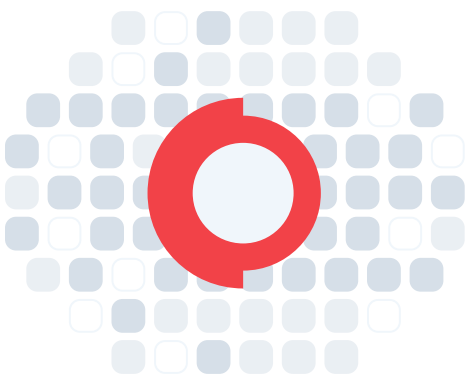


Document Verification for Social Networks & Creator Platforms

Verified Badges Mean Nothing If The Identity Behind Them Is Fake.



Social networks and creator platforms face an **identity problem** that is structural, not incidental.



Fake accounts, impersonation, coordinated abuse rings, and underage access are not edge cases, they are operating at scale. AI tools now generate photorealistic national IDs and passports that pass basic visual inspection. A fraudster doesn't need a real identity anymore; they need a good enough document. And as platforms move toward monetisation KYC, verified badge programs, and safety-event step-up flows, the stakes of getting verification wrong are rising simultaneously on every front: regulatory, reputational, and operational.

Creator monetisation programs, tipping, subscriptions, and payout events require identity verification before funds flow. Shufti's sub-15-second decisions and 98.49% TAR keep the experience frictionless for legitimate creators, while the 9-layer pipeline stops fraudulent monetisation claims at submission.

When Fraud Operates At This Level, Verification Has To Match It



Impersonation and fake verified accounts

Coordinated impersonation rings submit altered or AI-generated documents to claim verified badges against real public figures and brands. Shufti's DCT frequency analysis catches AI-generated documents invisible to RGB-only platforms. Fraud Memory flags document reuse across multiple account registration attempts. FAR 0.0163 — DHS RIVR 2025 validated.

Underage access

Self-declared age is not verification. Shufti extracts date of birth directly from the government-issued document via OCR — document-derived age, not self-reported. Every rejection is coded, evidenced, and stored for regulatory and legal defence.

Monetisation KYC at scale

Creator monetisation programs, tipping, subscriptions, and payout events require identity verification before funds flow. Shufti's sub-15-second decisions and 98.49% TAR keep the experience frictionless for legitimate creators, while the 9-layer pipeline stops fraudulent monetisation claims at submission.

Safety-event step-up

Harassment investigations, account recovery after compromise, and high-risk content events require identity re-confirmation. Video-Only mode blocks replay, screenshot, printed copy, and edited proof attacks and delivering live capture-based identity assurance for the highest-risk platform events.

Global creator and user base

Driving licences, work permits, and residency documents expire. Continuous Verification monitors document validity across your active worker base and triggers automated re-verification and eliminating the manual tracking gaps that create compliance exposure.

Feature Matrix

Module	Core Capability	Social Network Strategic Edge
9-Layer Forensic Pipeline	Document liveness, image properties, MRZ/security checks, template integrity, similarity search, copy-move, GenAI detection, DCT frequency, AutoML aggregation	Catches AI-generated documents used to fraudulently claim verified badges and monetisation access
DCT Frequency Analysis	Catches AI artifacts invisible in the RGB spectrum. 99% deepfake detection accuracy.	Detects ChatGPT/Grok/Gemini-generated IDs that pass every RGB-only verification check
Document-Derived Age Verification	DOB extracted directly from document via OCR. Not self-reported.	Eliminates regulatory and legal liability from self-declared age across all markets
Fraud Memory & Deduplication	Flags document reuse and re-registration patterns across every submission	Detects coordinated fake account rings cycling the same identity across multiple profiles
Video-Only Mode	Live capture blocks replay, screenshot, printed copy, and edited proof attacks	Identity re-confirmation for safety events, account recovery, and high-risk platform actions
Global Document Coverage	Any government-issued document, 250+ countries. New types added on demand.	One integration covering your entire global user base without per-country configuration
Heatmap Evidence	Pixel-level manipulation visualisation on every rejection	Defensible forensic evidence for regulatory investigation, litigation, and platform trust & safety review
Journey Builder	Configures verification flows per event type and risk tier without engineering rebuild	Lightweight badge verification for standard users. Full KYC for monetisation. Video step-up for safety events. Same API.

Performance Built For Platform Scale

False Rejection Rate (FRR)

0.0151, only **1.51%** of legitimate documents wrongly rejected.

True Acceptance Rate (TAR)

~98.49%, genuine documents pass on first attempt.

Equal Error Rate (EER)

~0.015–0.016, security and user experience optimised simultaneously.

False Transaction Count (FTC)

0, every document processed to completion, no exceptions.

OCR Accuracy

99.7% across **150+** languages on any government-issued document.

PVC Card Detection

Over **95%** accuracy, including Japanese PVC cards, an industry first.

Processing Speed

Under **15 seconds** end-to-end

Certifications

PCI DSS certified.

Deepfake Detection

99% accuracy via RGB and DCT frequency analysis.

Government Validation

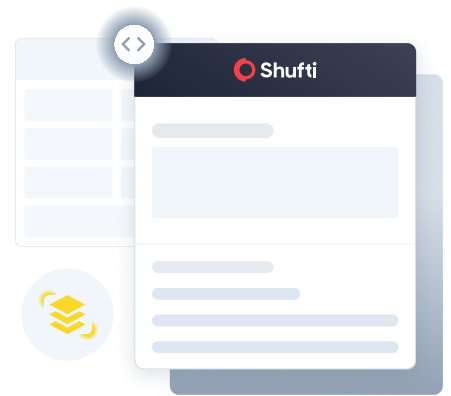
DHS RIVR 2025 Top Performer and Gartner recognised.

Regulatory Alignment

Framework	Requirement	How Shufti Delivers
EU Digital Services Act (DSA)	Age verification for minors; identity verification for traders; transparent moderation decisions	Document-derived age via OCR; heatmap evidence supports transparent, contestable decisions
GDPR — Arts. 5, 6, 9, 22, 28	Processor obligations; biometric data as special category; explainability of automated decisions	Article 28 processor status; no aggregators; heatmap evidence satisfies Article 22 contestability
CCPA / CPRA (California)	Sensitive personal information protections; biometric data obligations	In-house processing; no third-party routing; SOC 2 / ISO 27001 certified
COPPA (US)	Children's online privacy; age verification obligations	Document-derived age verification — not self-reported
FATF AML/CFT	CDD for platforms enabling financial transactions	Evidence-backed verification outcomes; AML screening add-on for monetisation flows
AMLR (EU) 2024/1624	Emerging obligations for platforms enabling value transfer	Journey Builder configures CDD tiers; examination-ready evidence per submission

Deployment

- ▶ **REST API**
Submit documents, select checks, receive structured results with reason codes. Operational in days.
- ▶ **Mobile & Web SDKs**
Guided capture embedded directly into badge application, creator onboarding, and safety-event flows.
- ▶ **Journey Builder**
Configure lightweight verification for badge programs, full KYC for monetisation, and video step-up for safety events — all from one platform, no engineering rebuild.
- ▶ **Deployment Options**
Cloud, On-Premises, Hybrid. PCI DSS certified.



Ready to Protect Your Platform?

See Shufti live against your verification use cases, your user populations, and your trust & safety requirements. **Request a Blind Spot Audit**, Test your current stack against AI-generated documents, fake badge applications, and coordinated account fraud. See what gets through.

www.shufti.com
sales@shufti.com

[Book a Demo](#)