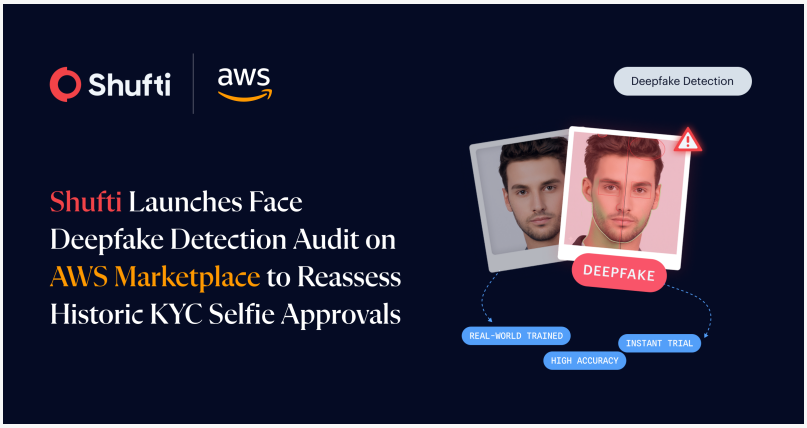
Shufti Launches Face Deepfake Detection Audit on AWS Marketplace to Reassess Historic KYC Selfie Approvals

Shufti Deepfake Detection Audit on AWS Marketplace helps institutions identify AI-generated or manipulated faces hidden in historic KYC records.



LONDON, UNITED KINGDOM, January 28, 2026 /EINPresswire.com/ -- Shufti, the global identity verification and fraud prevention provider, has launched Shufti Face Deepfake Detection on AWS Marketplace, enabling regulated organisations to reassess historic KYC selfie images for AI-generated faces and face swaps that were not detected at the time of onboarding.

As deepfake and face manipulation techniques continue to advance, many earlier verification decisions were made under legacy KYC conditions that did not fully account for today's generative methods.

> Shufti face deepfake detection audit on AWS Marketplace enables teams to review historic approvals for deepfake and face-swap indicators within their own AWS environment with evidence-based outcomes."
>
> *Shahid Hanif, Chief Executive Officer of Shufti*

In some cases, synthetic or manipulated facial images were able to pass existing controls and become embedded in approved customer profiles from 2020-2025. These risks may remain undetected until they surface through fraud incidents, investigations, or regulatory reviews.

Shufti Face Deepfake Detection is designed to help organisations identify and measure this exposure. The audit engine enables compliance, risk, and technology teams to scan previously approved customer selfies from 2020 to 2025 and quantify how many customer accounts would fail current deepfake detection standards. Findings are generated from real historical onboarding and authentication data, providing an evidence-based view of legacy verification performance.

Delivered as an Amazon Machine Image (AMI), the engine is deployed inside the company's own AWS account and Virtual Private Cloud (VPC). All biometric data processing remains within the company's existing cloud accounts, ensuring alignment with security, privacy, and data encryption requirements.

A key focus of this blind spot audit release on AWS Marketplace is operational simplicity. The audit engine can be deployed directly from AWS Marketplace with a single click, without system integrations, coding, or changes to existing verification platforms. No lengthy procurement cycles, unnecessary contracts, or long-term infrastructure commitments are required, allowing teams to initiate rechecks quickly and independently.

The Deepfake Detection engine rescan historic selfie images and flags patterns associated with deepfakes, face swaps, and generative artefacts that older controls may have missed. Reviews can be scoped by time period, geography, or product line, enabling organisations to focus on higher-risk cohorts without disrupting live onboarding or authentication journeys. The system supports both batch audits and individual session checks, providing flexibility for portfolio-wide reviews and targeted investigations.

How the detection works in practice
-When rescanning historic selfie images, Shufti's Multi-Layered Deepfake Detection evaluates:
-Facial landmark and skin-tone inconsistencies linked to face swaps
-Structural artefacts associated with AI-generated imagery
-Camera and Sensor-noise patterns to distinguish real captures from rendered images

"Companies make long-term risk decisions based on customer identity evidence collected at onboarding," said Shahid Hanif, CEO of Shufti. "As deepfake and face-manipulation techniques evolve, those records need to be reassessed against current detection standards. Shufti's face deepfake detection audit on AWS Marketplace enables teams to review historic approvals for deepfake and face-swap indicators within their own AWS environment and to base risk management and governance decisions on evidence-based outcomes."

Key highlights include:
-Detects AI-generated faces and face-swapped images within historic KYC selfie records.
-Measures deepfake exposure across previously approved customer segments from 2020 to 2025.
-One-click AMI deployment inside the company's AWS account, with no integration or without extended contracting or procurement cycles.
-No disruption to live KYC journeys, as forensic analysis is conducted on historic onboarding records.
-Fully customer-hosted processing, with no external data transfer or third-party handling of biometric data.
-Flexible audit scoping to prioritise higher-risk segments and investigation cases.

Shufti Face Deepfake Detection forms part of Shufti's complete portfolio of Blind Spot Audit engines on AWS Marketplace, alongside Shufti Face Liveness Detection (for identifying replayed, spoofed, and injected liveness sessions), Shufti Document Deepfake Detection (for uncovering AI-generated or fabricated ID documents), and Shufti Document Originality Detection (for verifying the authenticity of identity documents).

Together, these audit engines support a structured review of biometric and document records within the organisation's own AWS account and VPC.
The audit engine is available now on AWS Marketplace. To learn more about Shufti Face Deepfake Detection, visit: https://shuftipro.com/blind-spot-audit/deepfake-detection/

About Shufti

Shufti is a global identity verification and fraud prevention platform that helps organisations meet KYC, AML, and regulatory compliance requirements while reducing identity-related risk. Trusted by more than 1,000 businesses worldwide, Shufti's fully in-house technology stack includes real-time biometric face verification and liveness checks, document verification, electronic identity verification, sanctions and watchlist screening, and risk signal analysis across diverse markets and document types.

Designed to evolve with changing fraud techniques, Shufti's blind spot audit engines on AWS Marketplace enable organisations to re-evaluate existing customer profiles through one-click deployments within customer-controlled cloud environments. Shufti supports fraud, risk, and compliance teams in assessing verification outcomes, investigating suspicious activity, and strengthening controls across regulated digital journeys.

SOURCE SHUFTI

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