EINPRESSWIRE

Shufti Whitepaper Reveals How the Overlooked 1% Fraud Gap Fuels Industrial-Scale Crime

With deepfake losses up 1,740% in a year and synthetic IDs fueling $3.2B in fraud, Shufti Whitepaper shows why only accuracy claims aren't enough.

Shufti Whitepaper: The Critical 1%: Closing Systemic Gaps in Global Identity Verification

LONDON, UNITED KINGDOM, September 30, 2025 /EINPresswire.com/ -- Shufti, a leading global identity verification provider, has released a new whitepaper, The Critical 1%: Closing Systemic Gaps in Global Identity Verification, highlighting how the smallest gaps in verification frameworks are enabling industrial-scale fraud.

While many vendors cite 99% accuracy in identity verification, Shufti's research demonstrates that the remaining one percent is where the most damaging attacks occur, from deepfake impersonations and synthetic identities to cross-border document manipulation.

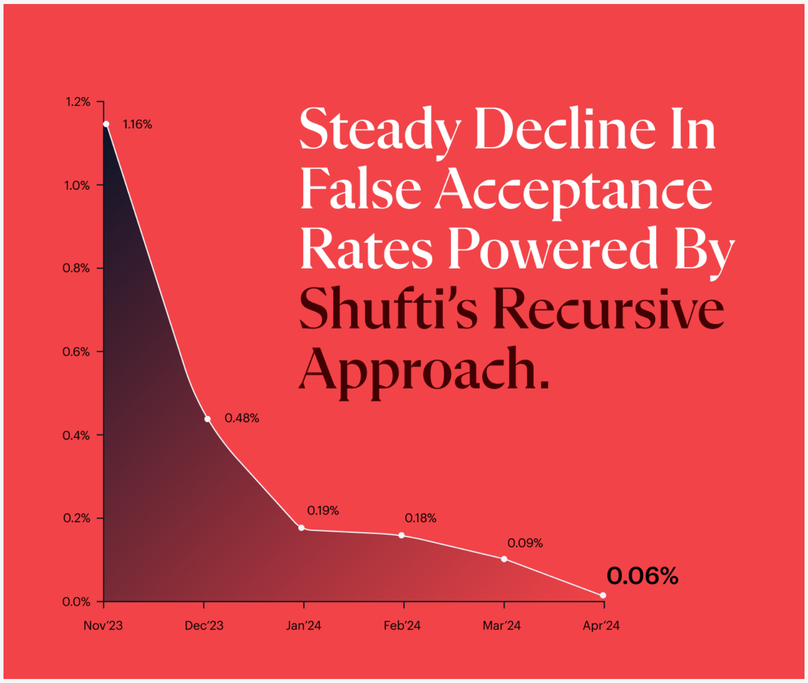
> Outsourced verification locks companies into someone else's limitations, slowing their ability to adapt to new fraud and regulatory challenges."
>
> *Shahid Hanif, Co-founder and CEO of Shufti*

The report traces fraud's evolution from forged IDs and stolen credentials to algorithmic manipulation powered by generative AI. Once opportunistic, fraud has now become industrialized, targeting fast-growth sectors like crypto, iGaming, fintech, and social commerce. AI. Deloitte forecasts AI-related fraud losses in the U.S. alone will rise from $12.3 billion in 2023 to $40 billion by 2027, growing at 32% annually.

Warnings from regulators add urgency. The FBI has highlighted escalating AI-enhanced phishing and social engineering attacks, while FinCEN's 2024 advisory flagged a surge in suspicious activity reports tied to synthetic identities and deepfake media. The cost of overlooking edge cases is already being measured in billions.

Real-world cases illustrate the urgency: a Hong Kong firm lost $25 million in a deepfake-enabled scam, while Deepfake-related incidents surged 1,740% in North America between 2022 and 2023.

Through the narrative lens of “Jack,” a composite fraudster, the report illustrates how organized networks exploit overlooked weaknesses.



Shufti Recursive Approach: False Acceptance Rate

Shufti’s research outlines:
-Birth registration gaps: 150 million children under five remain unregistered globally, offering a blueprint for synthetic IDs.
-Biometric blind spots: Error rates ranging from 5%–50% in facial recognition under different conditions give cover to AI-generated faces.
-Document authenticity gaps: Outdated and fragmented ID standards allow fraudsters to cross borders undetected.
-Synthetic identities: Now accounting for over 80% of all new-account fraud in the U.S., costing lenders billions annually

Industries prioritizing growth over assurance have emerged as the most exposed. In 2024, the FBI’s Internet Crime Complaint Center logged nearly 150,000 complaints linked to cryptocurrency fraud with reported losses of $9.3 billion, a 66% year-on-year increase.

Online gaming platforms recorded a 60% rise in fraud cases, while FTC data shows social-media-originated scams accounted for $1.9 billion in U.S. losses, with 70% of contacted users losing money.

“Fraud does not occur in the 99% that systems can measure — it thrives in the 1% that is ignored,” said Shahid Hanif, CEO of Shufti. “The most damaging attacks exploit non-standard IDs, biometric blind spots, and registration gaps. Criminals are evolving faster than legacy systems, and businesses cannot afford to leave that 1% unchecked.”

The whitepaper presents Shufti’s approach: treating verification as an ongoing defense, not a one-time check. Proprietary in-house technology integrates forensic document inspection, behavioral biometrics, device intelligence, OCR reads complex scripts, and intelligent escalation paths, including biometric re-verification and expert review.

This adaptive model has reduced false acceptance rates to as low as 0.63% in some sectors, while supporting verification across 240+ countries and territories, even in regions with weak documentation or complex scripts.. A recursive approach allows Shufti to analyze false declines and retrain models continuously, ensuring resilience against evolving threats.

Real-world applications demonstrate the value of this approach. In Japan, a coordinated fraud ring attempted to infiltrate a crypto exchange using multiple slightly altered IDs. Traditional verification systems failed, but Shufti's device fingerprinting and behavioral analysis linked the submissions to a single device, neutralizing the network.

In another case, a deepfake morphing attack against a forex platform was uncovered through forensic checks and retrospective audits, preventing losses that standard face-matching tools would have missed.

Outsourced verification locks companies into someone else's limitations," added Shahid Hanif, Co-founder and CEO of Shufti. "By owning our technology end-to-end, we control accuracy, speed, and coverage — from reading non-Latin scripts with custom OCR to exposing morphing attacks with forensic analysis. That's how Shufti keeps fraud under one percent while others are still catching up."

The whitepaper also challenges the industry's reliance on rigid compliance scripts. Instead, it calls for flexible, intent-aware frameworks that balance assurance with inclusivity, ensuring vulnerable or under-documented populations are not excluded while fraud is systematically reduced.

It emphasizes that verification systems must evolve in lockstep with fraud, shifting the focus from measuring accuracy to closing the systemic 1% gap.

The full whitepaper, The Critical 1%: Closing Systemic Gaps in Global Identity Verification, is available for download: https://shuftipro.com/one-percent/

About Shufti

Shufti is a global identity verification and fraud prevention company committed to keeping fraud below one percent. Its in-house technology covers more than 10,000 government-issued ID types across 240+ countries and territories, offering highly customizable solutions designed for regulatory assurance and fraud resilience.

Proprietary OCR handles complex scripts and non-standard formats, while forensic document analysis, biometric verification, device fingerprinting, behavioral intelligence, and expert review work in unison to detect sophisticated threats. Unlike off-the-shelf vendors, Shufti's recursive approach ensures every false decline and new fraud attempt informs ongoing improvements, strengthening defenses with each iteration.

This adaptability allows businesses to meet evolving compliance requirements, from GDPR and eIDAS 2.0 to FATF guidance, while protecting user trust and maintaining conversion rates.

Today, more than 2,000 clients worldwide, including banks, fintechs, gaming operators, e-commerce platforms, and social networks, rely on Shufti to secure the customer journey from onboarding to account recovery.

SOURCE: Shufti

Neliswa Mncube
Shufti
+44 1225 290329
email us here
Visit us on social media:
LinkedIn
Bluesky
Instagram
Facebook
YouTube
TikTok
X