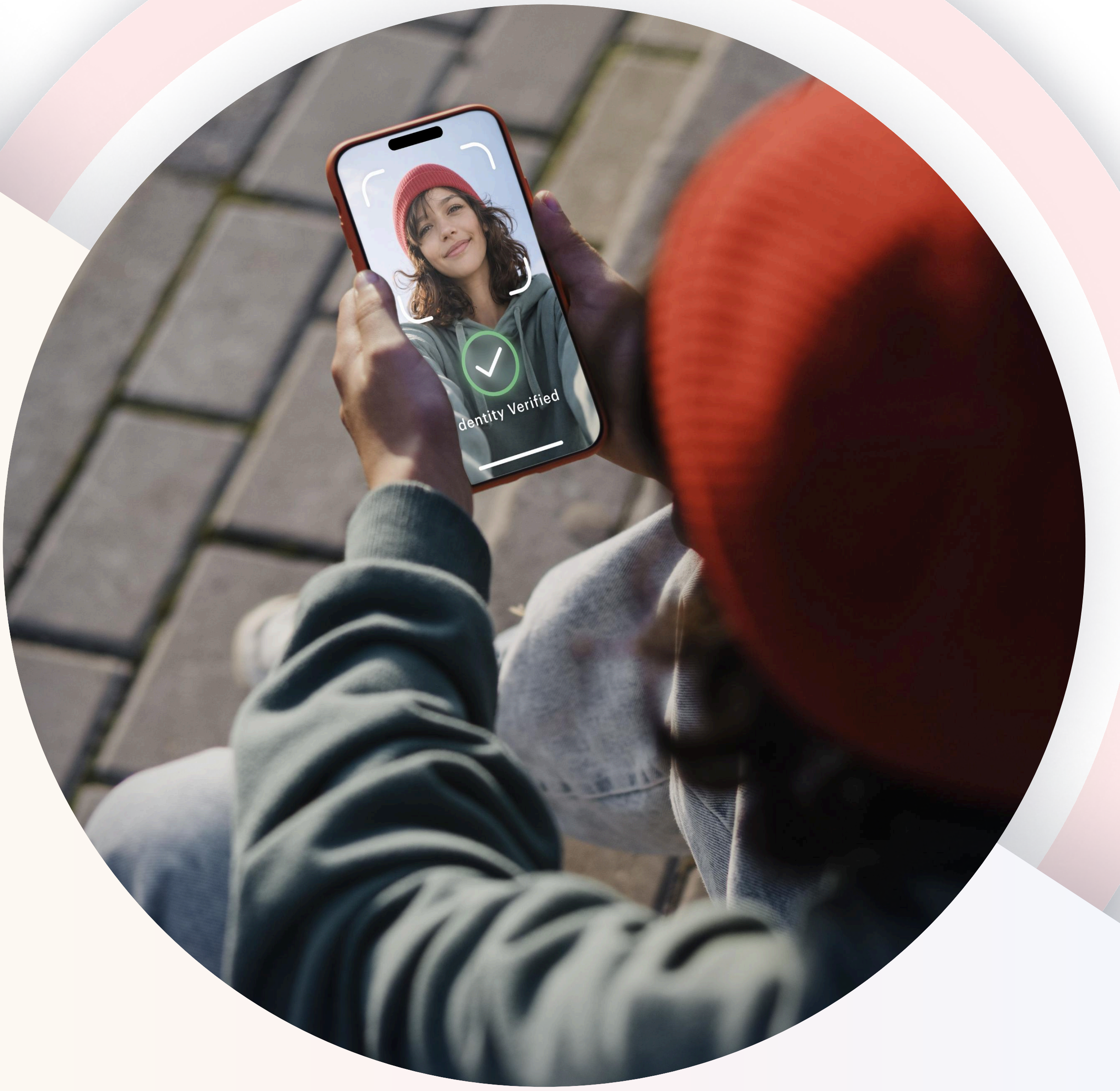
Shufti



GUIDE

An Enterprise Guide to Choose the Right Identity Verification Solution

VÉRIFICATION D'ÂGE KJM

PCI DSS

iBeta Niveau 1

ISO 27001: 2013

CE+

QG GDPR

SOC2

GDPR

CCPA

Executive Summary

Identity has become the primary control point of digital business. As onboarding, payments, access, and compliance move fully online, identity verification (IDV) now functions as core enterprise infrastructure.

The risk picture has shifted to synthetic identities, deepfakes, and automated attacks aimed directly at verification flows. At the same time, regulators expect explainable decisions and users expect to be verified in seconds. There is no tolerance for loopholes or one-size-fits-all controls.

This guide is for enterprises seeking to operate IDV as a strategic system rather than a black-box widget. It sets out how to evaluate platforms on what actually matters: who owns and controls the technology, how effectively multiple signals are used in real time, how easily workflows adapt to different markets and products, and whether monitoring and compliance keep pace with changing threats and rules. When an organization approaches IDV as part of core infrastructure, it becomes an advantage: faster onboarding for the right users, lower fraud and manual effort, and greater confidence in expanding into new markets.

Table of Contents

Table of Contents

This Guide Will enable enterprises to:

- Understand the evolving role of Identity Verification (IDV) — from compliance necessity to growth enabler.
- Explore how IDV reduces fraud exposure — blocking synthetic identities, impersonation, and repeat abuse while preserving conversion.
- Identify the core challenges enterprises face in scaling trust, compliance, and user experience globally.
- Evaluate what a future-ready IDV solution must deliver to balance assurance, speed, and adaptability.
- Learn how to assess vendors strategically — testing real performance, flexibility, and ownership of technology.
- Compare your current processes against measurable IDV ROI and stakeholder priorities.

Introduction

Identity verification has evolved far beyond a regulatory requirement. Today, it is the foundation of digital trust and a core engine of enterprise growth.

Remote onboarding is now the first interaction users have with an organization. How the verification layer performs, its speed, accuracy, and transparency directly influence approval rates, fraud losses, compliance efforts, and user experience.

Fragmented or rigid IDV systems introduce hidden costs: higher abandonment, inconsistent decisions across markets, and growing operational overhead.

When executed as strategic infrastructure, right IDV enables faster onboarding, expands global reach, and reduces enterprise risk.

63%

of users abandon digital onboarding mid-process

Remote identity verification processes that require users to scan identity documents, complete facial biometric matching, and pass liveness detection introduce inherent friction into onboarding journeys. When these steps are poorly designed or inconsistently executed, the resulting user experience compounds that friction, increasing the likelihood of mid-process abandonment.

[1] 2025 Digital Banking Performance Metrics.” Accessed: Dec. 19, 2025. [Online].
Available: https://www.crnrstone.com/gritty-insights/research/2025-digital-banking-performance-metrics

UNITED STATES ID CARD
JANE DOE
✓ VERIFIED

Identity Verification Solution as a Strategic Investment for Enterprises

Speed • Fraud Defense • Compliance • Efficiency

Identity verification is a core component of the infrastructure of the digital first world. The expansion of the digital world is dependent on remote identity verification, which now underpins how individuals access services, opportunities, and trust online.

Digital identity checks are projected to reach 86 billion in 2025, up from 75 billion in 2024 [2]. At the same time, identity theft and resulting fraud losses are also increasing. Enterprises with more than 5,000 employees report average annual identity-fraud costs of around US$13 million [3]. Scalable, accurate IDV is one of the few levers that can visibly reduce that drag on performance.

86B

Digital ID checks (2025 projection)

$13M

Avg annual identity fraud losses for large enterprises

Digital identity checks are surging globally. However, existing Identity Verification systems deployed by enterprises are failing to keep pace with the rising volumes of customers, the need for quicker onboarding, detecting the synthetic identities, and hence preventing the resultant fraud losses.

A modern enterprise identity verification platform must demonstrate measurable return on investment by improving the following areas

- Higher approvals
- Lower rate accepting fraudulent identities
- Less manual review
- Expansion across borders

[2] T. Wilson, "Substantial 15% Growth in Global Digital ID Verification Checks Over Next 12 Months." Accessed: Dec. 03, 2025. [Online]. Available: https://www.juniperresearch.com/press/substantial-15percent-growth-in-global-digital-id-verification-checks/

[3] Fintech News Singapore, "Identity Fraud Surges in Scale and Sophistication, with APAC's Financial Services Becoming a Prime Target," Fintech Singapore. Accessed: Dec. 03, 2025. [Online]. Available: https://fintechnews.sg/110619/regtech/identity-fraud-surges-in-scale-and-sophistication-with-apacs-financial-services-becoming-a-prime-target/

Quick Buyer Lens to Strategically Choose Identity Verification?

Metric	What It Means	Target / Ideal Benchmark	Why It Matters
Document & Market Coverage	Number of supported document types and jurisdictions.	Maximum global coverage	Enables expansion into new markets.
eID / Wallet Interoperability	Ability to accept and validate national eIDs and digital wallets.	Native or certified support	Future-proofs compliance and enhances usability.
FAR / FMR (False Accept / Match Rate)	How often the system incorrectly accepts an impostor.	< 0.1–0.3% (tighter for high-risk flows)	Keeps fraudsters from passing verification.
FRR / FNMR (False Reject / Non-Match Rate)	How often genuine users are wrongly rejected.	≤ 1–3%	Minimizes friction for legitimate users.
Liveness / PAD Efficacy	Effectiveness in detecting spoofing or presentation attacks.	Higher than 95% with PAD enabled	Protects against deepfakes & replay fraud.
Pass / Approval Rate	Percentage of users verified on first attempt.	Consistent quarterly improvement with stable fraud levels	Shows efficiency and conversion health.
Completion Time (P50 / P95)	Average and 95th percentile time to complete verification.	< 60s median / < 2–3 min at P95	Faster onboarding boosts conversion.
Abandonment Rate	Users who drop off during verification.	As low as possible	Indicates friction or poor UX design.
Manual Review Rate	Cases requiring human intervention.	As low as possible	Reduces cost and time-to-approve.
Tech-Stack Ownership	Extent of in-house control over core engines and models.	High in-house ownership	Improves accuracy, security, and accountability.
Human-in-the-Loop	Cases routed to expert review for complex or high-risk exceptions	Low rate; defined SLAs; consistent QA.	Reduces cost while keeping decisions defensible.
Customer Support & Incident Response	Support coverage for integration, operations, and production incidents.	24/7 coverage; SLAs; escalation path; RCA.	Minimizes downtime and speeds recovery.
Non-Document Verification	Verify identity via non-doc signals for lower-friction, less intrusive journeys.	Key jurisdiction coverage; clear assurance; configurable routing.	Improves completion and reduces intrusiveness.

A strategic IDV investment delivers measurable business impact — from faster onboarding to fraud reduction and audit readiness. Use this lens to separate promises from proof.

Enterprise Risk Areas Managed by Identity Verification Solutions

Synthetic Fraud Prevention

Synthetic identities now account for a growing share of fraud losses, with lender exposure reaching around US$3.2 billion by mid-2024 and rising 18% year over year. Preventing this requires document forensics, biometric assurance, and data-consistency checks that adapt to evolving attack patterns—blocking identities that do not exist in the real world without raising false rejects.

KYC & AML Compliance

Enterprises require reliable identity proofing, sanctions screening, and audit-ready evidence of what was checked and when. Verification outcomes must be exportable, defensible, and easy to interpret so compliance teams can navigate regulatory reviews, partner assessments, and rapid policy changes across jurisdictions.

Account Takeover (ATO) Prevention & Recovery

Credential resets, new devices, and high-value actions demand precise re-verification to confirm the rightful owner. Strong ATO defenses limit downstream loss while ensuring genuine users quickly regain access, preserving trust during the most sensitive moments of an account's lifecycle.

Age Assurance

Many countries including, Australia, North Americas, and certain European nations are tightening age regulation to restrict teens from harmful content online. Other countries are also likely to follow them, indicating the need for an effective IDV solution. Effective age assurance uses minimal data, offers seamless fallback options, and adapts to regional rules without adding undue friction for legitimate customers.

Modern identity verification addresses multiple layers of enterprise risk—from compliance and synthetic fraud to user protection and account recovery—balancing assurance with user experience

Must-Have Capabilities in an Enterprise IDV Solution

A modern IDV platform operates through interoperable layers that work together to deliver accuracy, speed, and assurance. Each capability plays a critical role in protecting end users, meeting compliance obligations, and strengthening trust in every transaction.

Identity Document Verification

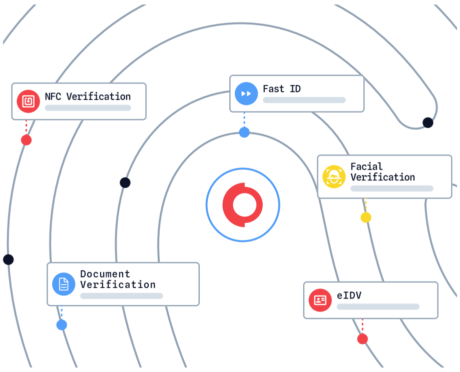
Verifies the authenticity of passports, Government IDs, driving licences, or any other document that can be used to verify the identity of the user, so only genuine documents enter the system. This is the foundation for KYC, age checks, and secure account opening.

What to Look For

Ability to verify a wide range of identity documents, including ID cards, driving licences, and utility bills, across Latin and non-Latin markets while accurately detecting fraudulent and manipulated documents.

Pilot Checks

Check first-pass capture rate, OCR accuracy by country/script, and document forgery catch rate.



Electronic ID (eID) Verification

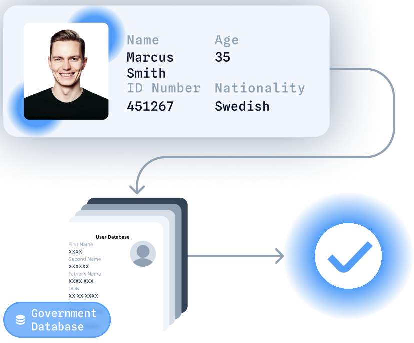
Connects with national eIDs, NFC-enabled documents, commercial databases, and digital wallets to validate users in real time. Enables faster onboarding and compliant access across global markets while preserving trust.

What to Look For

Supported eIDs/jurisdictions, NFC Document; cryptographic assurance levels; fallback reliability.

Pilot Checks

Measure eID/NFC Document success rate, latency, and error handling across priority jurisdictions.



Face Verification

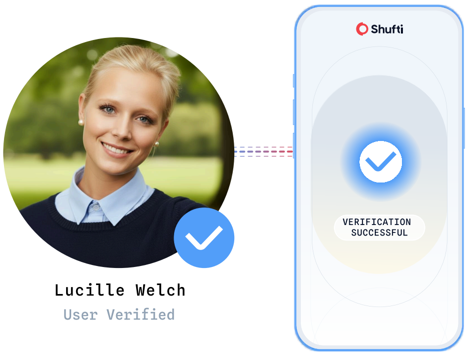
Performs one-to-one matching between the document portrait and a live face capture, ensuring the right person is present at onboarding.

What to Look For

Disclosed error rates (FAR/FRR), robustness across devices and lighting, and clear tuning options.

Pilot Checks

Test match accuracy and false reject ratio on real devices, networks, and document mix.



Liveness Detection

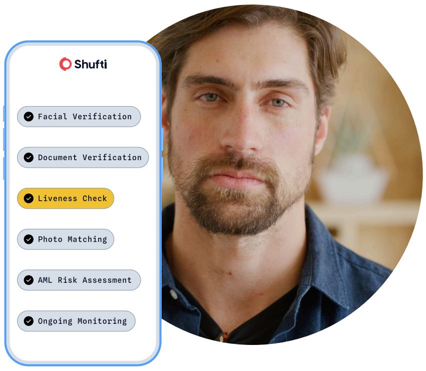
Confirms that a real, live person is present, not a photo, mask, replay, or deepfake, before trusting a face match or approval.

What to Look For

PAD evaluations, resistance to spoofing and injections, performance in low-light/low-bandwidth scenarios, and ease of fallback.

Pilot Checks

Measure first-attempt pass rate for genuine users, spoof catch accuracy, and false positives on platform traffic.



Device Fingerprinting

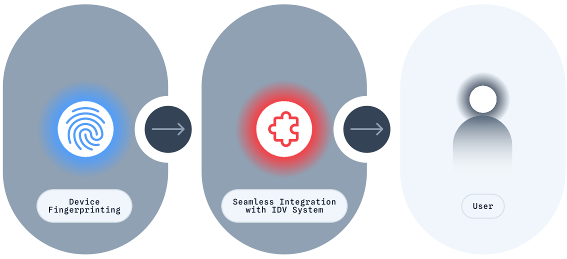
Assesses device integrity and environment (for example, VPNs, emulators, or risky device patterns) to surface hidden risk without extra steps for the user.

What to Look For

Precision at scale, privacy-by-design setup, and minimal latency impact.

Pilot Checks

Review false positive rates, added latency, and reduction in multi-accounting or obvious abuse.



Behavioral Biometrics

Analyses interaction patterns such as typing rhythm or motion to distinguish genuine users from bots or scripted behaviour in real time.

What to Look For

Explainability of signals, opt-out controls, and safeguards against penalising normal user variation.

Pilot Checks

Track false rejection rates for normal users and uplift in the detection of automated or synthetic activity.

Human-in-the-Loop Verification

Blends automation with expert review for complex or high-risk cases. Ensures regulatory precision and fairness by pairing machine efficiency with human judgment.

What to Look For

Reviewer SLAs, oversight quality, and secure data handling.

Pilot Checks

Evaluate average review time, agreement rate with automation, and appeal overturns.

Reusable Identity Verification

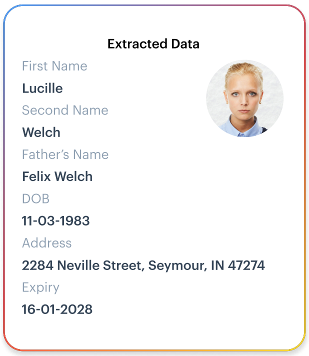
Quickly detects duplicate identities across the system to surface repeated abuse such as mule activity or bonus misuse, without manual investigation. Moreover, enables Reusable Identity to save onboarding time.

What to Look For

Capability to link repeated use of the same ID, device, or identity profile with configurable thresholds and alerts. Users' ability to generate a reusable identity.

Pilot Checks

Check how many duplicate or repeated identities are surfaced and how much manual review time is saved.



Extracted Data

First Name
Lucille

Second Name
Welch

Father's Name
Felix Welch

DOB
11-03-1983

Address
2284 Neville Street, Seymour, IN 47274

Expiry
16-01-2028

Multi-Signal Fraud Intelligence

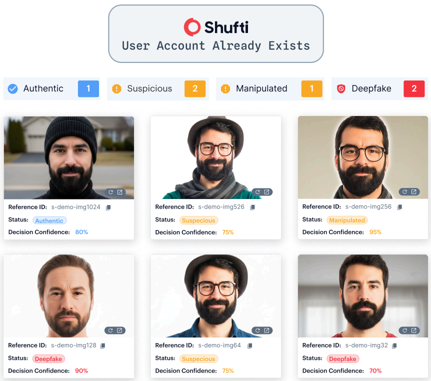
Fraud prevention requires more than rejecting deepfakes or forged documents. Organized networks often cycle stacks of fake IDs through the same devices or emulators. An IDV system that unifies document forensics, liveness, device intelligence, and behavioral signals can detect these coordinated attacks instantly.

What to Look For

Cross-signal correlation across device IDs, emulator detection, document patterns, and behavioral anomalies.

Pilot Checks

Validate the ability to detect repeated attempts from the same device/emulator and expose coordinated identity attacks.



Shufti
User Account Already Exists

Authentic 1 | Suspicious 2 | Manipulated 1 | Deepfake 2

Reference ID: s-demo-img1024
Status: Authentic
Decision Confidence: 80%

Reference ID: s-demo-img526
Status: Suspecious
Decision Confidence: 75%

Reference ID: s-demo-img256
Status: Manipulated
Decision Confidence: 95%

Reference ID: s-demo-img128
Status: Deepfake
Decision Confidence: 90%

Reference ID: s-demo-img64
Status: Suspecious
Decision Confidence: 75%

Reference ID: s-demo-img32
Status: Deepfake
Decision Confidence: 70%

Pass rate impact on conversions

At 100,000 monthly applications, pass-rate improvements directly compound approved customers. The visuals below compare a 70% baseline with an 80% pass-rate scenario.

Baseline 70% pass rate

Approved/month
70,000

Approved/year
840,000

Improved 80% pass rate

Approved/month
80,000

Approved/year
960,000

Impact of a +10 Percentage Point Increase (70% → 80%)

+10,000 additional approved customers per month

+120,000 additional approvals per year

This uplift is achieved without increasing acquisition spend—purely through improved verification accuracy and reduced false rejections.

Why is automating KYC necessary for seamless expansion and fraud prevention?

40% of total onboarding time is consumed by KYC due diligence and account opening - turning compliance into one of the biggest bottlenecks in financial services.

Manual data entry, disconnected systems, and duplicative forms slow onboarding and increase error rates across regulated industries.

Automating ID verification and reusing verified data can cut onboarding time by half - improving compliance accuracy and customer satisfaction.

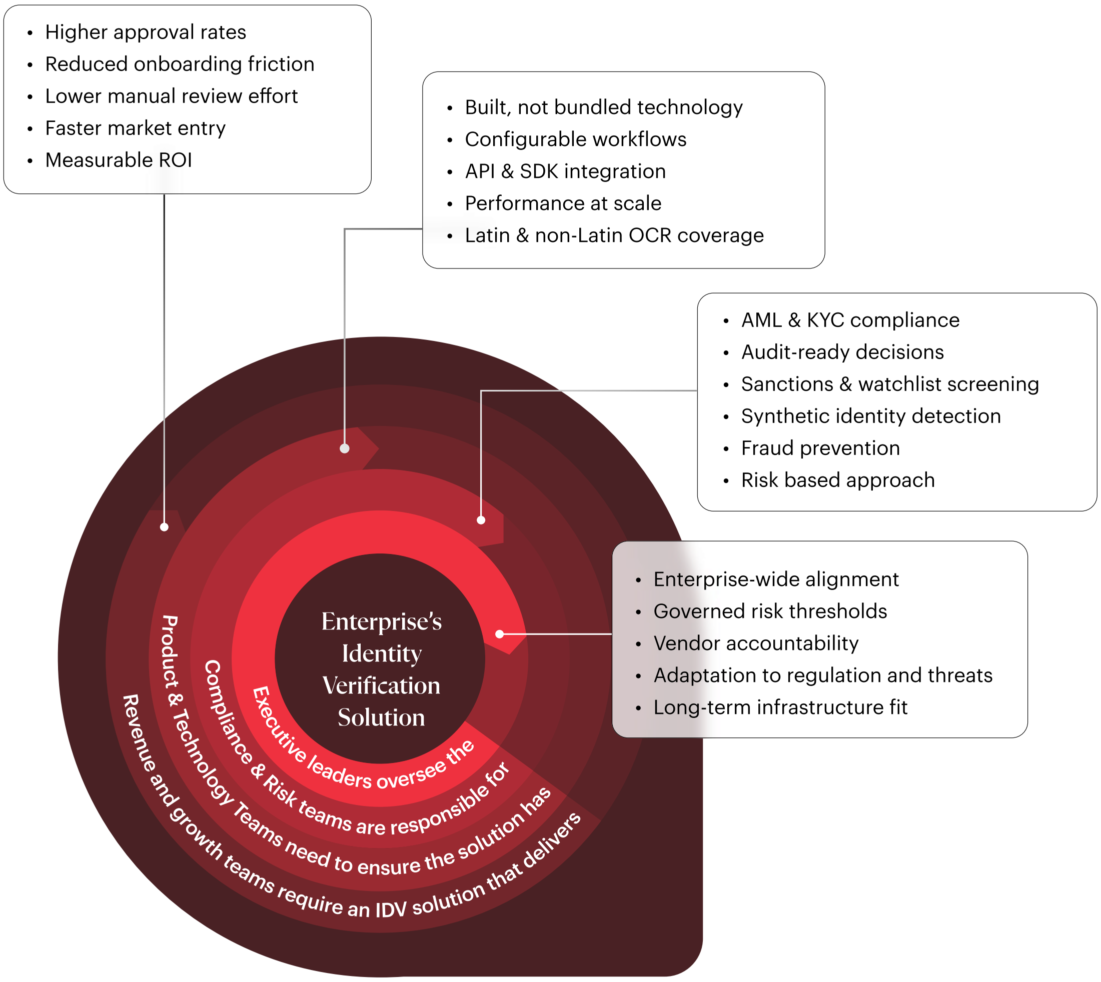
Source: McKinsey (2024) – "Rethinking KYC and Onboarding", Exhibit 2

An ideal Vendor must satisfy the concerns of all stakeholders within the organization.

A truly enterprise-grade IDV platform must satisfy the priorities of compliance, product, engineering, growth, UX, and leadership, without forcing trade-offs between speed, assurance, or scale.

> Is the IDV solution forcing businesses to compromise on User Experience, compliance, and security?

Enterprises must assess whether an identity verification solution meets the needs of all stakeholders, from compliance and risk to product and revenue. Achieving that alignment requires each team to evaluate the platform against the questions that matter to its mandate, ensuring the IDV decision holds up across the organization.



Revenue and growth teams require an IDV solution that delivers

- Higher approval rates
- Reduced onboarding friction
- Lower manual review effort
- Faster market entry
- Measurable ROI

Product & Technology Teams need to ensure the solution has

- Built, not bundled technology
- Configurable workflows
- API & SDK integration
- Performance at scale
- Latin & non-Latin OCR coverage

Compliance & Risk teams are responsible for

- AML & KYC compliance
- Audit-ready decisions
- Sanctions & watchlist screening
- Synthetic identity detection
- Fraud prevention
- Risk based approach

Executive leaders oversee the

- Enterprise-wide alignment
- Governed risk thresholds
- Vendor accountability
- Adaptation to regulation and threats
- Long-term infrastructure fit

Each team must evaluate the IDV solution based on its specific mandate and assess whether the solution meets those requirements.

[7] Shufti. (2025). The Top 10 Most Difficult Countries for Identity Verification.

Compliance & Risk Leaders

"Compliance and risk leaders need accurate, fraud-resistant identity verification that enables KYC compliance without adding unnecessary friction."

- Does the IDV solution provide ID verification and AML screening according to the risk appetite or risk exposure of the enterprise?
- Can every verification decision be explained and defended under audit?
- Are all risk signals, rules, and decision paths fully transparent?
- Is the entire verification pipeline under strict data-handling and aligned with the regulatory mandate?
- Does the platform cover diverse, jurisdiction-specific document types with reliable accuracy across languages and formats?
- Is non-document identity verification available in order to provide low friction and less intrusive digital onboarding
- How much solution is adaptive to changes in the policy layer, reflecting AML and Sanctions regulations

Product & Tech Teams

"Product and technology teams need a stable, configurable, & scalable identity verification platform that integrates once and performs reliably across environments and volumes."

- Can the organisation integrate the platform once and maintain long-term stability across updates?
- Can verification flows be changed without code or vendor intervention?
- Does the system behave consistently across devices, platforms, and bandwidth levels?
- Does the platform support SDK, API-based, and fully embeddable integrations?
- Does the solution harmonize the KYC data for CRM?
- Does the solution support a mix of deployment options—on-premises, private cloud, and SaaS—and can these be combined in a hybrid setup if required?
- How well does the solution withstand traffic spikes and parallel onboarding loads?

Revenue & Growth Teams

"The Revenue team needs identity verification that maximizes the customer conversion and approval rates while minimizing fraud, friction, and manual effort to drive measurable ROI."

- How many legitimate users pass IDV on the first attempt, and why do others fail?
- How well does the system prevent fraud without suppressing conversions?
- What is the expected impact on Customer Acquisition Cost (CAC), approval rate, and overall onboarding yield?
- Can the organization enter new markets without redesigning verification flows from scratch?
- How much manual review effort does the system eliminate?
- Does the system accelerate onboarding of qualified users while filtering high-risk profiles?
- Does the IDV solution provide a measurable Return on Investment (ROI)?

UX & Design Teams

"The Design team needs a consistent, accessible, and localized verification experience that reduces user friction and supports brand-controlled journeys across devices and networks."

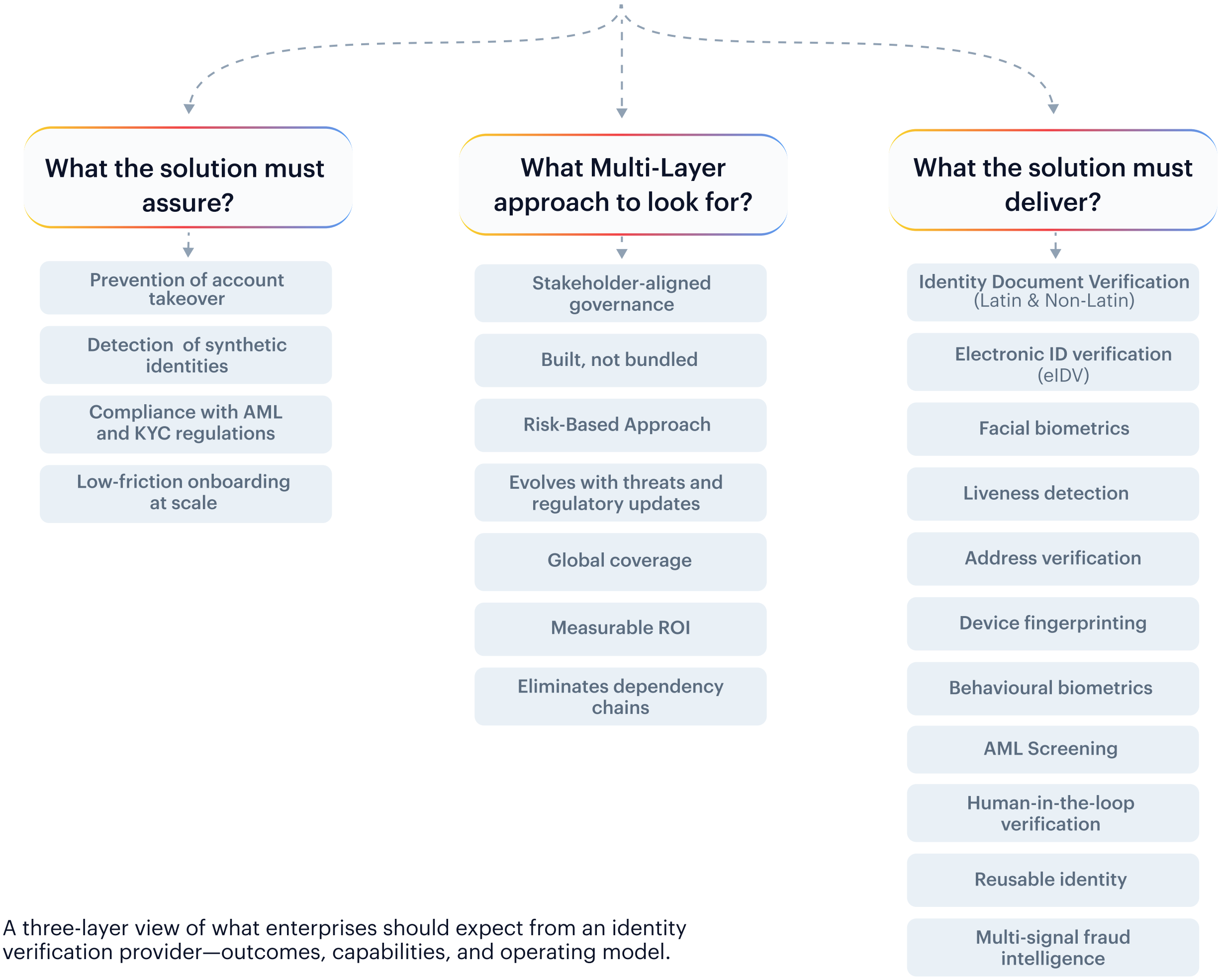
- Is the verification experience consistent and predictable across devices and networks?
- Do users receive real-time guidance to prevent avoidable failures for a smooth onboarding workflow?
- Can the experience be localized—content, structure, and micro-copy?
- How much cognitive load does the verification flow impose on users?
- Does the solution let you present the verification flow in the organization's own brand look and feel?
- Are accessibility standards supported in the verification journey?
- Can the flow adapt to user context without forcing unnecessary steps?
- Does the solution give the onboarding instructions in various languages based on the user's region?

Executive & Strategy Leadership

"The Executives need identity verification as a resilient, controllable infrastructure that scales across markets, adapts over time, and delivers predictable outcomes with enterprise-grade oversight."

- Does IDV function as controllable infrastructure rather than a fixed workflow?
- Can it support expansion into new markets without architectural change?
- Are accuracy, uptime, and latency backed by transparent SLAs?
- How resilient is verification to model drift, document changes, and volume spikes?
- Do governance, permissions, and reporting align with enterprise standards?
- Does the platform keep pace with emerging digital identity ecosystems?
- Can the organisation forecast and measure verification outcomes reliably?

Ideal Identity Verification Vendor Profile



What the solution must assure?

- Prevention of account takeover
- Detection of synthetic identities
- Compliance with AML and KYC regulations
- Low-friction onboarding at scale

What Multi-Layer approach to look for?

- Stakeholder-aligned governance
- Built, not bundled
- Risk-Based Approach
- Evolves with threats and regulatory updates
- Global coverage
- Measurable ROI
- Eliminates dependency chains

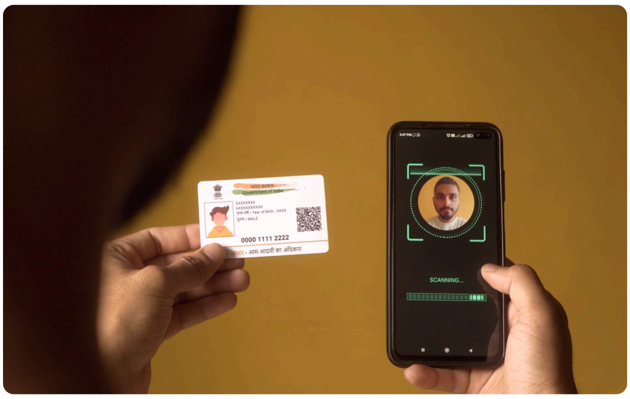
What the solution must deliver?

- Identity Document Verification (Latin & Non-Latin)
- Electronic ID verification (eIDV)
- Facial biometrics
- Liveness detection
- Address verification
- Device fingerprinting
- Behavioural biometrics
- AML Screening
- Human-in-the-loop verification
- Reusable identity
- Multi-signal fraud intelligence

A three-layer view of what enterprises should expect from an identity verification provider—outcomes, capabilities, and operating model.

Rising Fraud Risks & Expectations from Identity Verification Providers:

Enterprises now face synthetic identities, deepfake impersonation, and automated attacks that continuously probe onboarding flows for weak points. These threats evolve faster than static defenses and target the verification layer itself, not just payments or account activity.

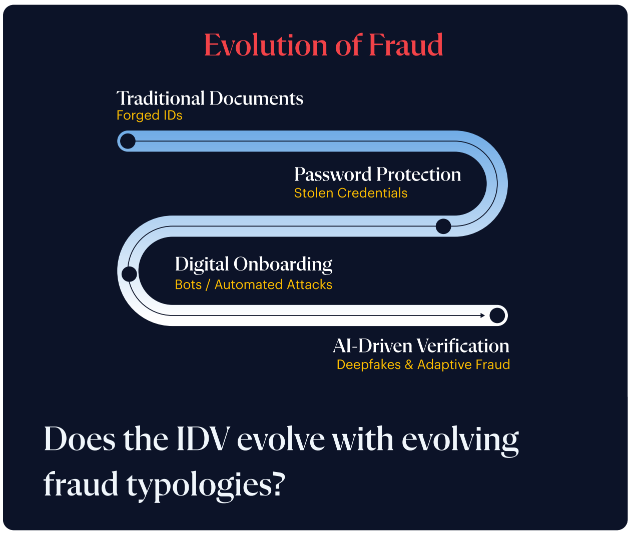


Regulatory and loss data reflect this shift. FinCEN's review of Bank Secrecy Act [4] filings shows that identity-driven activity, fraud, false records, identity theft, and attempts to bypass verification account for most identity-related reports and the largest share of losses linked to them.

Need for KYC Solutions to Innovate with Evolving Threats and Regulatory Velocity

For enterprises, an Ideal Vendor Profile in an enterprise KYC solution must have this crucial feature- It should innovate to introduce capabilities that help comply with the latest regulations.

The threat landscape confronting identity verification is changing at an unprecedented pace. Generative AI has made it easy to produce deepfakes, synthetic identities, and high-quality fake documents at scale, allowing


Evolution of Fraud

Traditional Documents
Forged IDs

Password Protection
Stolen Credentials

Digital Onboarding
Bots / Automated Attacks

AI-Driven Verification
Deepfakes & Adaptive Fraud

Does the IDV evolve with evolving fraud typologies?

[4] "FinCEN Issues Analysis of Identity-Related Suspicious Activity," FinCEN.gov. Accessed: Dec. 03, 2025. [Online]. Available: https://www.fincen.gov/news/news-releases/fincen-issues-analysis-identity-related-suspicious-activity#:~:text=Report%20examines%20suspicious%20activity%20tied,as%20opening%20and%20accessing%20accounts.

fraudsters to bypass traditional KYC checks and reuse compromised identities across platforms. These techniques increasingly fuel account takeover fraud, where identities that once passed verification are later exploited, exposing the limitations of static, one-time onboarding controls.

In parallel, the AML and sanctions environment continues to shift, with frequent updates to sanctions lists, evolving PEP classifications, and jurisdiction-specific regulatory requirements that can rapidly change the risk status of individuals and entities. Identity verification providers must therefore evolve from fixed workflows to adaptive systems that continuously interpret risk signals, incorporate regulatory changes, and adjust verification paths without requiring process redesign. In addition, these platforms must continuously innovate to help enterprises comply with evolving requirements, offering configurable and customisable capabilities that align with changing regulations, risk appetites, and market-specific compliance needs.

This is more necessary for major financial service providers that offer diverse customers and cater to jurisdictions across the globe.

The core banking industry alliances, such as the Wolfsberg Group in the Wolfsberg Statement on Effective Monitoring for Suspicious Activity, Part II, Transitioning to Innovation, also emphasize having an adaptable governance framework

> **“As criminal networks continue to evolve at a rapid pace, as do national security priorities, FIs must embrace an innovation governance framework that is nimble and allows for prompt responses to evolving threats.”**

Thus, Organizations need to evaluate the vendor based on its adaptability and innovation that aligns with changing fraud typologies and regulatory requirements.

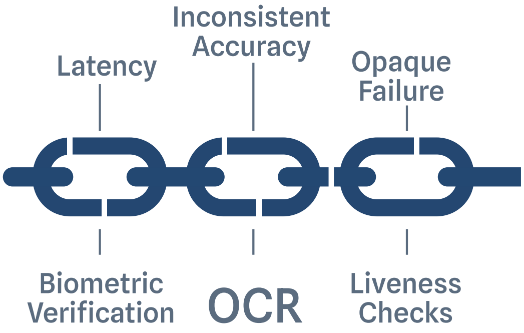
An ideal IDV must reliably address these core risk and compliance scenarios across the enterprise's lifecycle.

These pillars represent the critical areas where robust identity verification strengthens trust and reduces enterprise risk.

Built vs. Bundled: Why Technology Ownership Defines IDV Integrity

What Does It Mean When an Identity Verification Solution Doesn't Build the Tech In-House

When a provider stitches together multiple external engines, Latin IDV from one vendor, non-Latin from another, Custom UI/UX from a third, businesses inherit a chain of vulnerabilities: uneven quality, conflicting release cycles, opaque failure modes, and cascading outages.



The enterprises that aim to expand their business from one region to another, this expansion would bring various fraud typologies, risk factors regulatory compliance that need to be addressed.

Did you know?

Using an identity verification stack stitched from multiple third-party vendors can increase the *chain of vulnerability* — one weak link can compromise the whole flow and widen your exposure.

Each subprocessor adds latency, raises data-sharing exposure, and complicates incident response for regulatory audits like Data Protection Impact Assessments (DPIAs; applicable under GDPR). In practice, this means more false accepts or rejects that can't be fully explained, and enhances the chances of a data breach due to multiple vendors' involvement.

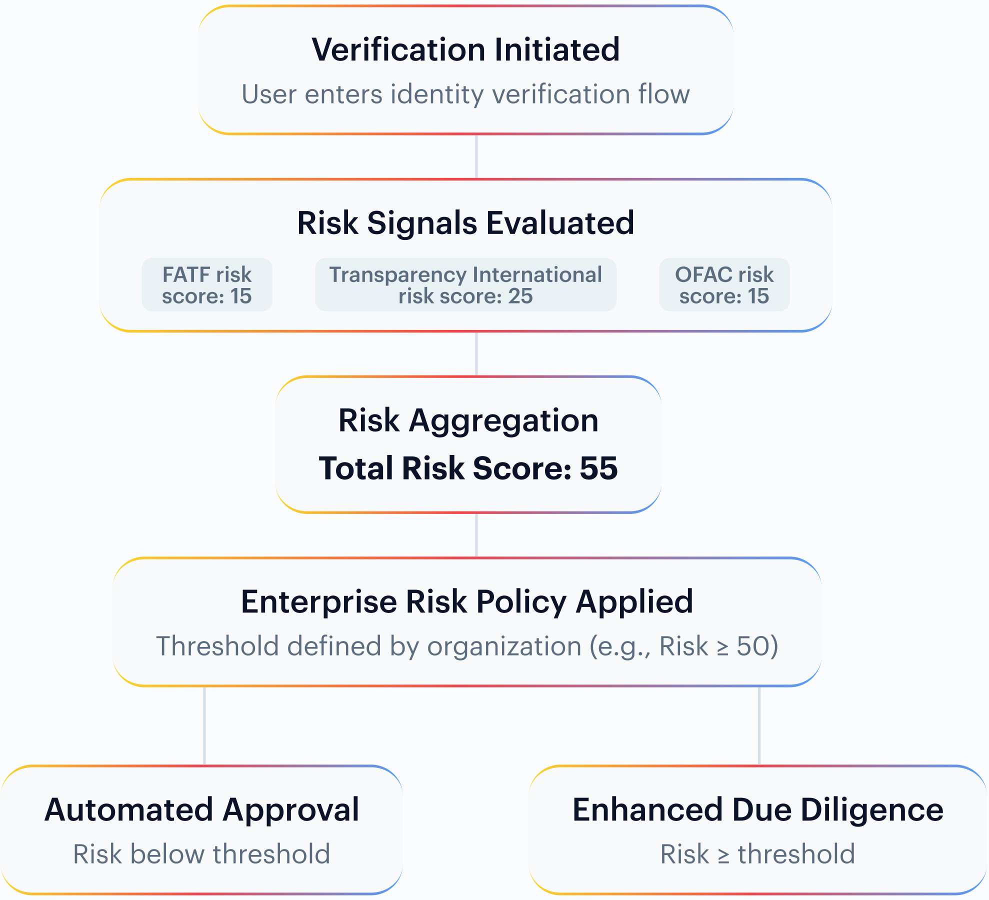
Many IDV solutions support Latin-script OCR in house, but depend on third parties for non-Latin documents, introducing fragmented control and a broader chain of vulnerability.

Customizable Workflows: Making Identity Verification Solution a Natural Extension of the Enterprise

An enterprise-ready IDV solution adapts to different industries, markets, and risk profiles instead of enforcing a rigid, one-size-fits-all journey. The right platform lets teams configure flows end-to-end, selecting document types, data sources, liveness and biometric steps, escalation rules, and fallback paths, so assurance can be tuned to each use case without rebuilding systems or trading off speed, compliance, or experience. When workflows are configurable at this level, identity verification becomes a seamless, scalable component of the organisation's digital infrastructure.

Risk-Based Identity Verification Flow

This flowchart shows how enterprises combine multiple risk signals and apply custom thresholds to control verification outcomes.



Verification Initiated
User enters identity verification flow

Risk Signals Evaluated
FATF risk score: 15
Transparency International risk score: 25
OFAC risk score: 15

Risk Aggregation
Total Risk Score: 55

Enterprise Risk Policy Applied
Threshold defined by organization (e.g., Risk ≥ 50)

Automated Approval
Risk below threshold

Enhanced Due Diligence
Risk ≥ threshold

The above workflow shows one of the examples, of Identity Verification Flows used by Enterprises to enhanced onboarding of legitimate users and drop the high-risk one.

How does Shufti enable enterprises to comply, prevent fraud, and grow simultaneously?

One platform, tailored to enterprises' needs

Shufti's platform is built to adapt to the enterprise's risk profile and regulatory landscape, rather than enforcing a fixed approach. Recognised as ID Verification Innovator of the Year 2025 at the Brit FinTech Awards, it continuously innovates, models, and workflows as fraud tactics, threat vectors, and regulations change, helping organisations sustain security, compliance, and user experience over time.

Built from the ground up

Every core component, including OCR engines built from scratch for both Latin and non-Latin scripts, biometrics, liveness detection, and risk models, is developed and managed in-house. This unified foundation delivers consistent accuracy, low latency, and full control over data. When fraud patterns change or regulations shift, Shufti empowers rapid adaptation without reliance on third parties or additional engineering burden. The solution has supported the leading FinTechs in expanding securely across some of the world's most complex and tightly regulated markets.

Design journeys, don't inherit them

With Shufti's Journey Builder, Organizations can design and modify onboarding and verification flows without code. Drag-and-drop the steps required, define rules by country or risk segment, add step-up checks where required, and preview the end-user experience in real time. This lets the businesses respond to new regulations, use cases, or fraud patterns in minutes, without long development cycles.

Global reach, local precision

Shufti combines global coverage with local intelligence. It recognises regional documents, supports national eIDs and digital wallets, handles multiple languages and scripts, and offers clear data-residency options. This "glocal" approach lets enterprises enter new markets with confidence while keeping compliance and user experience aligned to local rules.

Transparent and auditable decisions

Every verification comes with context. Shufti shows what was checked, which signals were triggered, and why each outcome was reached. Audit trails, configurable workflows, and ongoing AML monitoring turn compliance from a cost centre into a source of defensible, documented trust.

- **Built for businesses that move fast**

From fintech and banking to marketplaces and telecommunications, organisations use Shufti to combine speed, accuracy, and regulatory confidence. The platform evolves with new threats, adapts to emerging laws, and scales alongside the enterprise's growth strategy.

- **Rapid, self-service evaluation**

Validate this guide in minutes. Access Shufti's Self-Service Portal to spin up a sandbox, run live KYC/AML and face checks, and review real results, without sales cycles or fixed-term commitments. Use sample data or internal test sets, export findings internally, and decide based on evidence, not claims.

Test Shufti on AWS Marketplace for Synthetic IDs Existing in Your Customer Base

Shufti on AWS Marketplace enables enterprises to identify synthetic identities that may already exist within their customer base, without disrupting live systems or sharing data externally. By applying advanced checks such as deepfake detection, document originality analysis, document deepfake detection, and liveness verification, organisations reverify the synthetic identities that may have bypassed existing verification controls.

All testing runs within the organisation's own AWS environment, preserving data confidentiality and meeting internal security, audit, and governance requirements. This allows risk and compliance teams to audit their current verification setup, validate whether an existing vendor is performing as expected, and quantify hidden fraud exposure, before it results in losses or regulatory scrutiny.

Run the assessment, review the evidence, and make vendor decisions based on facts, not assumptions.

Shufti

Ready to build verification infrastructure that protects your business from regulatory action and executive liability?

See how Shufti's comprehensive identity verification solutions help organizations maintain operational continuity while meeting the evolving compliance standards that regulators demand.

Learn More