Organised Fraud Rings Use Deepfakes and Reused Identities to Target Digital Businesses, Shufti Identity Fraud Report2026

Digital assets record the highest share of remote onboarding fraud at 22.49%, ahead of fintech at 18.36% and forex at 17.18% across eleven sectors.



LONDON, UNITED KINGDOM, September 9, 2026 /EINPresswire.com/ -- Shufti, a Glocal identity verification, KYC, AML, and full compliance lifecycle platform, today published the Identity Fraud Report 2026, its annual analysis of identity fraud during remote onboarding, drawn from its production verification data across eleven industries in the first half of 2026.

The report finds that deepfakes and AI-generated identity fraud are no longer limited to individual fraud attempts. Organised crime networks and coordinated fraud rings are also increasingly using forged identity documents, synthetic identities, shared devices and controlled digital infrastructure to bypass KYC checks, facilitate financial crime and operate across multiple jurisdictions.

> Deepfakes aren't just an individual fraudster's tool. Organised crime networks now use same AI-generated documents and identities across borders, reusing them via shared devices and digital systems."
>
> *Faryam Asif, Chief Technology Officer at Shufti*

Among linked fraudulent verification attempts, 65.68% of attribute matches traced back to forged identity documents, showing how coordinated fraud rings repeatedly recycle manipulated identity assets across institutions.

One Forged Document Is What Ties A Ring Together:
Shufti finds that generative AI has reduced the cost of producing a convincing fake identity, so one operator can recycle a single document, face, or device across many verification attempts. A

document declined as forged at one institution is not spent. It returns under another name, on another device, and is submitted again elsewhere, shifting exposure to repetition rather than any single submission.

-Matches between separate fraudulent attempts break down as reused fraudulent documents at 65.68%, shared controlled IP addresses at 17.67%, and shared devices at 16.64%. Document reuse is the strongest matching signal, because people legitimately share networks and devices.
-The largest connected cluster observed linked 70 identities across 13 devices, with a single device anchoring 16 verification events.

"Deepfakes are no longer just an individual fraudster's tool. Organised crime networks are using the same AI-generated documents and identities across borders, reusing them through shared devices and infrastructure. A document authenticity check has no memory. It tests an artefact against a template, not against the attempts that came before it, so a ring clears onboarding one request at a time," said Faryam Asif, CTO at Shufti.

Organised Fraud Rings Operate Across Borders:
The report says 2.01% of network fraud spanned more than one country, highlighting how AI-enabled identity fraud increasingly overlaps with cross-border financial crime and money laundering.

Within those cross-border groups, the typical interval between activity in one country and the next was 9 minutes 33 seconds, and the fastest observed was 38 seconds, a timing pattern inconsistent with physical movement between jurisdictions.

Once a ring crosses a border, no single institution or supervisor sees the whole of it, and an identity verification gap becomes an AML exposure downstream.

Digital Assets Records the Highest Share of Remote Onboarding Fraud:
Identity fraud exposure varied more than fivefold across the eleven industries measured, tracking the sectors whose remote onboarding volume is highest rather than those under closest supervision. It includes:

-Digital Assets recorded the highest exposure at 22.49% of all verification requests, followed by fintech at 18.36%, forex at 17.18%, lending and investment at 17.08%, and iGaming at 12.45%.
-Deepfake document fraud accounted for 80.10% of AI-enabled fraud, the dominant attack instrument by a wide margin, ahead of synthetic identities at 12.31%, injected videos at 4.01%, and face swaps at 3.58%.
-Altered documents led the detection rate by attack instrument in nine of the eleven industries measured. Banking recorded a fraud rate of 4.24%, where replay and screenshot attacks remained the leading attack vectors.

The report cautions that a sector rate reflects attempted attacks and the controls applied to them together, so exposure describes attack pressure rather than relative security posture.

Additional Findings From The Shufti Identity Fraud Report 2026 Include:
-Attacks divide into presentation attacks, where a manipulated artefact reaches the system through the camera, and injection attacks, where images or video streams are inserted directly into the verification pipeline through virtual cameras, emulators, or frame injection.
-Because an injection attack never reaches a physical sensor, it is a software integrity problem as much as a document one, and controls built only for presentation attacks do not register it.
-Multi-identity account abuse concentrates in iGaming, forex and lending, where one operator can farm sign-up bonuses, evade self-exclusion or hold opposing positions across accounts that appear unrelated.
-The report closes with a four-part framework covering multi-layered verification, identity network intelligence, behavioural and continuous verification, and risk-based decisioning, alongside an evaluation checklist that compliance and product teams can put to any identity verification provider.

Methodology
The Shufti Identity Fraud Report 2026 draws on identity verification checks Shufti processed for its customers between January and June 2026 across eleven industries. For each industry, the identity fraud rate is calculated as confirmed fraudulent verification attempts as a share of the industry's total verification requests during the reporting period. Each industry figure is confirmed fraud as a share of that industry's own verification requests. To test whether separate attempts belong to one ring, the analysis takes attempts where the document was confirmed fraudulent, manipulated, or AI-generated, then looks for others sharing the same document, device, or IP address. No fraudulent attempt has been attributed to a named individual or organisation.

Download the full Shufti Identity Fraud Report 2026 here, or contact the Shufti team to learn how identity verification, deepfake detection, and fraud ring detection can help protect your business from identity fraud threats.

https://shuftipro.com/resources/whitepapers-reports/identity-fraud-report-2026/?utm_source=EINPresswire&utm_medium=PressRelease&utm_campaign=IdentityFraudReport

About Shufti
Shufti is a Glocal identity verification and full compliance lifecycle platform that combines document verification, liveness detection, biometric authentication, and deepfake detection with fraud ring detection and identity network intelligence inside one risk-based decision, so regulated businesses can meet KYC and AML obligations, onboard genuine customers quickly, and identify the coordinated networks operating behind remote onboarding.

Follow Shufti on LinkedIn and YouTube for the latest news and updates.

SOURCE SHUFTI

Aroosa Virk
Shufti
partnership@shuftipro.com
Visit us on social media:
LinkedIn
Bluesky
Instagram
Facebook
YouTube
TikTok
X

This press release can be viewed online at: https://www.einpresswire.com/article/940577077

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.