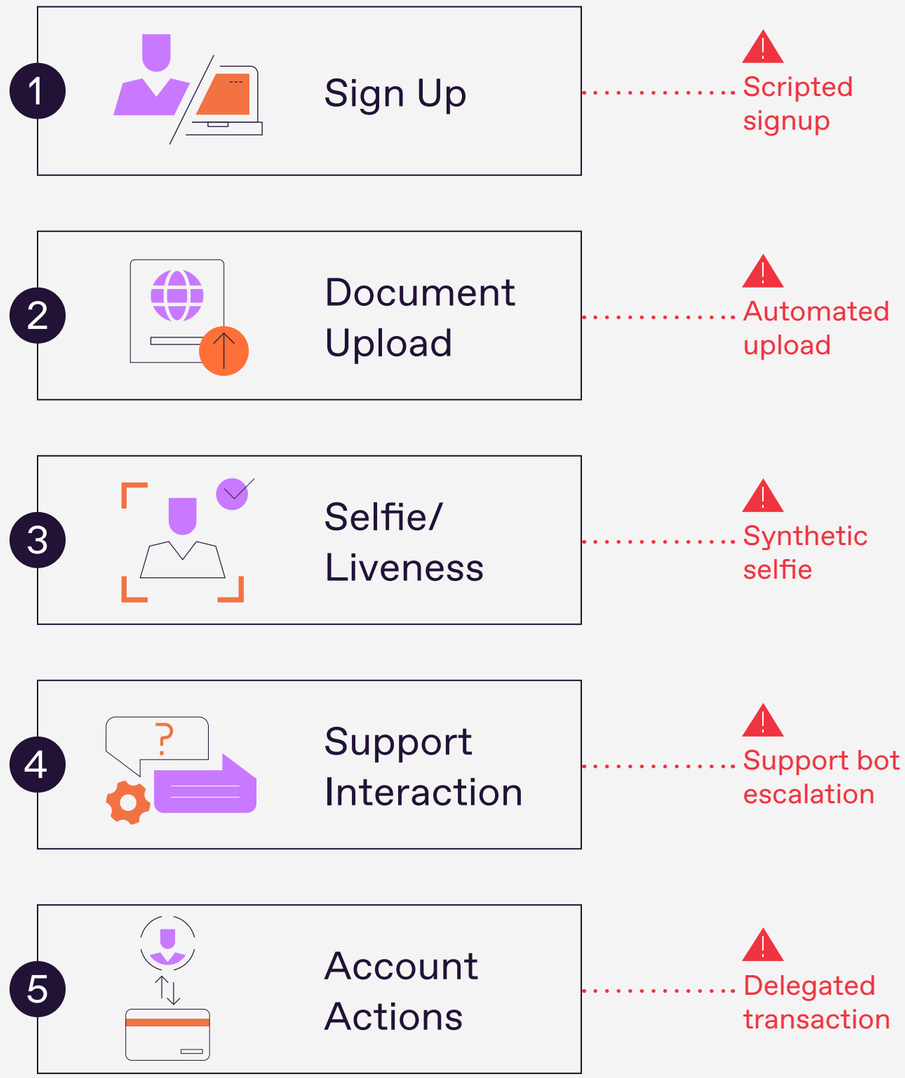
A New Threat Appears: AI Agents as Users

26%

of organizations already cite AI agents acting on behalf of users as a concern.

The top three threats show deepfake impersonation is now viewed almost on par with document fraud and identity spoofing. But another signal stands out: AI bots that behave like customers — moving through onboarding, login, and transaction flows built for people.

1 in 4 organizations already see it. The rest may not yet know it's there.



Customer journey with bot intrusion points

AI agents may automate onboarding, support interactions, and delegated account actions while appearing legitimate.

Regula

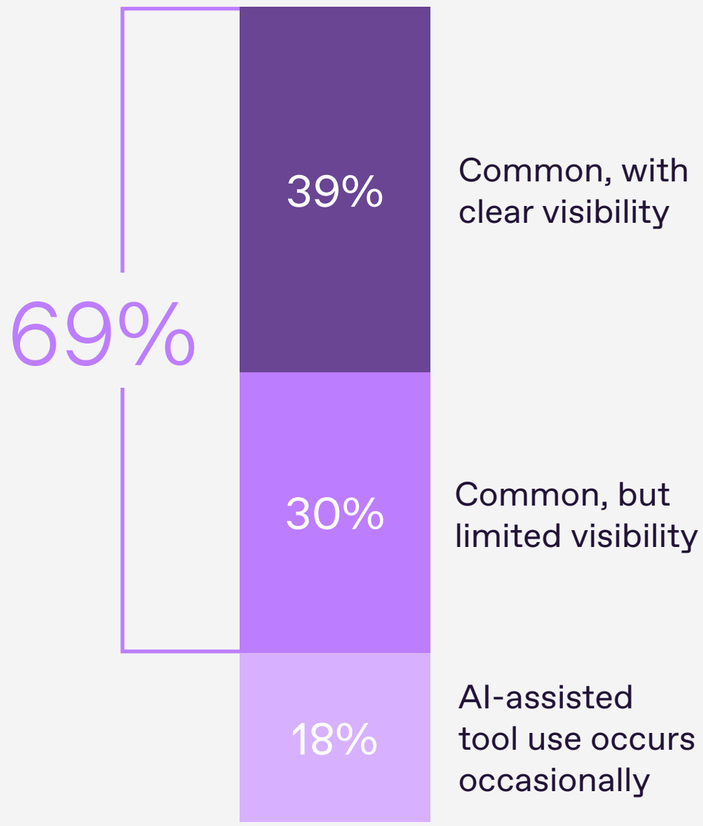
The Visibility Gap

AI Use Is Common, But Visibility Is Uneven

69%

say AI-assisted tools are already common in their identity or authentication flows.

Most organizations know AI is in the room. Fewer know exactly where it is or what it’s doing. And systems can’t control what they can’t detect.



Visibility into AI use

AI-bots Are Already Testing Your Systems

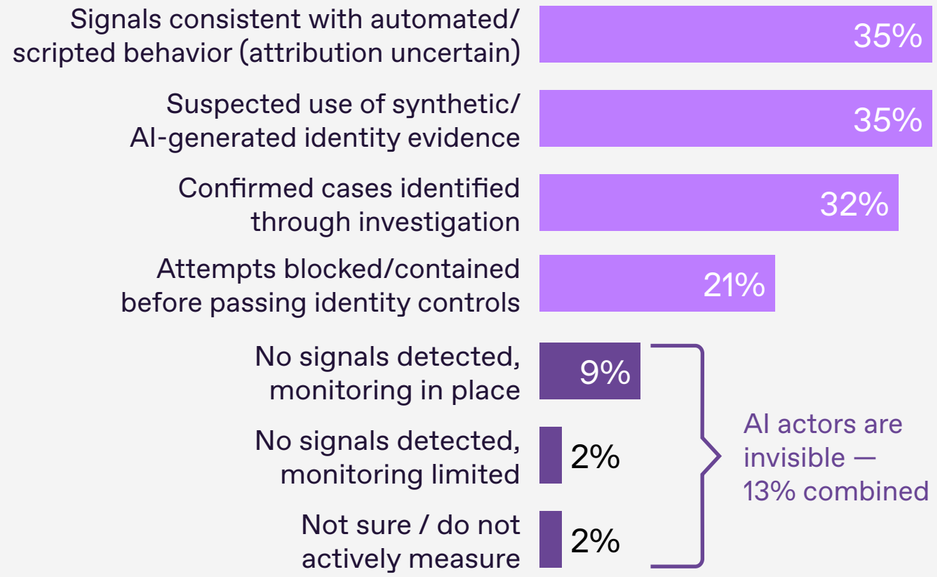
87%

of organizations report AI-assisted or automated actors attempting to interact with their identity processes in the past 12 months.

AI-assisted and automated actors are already interacting with live onboarding, authentication, and account access processes.

Some of it is fraud. Some are legitimate automation. Much of it sits in the middle — scripted behavior and synthetic evidence that obscures who's really behind the screen.

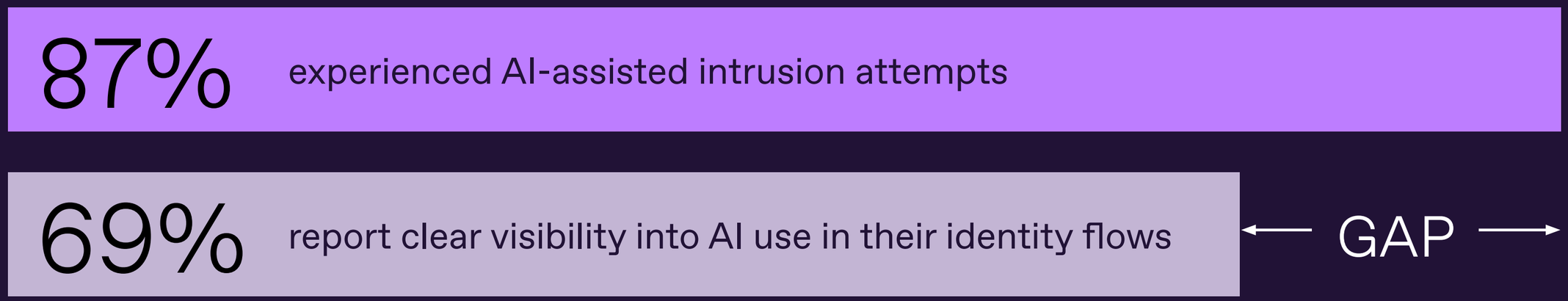
That ambiguity is the problem. When intent is unclear and attribution is hard, the true scale of exposure rarely shows up in incident reports.



Experience with AI-assisted or automated actors

Regula

The Blind Spot



Taken together, these findings point to a deeper issue.

AI-driven activity is already present — but not fully understood. Organizations are detecting signals they cannot reliably track, attribute, or explain.

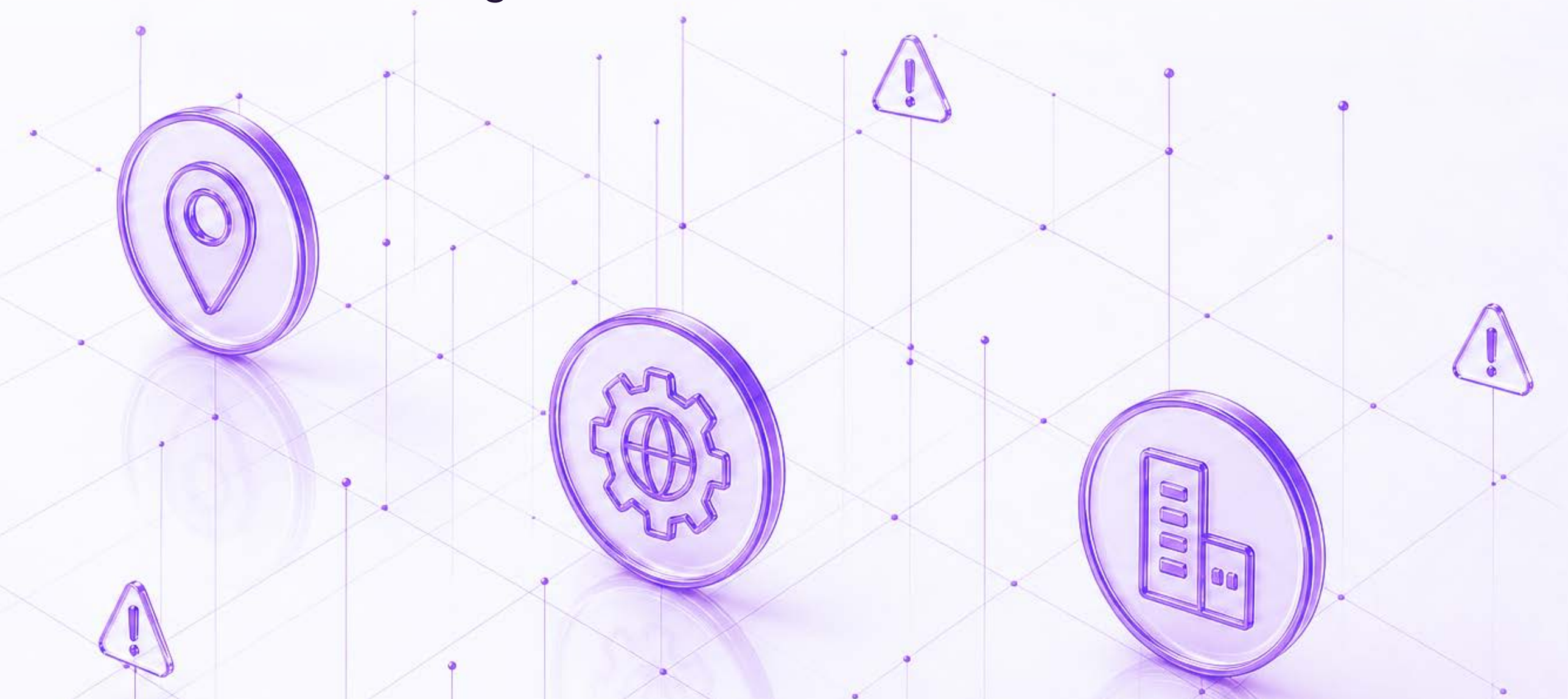
Exposure is high.

Visibility is partial.

Understanding is incomplete.

Core Threats Breakdown

How identity threats vary across countries, industries, and organizations



Identity Spoofing: The Most Common Threat

Identity spoofing — the reuse of stolen photos, videos, or credentials — ranks as the #1 identity threat globally. The gap with document fraud and deepfakes is minimal, placing all three in the same risk tier.

By country

Brazil stands out at **45%**, the highest of any market. The US (**41%**) and Mexico (**40%**) also report elevated concern.

Germany sits lowest at **32%**, continuing a pattern of lower concern across threat categories.

Some markets are seeing more direct exposure to credential-based attacks. Others may rely more on existing controls — or trust them more.

By industry

Gaming/Gambling leads at **42%**, where account takeover and credential reuse are persistent risks. Government (**40%**), Financial Services and Telecom (**39%**) follow closely. Crypto ranks lowest at **35%** — a reversal from its top position on document fraud.

Threat perception shifts across the user journey. Crypto firms focus heavily on onboarding risk (fake identities), while sectors with ongoing account access see more pressure from credential reuse.

By company size

Concern peaks among 5,000–9,999 employee organizations at **43%** — higher than both smaller firms and the largest enterprises.

Risk may concentrate in organizations which often handle large volumes of active users without the layered defenses of global enterprises.

Document Fraud Hits Differently Across the Board

Counterfeit, altered, or stolen IDs remain the #2 identity threat globally, on par with deepfakes.

By country

Mexico leads at **38%**, followed by Brazil, UAE, and the UK (all **37%**). Germany stands out at **29%**, the lowest of any market.

Exposure is not evenly distributed. Regional differences in document standards, onboarding practices, and fraud patterns likely shape how visible this threat becomes.

By industry

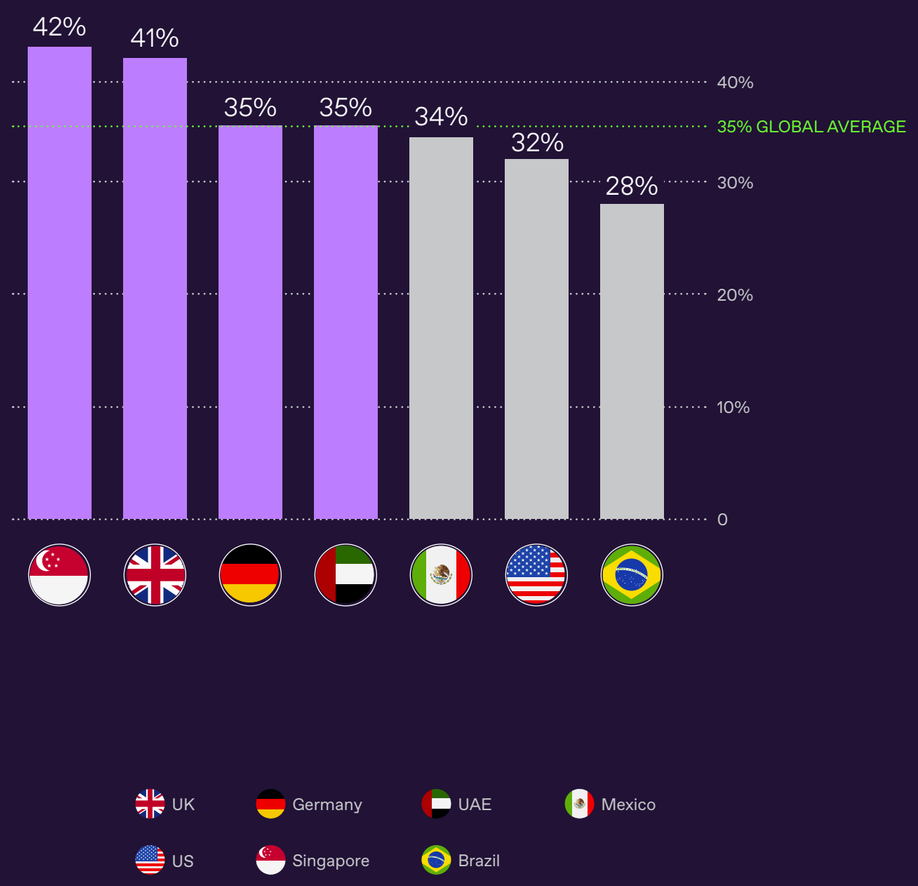
Crypto leads at **44%**, followed closely by Government at **43%** — an unusual pairing. Banks (**34%**) and Financial Services (**32%**) sit noticeably lower.

Sectors built around document-heavy processes or under intense onboarding pressure feel this risk most directly. More regulated incumbents may feel better covered by existing controls — whether that reflects reality or confidence is less clear.

By company size

Concern increases with scale: **250–499 employees** — 29% **10,000+ employees** — 41%.

Larger organizations present larger attack surfaces — more customers, more channels, more documents to verify. Scale increases both exposure and visibility.



Deepfakes: Country Perspective

Deepfakes are no longer an emerging threat — AI-generated faces and videos used to mimic real users in onboarding and authentication now rank among the top identity concerns globally, just behind identity spoofing.

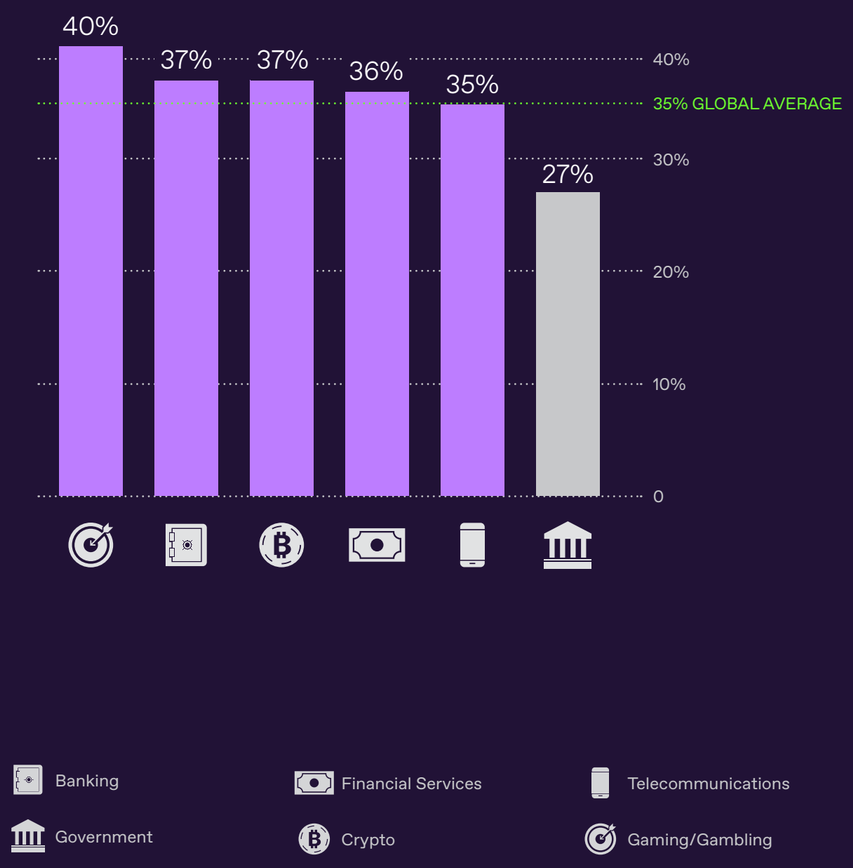
Singapore and UK lead mature fraud ecosystems, high-volume digital onboarding, and regulatory pressure that forced organizations to build vocabulary around synthetic media early.

UAE lands at the global average notable given it leads on AI agents. UAE organizations appear more alert to agent-based risk than to media-based impersonation.

USA falls below the global average possibly absorbing deepfake risk under adjacent labels like synthetic identity or social engineering. Familiarity may be breeding normalization.

Brazil sits lowest consistent with a broader pattern of underestimating AI-driven identity risk.

Deepfakes: Concern by Industry



Deepfakes: Industry Perspective

Unlike AI agents, deepfakes show real differentiation across sectors — the widest spread of any identity threat. Some industries have operationalized this risk. Others haven't started.

Gaming/Gambling leads high-velocity onboarding and video-based interactions make synthetic impersonation an active, tested attack vector, not a theoretical one.

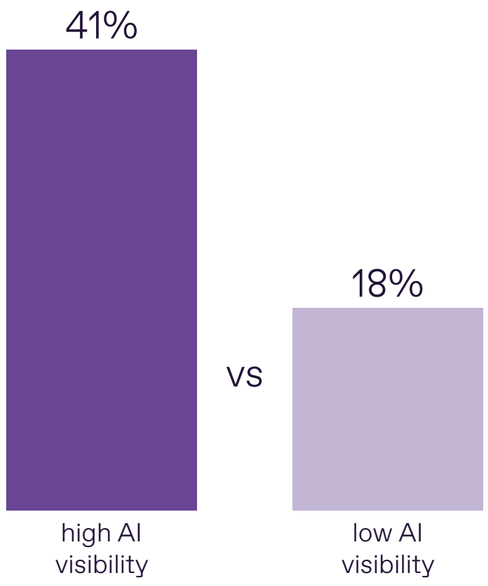
Banking and Crypto are tied above average both have clear line-of-sight to deepfake-enabled account takeover, push payment fraud, and onboarding bypass.

Government sits lowest same as it does on AI agents. Where in-person and document-based verification still dominates, synthetic media doesn't yet feel like a front-line threat.

Deepfakes: What else the data reveals

AWARENESS CLUSTER

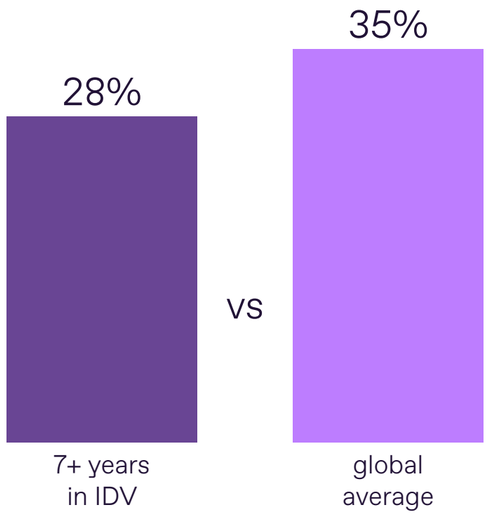
AI threat recognition rises together.



Organizations with stronger visibility into AI-assisted activity are over 2x more likely to recognize deepfakes as a major threat.

EXPERIENCE ≠ ADAPTATION

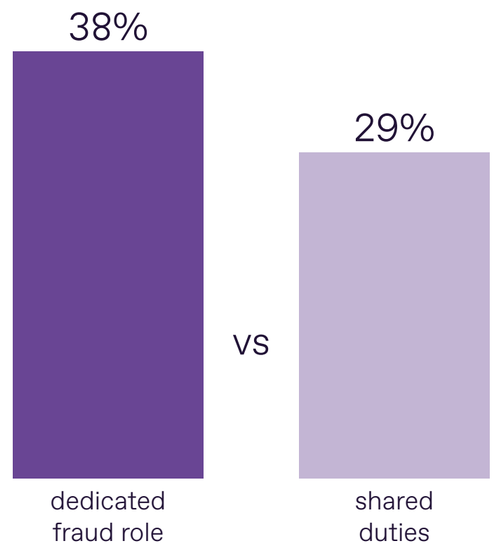
Tenure builds confidence. It doesn't always update it.



Veterans sit 7 points below global average. Confidence doesn't always update.

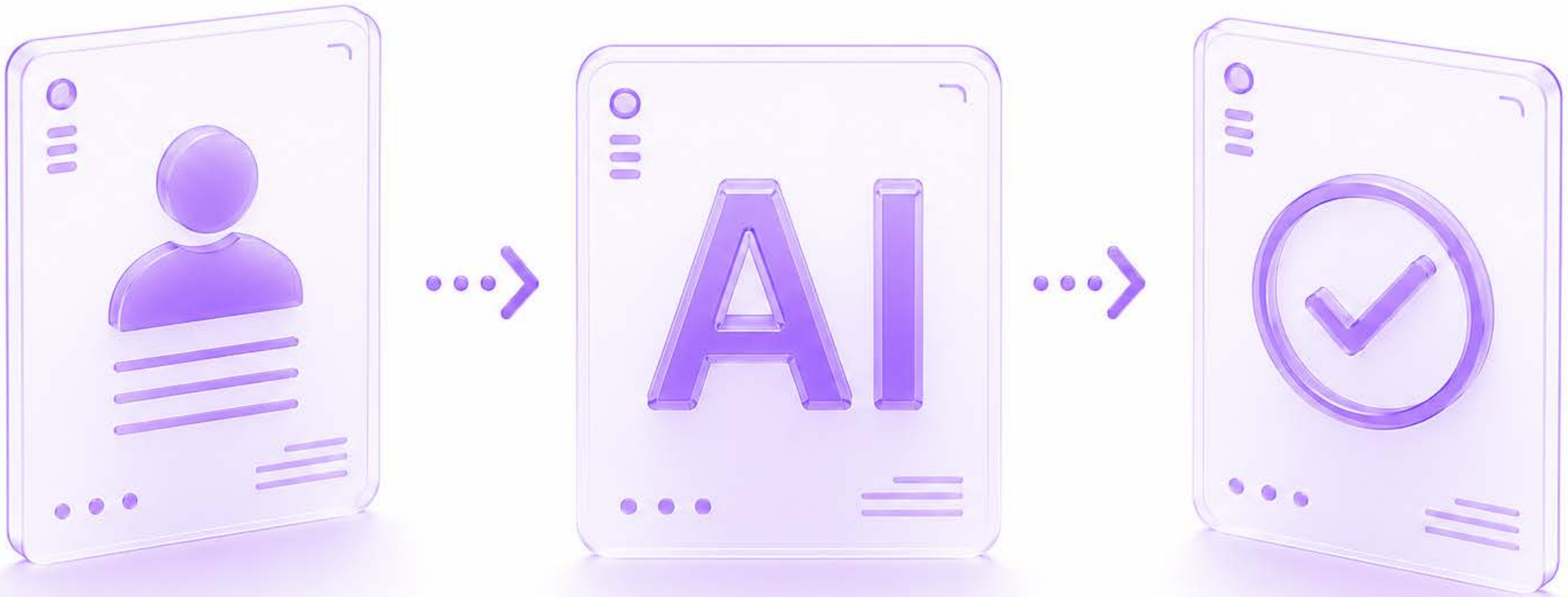
OWNERSHIP MATTERS

Diffused ownership diffuses risk perception.

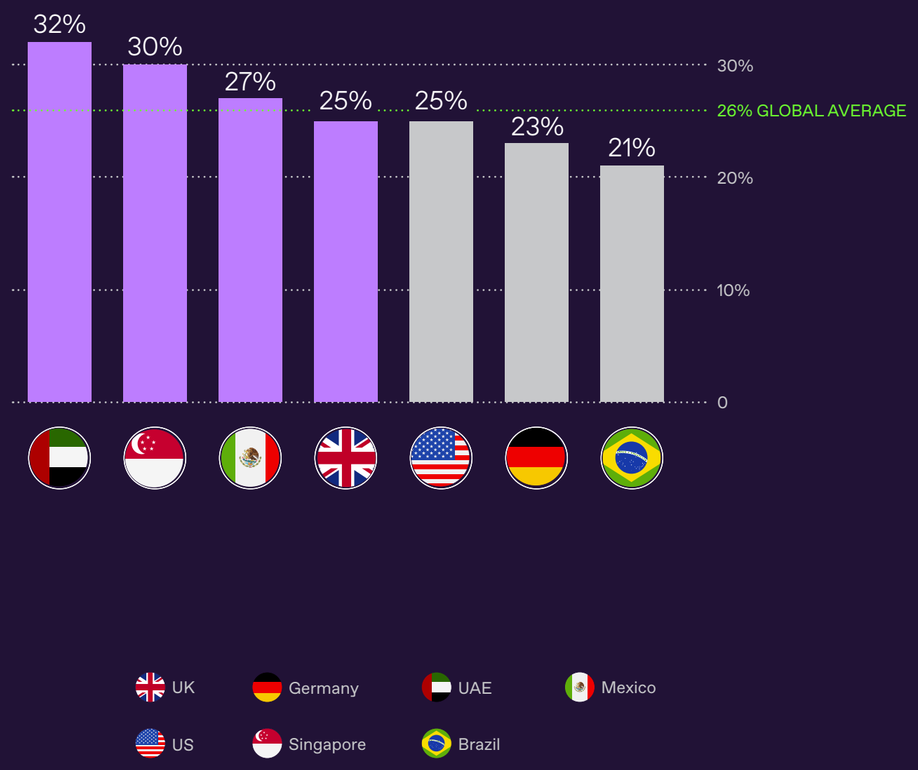


9-point gap between dedicated and shared fraud responsibility.

AI Agents as a New Risk Layer



AI Agents Acting as Users: Concern by Country



AI Agents Exposure: Country Perspective

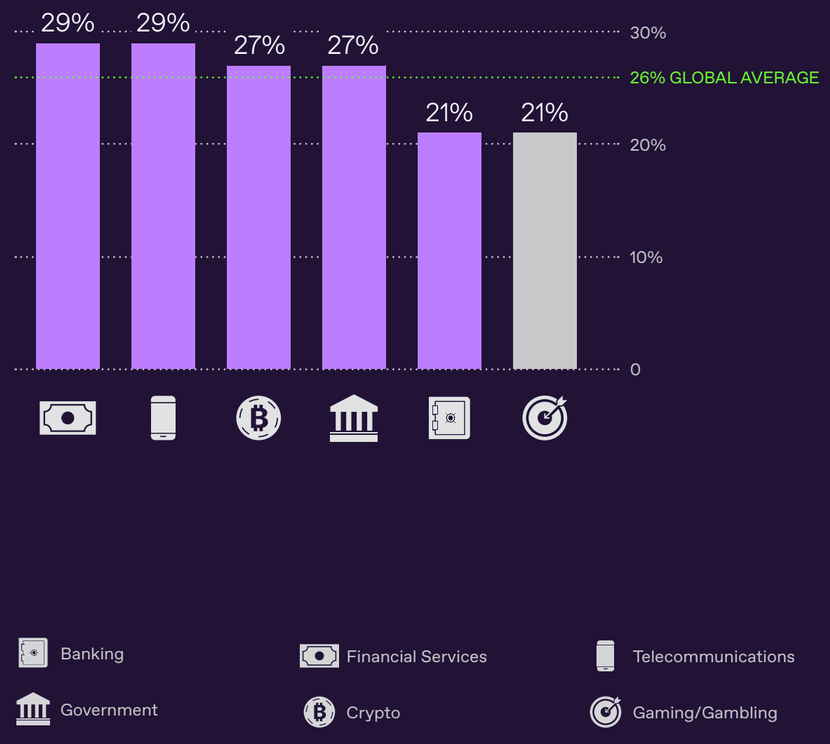
AI agents remain a blurry threat category. No country is alarmed. AI agents remain the least urgent identity threat across all markets surveyed.

Singapore and UK lead digital-first markets tend to encounter new identity risks first, especially where onboarding is heavily automated.

UAE lands at the global average despite being the most attack-aware country in the survey. Organizations may be seeing AI-agent activity but not yet naming it as a strategic threat.

Brazil sits lowest consistent with a broader pattern of underestimating AI-driven risk.

AI Agents Acting as Users: Concern by Industry



AI Agents Exposure: Industry Perspective

AI agents are recognized but not yet operationalized. Concern is flat across all sectors — the narrowest spread of any identity threat: just 8 percentage points from highest to lowest.

No sector has made this threat its own — it remains abstract and unassigned across the board.

Government and Crypto report identical concern levels despite completely different risk profiles — suggesting AI agents don't fit neatly into existing sector threat models.

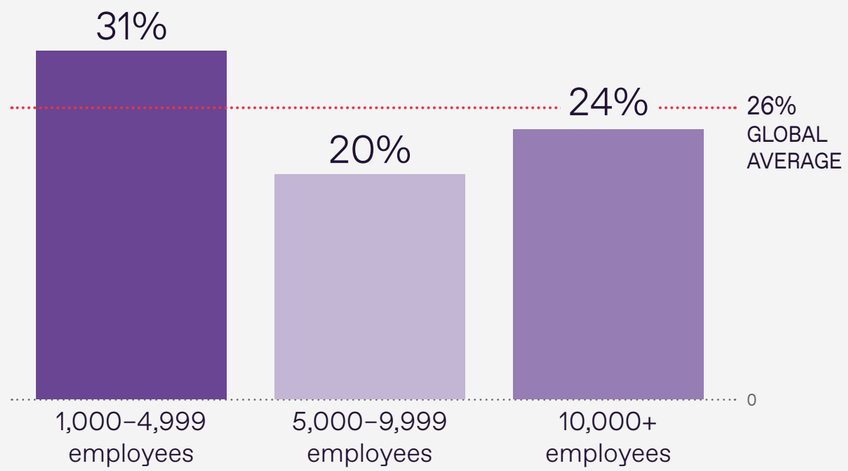
AI Agents Exposure: Company Size Perspective

Size shapes exposure — but not in a straight line.

Mid-market organizations (1,000–4,999 employees)
Highest concern, above global average. Large enough for high-volume digital onboarding, but not yet equipped with enterprise-grade detection. AI-agent activity hits harder when you can see it but can't fully contain it. That can make AI-agent activity more visible and more disruptive.

Large enterprises (5,000–9,999 employees)
Concern drops sharply. Stronger tooling, centralized controls, dedicated risk teams. The threat hasn't gone away — the urgency has.

Very large (10,000+ employees)
Back near the global average. Scale buys better defenses, but also more channels, vendors, and regions to defend.



AI Agents Acting as Users: Concern by company size

Key Conclusions

1 **Every sector is exposed.** Identity fraud is no longer concentrated in high-risk verticals — it's universal.

2 **Identity spoofing** remains the most common attack — but it no longer defines the threat landscape on its own.

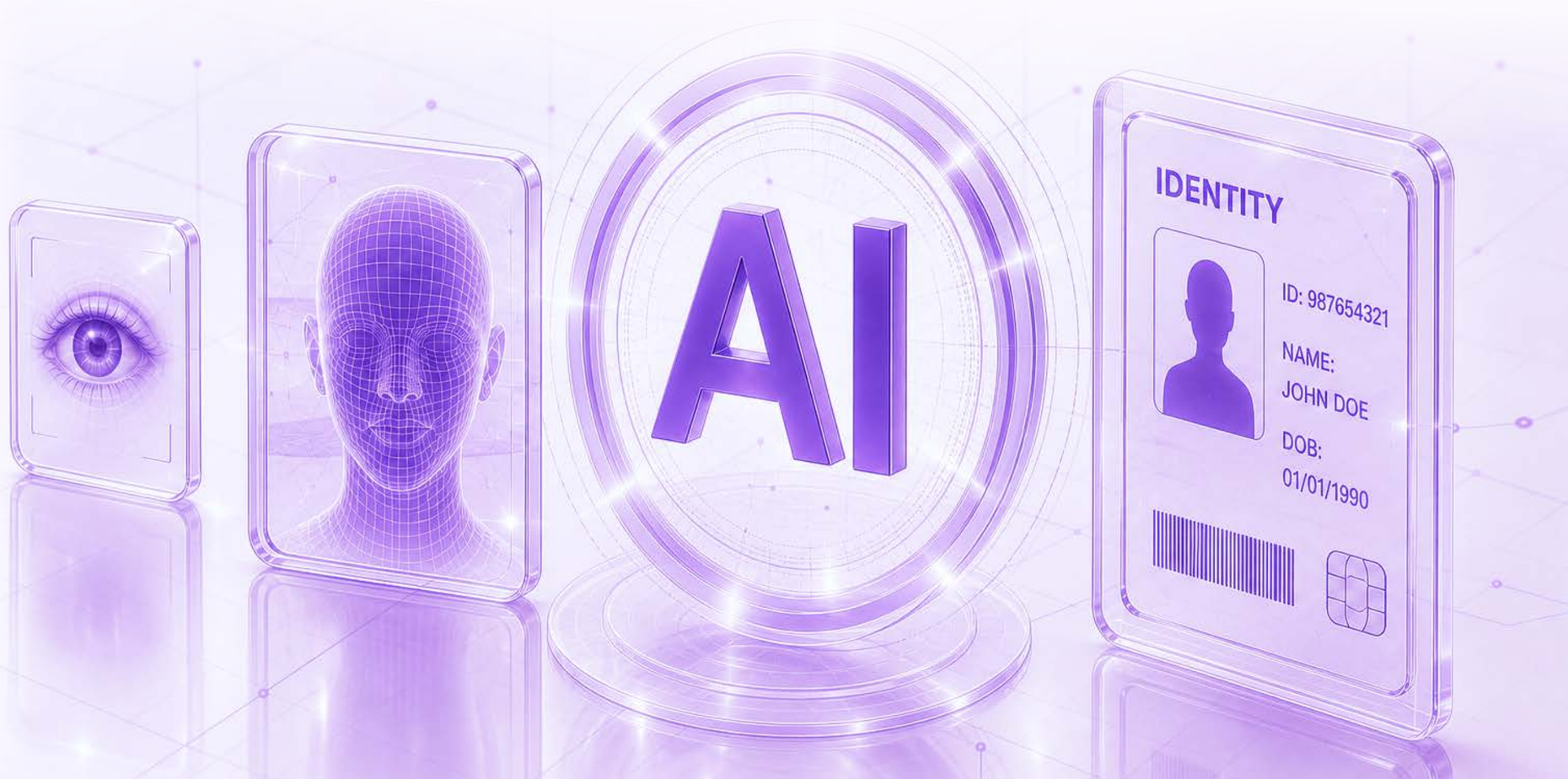
3 **Deepfakes went mainstream faster than expected** — a recent entrant to the identity threat landscape, now rivaling document fraud in perceived risk.

4 **AI bots are already inside the wire.** Automated and AI-assisted actors are actively moving through live identity flows.

5 **Visibility hasn't kept pace.** Most organizations know AI is present. Few can track, attribute, or act on it reliably.

6 **The highest exposure is where growth outran controls** — mid-market companies and fast-digitizing markets are feeling it most.

The next challenge
is software entering
systems that were built
to deal with people.



Regula

↗ Contact us: pr@regulaforensics.com
Learn more at regulaforensics.com