GUIDE

Scale Without Borders:

The ultimate adaptability advantage you need for global growth

Shufti

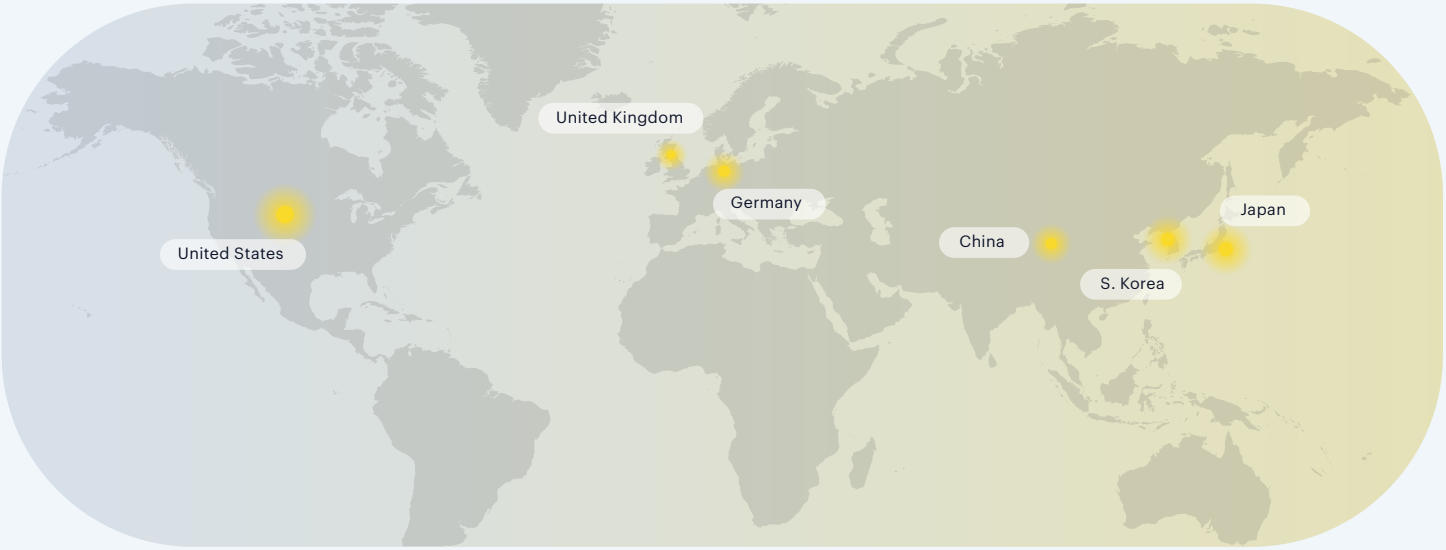
The digital economy has no borders

No matter where in the world you live or conduct business, change isn't just inevitable — it's happening at an unprecedented pace. With 7.34 billion people around the world expected to use smartphones this year, and 72.6% relying on mobile as their sole internet access, digital transformation has created a borderless economy.[1]

This shift is most dramatic in emerging markets. For example, internet users in Southeast Asia have doubled since 2016, with the region's digital economy projected to reach $600 billion by 2030. Around the world, entire populations are jumping ahead of traditional infrastructure to mobile-first digital services.[2]

But here's the challenge: While global expansion opportunities seem limitless, the technology for trust and verification remains extremely localized.

Consider the world's six largest digital economies: the U.S., China, the UK, Japan, Germany, and South Korea. Together, they represent vastly different cultures and approaches to identity documentation — from Japan's multiple writing systems to Germany's strict privacy laws, and China's digital ID ecosystem to state-issued documents in the U.S. Each market has its own regulatory frameworks, document types, and cultural expectations that make identity verification in each location uniquely complex.



1 | Forrester Research, Inc. (2024). Global digital economy forecast, 2023 to 2028. Forrester Research.
2 | Tech Collective Southeast Asia. (2024, December 18). The evolution of the digital economy in Southeast Asia. Tech Collective Southeast Asia.

For any business looking to expand globally, this creates a challenge. An identity verification solution that understands U.S. driver's licenses may be completely unprepared for Myanmar's handwritten documents.

The result?

Global expansion often stalls not because the local market isn't ready or willing, but because organizations can't reliably verify who their customers are across new markets.
That's why businesses must embrace what we call ultimate adaptability in identity verification, or the ability to rapidly transform processes to meet the unique business, technology, and compliance requirements of any market, anywhere in the world.

Ultimate adaptability in identity verification is not just a competitive advantage, **it's a necessity.**

Why one-size-fits-all identity verification fails globally

While these opportunities are compelling, many organizations fall into a critical trap: they pursue global growth without an adaptable identity verification system.

When those initial identity verification approaches fail, businesses often resort to quick fixes: patching together regional solutions that create data silos, or worse, abandoning promising markets entirely.

The reality is that every country has its own unique regulatory frameworks, document types, and customer behaviors that affect how you do business. The one-size-fits-all mentality becomes especially dangerous as regulations evolve.

When the EU implements new privacy rules or Singapore tightens financial compliance, rigid systems require complete overhauls — bringing expansion to a grinding halt.

The high price of getting identity wrong

When businesses realize their assumptions don't hold up in new markets, the consequences can be severe and costly. This can look like:

Lost revenue from abandoned transactions

When verification processes can't adapt to local preferences and document types, customers will likely abandon onboarding, or be unnecessarily denied. This not only erodes trust in the brand, but can exclude certain populations from critical services. According to a report by Forrester, complicated and often manual verification processes can lead to abandonment rates of 32% after just 10 minutes.[3] And when your acceptance rates are just 40%? That cuts potential revenue by more than half.

Compliance penalties

Fail to meet local regulatory requirements and you could be facing significant fines and operational restrictions. In Singapore, the financial sector saw compliance fines increase by 22%, from $2.68 million in 2023 to $3.28 million in 2024. These fines were for AML, KYC, and transaction monitoring of breaches. According to a report from Fenergo, this increase was fueled by "increased technology adoption by regulatory bodies and subsequent efficiency gains."[4]

Countries like Brazil, Mexico, and Argentina are strengthening enforcement and adopting GDPR-like frameworks, such as Brazil's General Personal Data Protection Act (locally known as LGPD). We can expect these changes to lead to increased penalties and regulatory actions, especially as new laws mature and enforcement capacity grows.

A patchwork of solutions

A survey by Forrester found that 79% of respondents reported a substantial increase in the number of digital transactions their organizations processed. With these volumes, patching together multiple regional identity solutions becomes not only an integration nightmare, but leads to higher costs and a less than ideal experience for users.[5]

3 | Forrester Research, Inc. (2024). Global digital economy forecast, 2023 to 2028.

4 | DocuSign. (2024, March 12). Top trends in identity verification technology. DocuSign.

5 | Fund Selector Asia. (2024, December 20). Singapore's financial sector prepares for more enforcement action in 2025. Fund Selector Asia.

Beyond Borders: When Expansion Hits a Wall

So what's the reasoning behind these failures?

The hidden complexity behind global IDs

Documents in countries across the world are as diverse as the people and cultures that populate them.

According to Shufti, more than 10,000 types of ID documents exist across the world, ranging from passports to handwritten documents in every language. Non-Latin scripts and languages require specialized technology that most providers just don't support.

Japan uses the Japanese era calendar (Reiwa, Heisei), Ethiopia is 7-8 years behind Gregorian, Sri Lanka uses the Buddhist era (543 years ahead), and Cambodia uses both Western and Buddhist formats. Countries like Myanmar, Ethiopia, Nigeria, and Libya still rely heavily on handwritten documents or low-quality paper-based IDs.

Even within the same country, you'll find that documents can differ wildly.

India's driver's licenses differ by state, South African documents vary by region, and Japan's licenses have different stripe colors based on driving history. Nigeria exemplifies how multiple ID systems (NIMC, FRSC, INEC) create verification challenges with different agencies issuing different documents with varying security features and formats.[6]

It's just not scalable to be an expert in every document. And failing to adapt to local markets means missing out on a new customer base.

Navigating rapidly evolving regulations

Document complexity is just one aspect of these challenges. Even with perfect document recognition, organizations must navigate equally complex regulatory requirements.

Global regulatory frameworks are constantly evolving to address emerging risks, and regulations are becoming more proactive than reactive, often with shorter implementation timelines.

6 | Shufti. (2025). The Top 10 Most Difficult Countries for Identity Verification.

For example:

> eIDAS 2.0 in the European Union is advancing real-time identity verification using trusted data sources. The Financial Action Task Force (FATF) continuously updates its guidelines on anti-money laundering (AML) and counter-terrorism financing (CTF), influencing regulations across multiple jurisdictions.
>
> In the United States, regulatory bodies such as FinCEN are introducing new compliance mandates for financial institutions. Countries in Southeast Asia, such as Indonesia, Vietnam, and the Philippines, are rapidly evolving their regulatory frameworks to support digital payments and e-commerce, but a lack of standardization remains a barrier to seamless cross-border identity verification.[7]

Perhaps no recent regulation better exemplifies this global impact than the EU's Markets in Crypto-Assets (MiCA) framework.

> The MiCA regulation, fully implemented in the EU in 2024, represents a landmark framework for harmonizing crypto regulations across all 27 EU member states. This comprehensive legislation requires crypto-asset service providers (CASPs) to implement strict KYC and AML procedures, making it the most stringent regulatory standard globally. Since cryptocurrency operations are inherently global and decentralized, CASPs worldwide must comply with MiCA to maintain access to European markets, effectively making it the new international gold standard for crypto regulation — similar to how GDPR shaped global data privacy standards.[8]

"When it comes to dealing with regulations across borders, there's a reason it's so complicated. The documents you use to travel and the cultural norms all differ, and local laws have to adapt to meet those needs.

Nuanced regulations across the globe make it even more challenging to put a compliance framework into place. For organizations looking to expand to a new country, I recommend stripping back your compliance program to the base level. Then you can see the commonalities across all of your jurisdictions, while recognizing any variations.

To do this successfully, you need a partner who can manage change at scale so you can operationalize the complexity of your policies and frameworks into day-to-day operations.

That level of flexibility means you can prove that your policies and operational process are in alignment. And if you can't? Your organization's finances and brand reputation can take a huge hit. In the industry, we typically see a 5.5% stock loss on the day a regulatory fine is announced, not to mention the cost of remediation. Damaging the brand is not an option."

Debra Geister
CEO, Section 2 Group

Regulatory changes may dramatically affect how businesses onboard and authenticate their users. The bottom line? **Both your business and your technology partners must be adaptable.**

7 | Forbes Technology Council. (2024, December 5). Identity verification in the digital-first world, part 1: Modern challenges. Forbes.
8 | Shufti. (2024, February 29). MiCA goes global: How to stay ahead with a future-ready compliance strategy. Shufti.

Digital divide: Bridging technology gaps

Despite the rapid growth in access to technology, countries vary widely in digital identity adoption. While Singapore has advanced digital systems, Myanmar still relies on paper-based documentation from the 1950s. This technological disparity requires solutions that can handle both cutting-edge and legacy document formats.

On the other end of the technology spectrum, Optical Character Recognition (OCR) systems must handle not only different languages but entirely different writing systems, contextual characters, and diacritical marks. Languages like Khmer (Cambodia), Tamil (Sri Lanka), and Thai don't use spaces between words, requiring advanced NLP and context-aware OCR to segment text correctly for accurate data extraction. Arabic-speaking countries present right-to-left text mixed with left-to-right numerals, requiring systems to handle bidirectional text processing.[10]

OCR technology must then go beyond extracting data from government-issued identity documents to support use cases such as tax documents, eSignature, or utility bills.

Considering the pace at which technology and fraud are evolving, businesses can't afford to wait for industry-wide adoption of new technologies, or spend months or years implementing cumbersome enterprise solutions.

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

The Architecture Behind Business Adaptability

This range of technology creates a ripple effect that goes beyond verification processes and into fundamental business model decisions. As governments begin to shift toward portable digital identities and decentralized KYC, gig economy verification, and cross-border financial services, business models and processes in the private sector must be able to keep up.

Flexible business models

Different markets require different business models and verification approaches. For example, adaptive authentication must dynamically adjust security measures based on contextual risk factors. Low-risk users experience a streamlined verification process, while high-risk transactions trigger additional authentication steps.

When exploring an expansion across borders, keep these variations in mind:

- Some markets may require on-premises solutions due to data sovereignty laws
- Fast verification is suited for high-volume, low-risk transactions
- Thorough checks are needed for regulated industries
- Alternative data verification may supplement where formal documentation is limited

Shifting paradigms

While technical flexibility forms the foundation, true global success requires adapting to evolving business trends that reshape how identity verification fits into broader strategies. Businesses around the world are evolving and adopting new processes and models that will drive additional requirements for identity verification.

User control of personal data

Historically, businesses have sought to own as much of their customers' data as possible to support marketing, analytics, and monetization. A combination of data protection regulations, consumer preferences and the emergence of digital identity wallets is causing a shift from data ownership to data stewardship. The shift demands robust identity management because businesses now prioritize responsible data handling over simply accumulating information.

Strong identity systems should enable precise control over how consumer data is collected, stored, and used, ensuring compliance with privacy regulations and honoring user consent. They also facilitate transparent data practices, allowing consumers to manage their preferences and access their data easily. Effective identity management helps link consent to individual profiles, supports data minimization strategies, and enhances security by reducing unnecessary data retention.

As reusable digital identity systems are adopted by consumers, businesses will also need to integrate these platforms to provide easy onboarding experiences, including support for consumer control of the data in their wallet. Reusable identity programs are starting exit development phases, prompting greater adaptability to these new emerging standards.

Rise of subscription purchase models

The success of subscription models such as Netflix, Spotify, or SaaS solutions and loyalty programs (airlines, retailers) makes persistent, accurate identity management critical. Identity management is crucial to subscription and membership models because it enables seamless, secure, and personalized customer experiences.

Accurate identity resolution ensures users can access their accounts across devices, manage preferences, and receive tailored content or offers. It also supports secure payment processing, account recovery, and fraud prevention. As consumers around the world expect convenience and personalization, businesses must maintain unified customer profiles while complying with privacy regulations.

Effective identity management allows companies to analyze user behavior, optimize retention strategies, and deliver value-added services. Without strong identity systems, businesses risk poor user experiences, increased churn, and challenges in scaling their subscription or membership models.

Monetizing first-party data

As third-party cookies fade away, companies are monetizing their authenticated user bases and first-party data on those users. Large retailers are creating retail media networks (RMNs) to turn their ecommerce websites into an advertising platform. RMNs rely heavily on robust consumer identity management. They use first-party data — like purchase history, loyalty programs, and browsing behavior—to accurately identify and target shoppers across devices and channels.

This requires precise identity resolution to link actions to individual consumers while maintaining privacy compliance and consent management. RMNs help brands deliver personalized ads directly where permissible within a retailer's ecosystem, enhancing ad relevance and driving conversions. Strong identity management ensures that ads reach the right consumers at the right time, while also respecting data privacy laws and evolving consumer expectations around data use. In these environments it will be key that RMNs and their merchants can share or reuse identities, under user control, to help merchants build relationships with RMN consumers.

Bringing customer identity verification and workforce IAM together

Traditionally, the systems used to manage customers and employees have been separate. But the line between customers, employees, gig workers, and contractors is blurring. This is in large part because the identity data and regulations that govern user data are so similar. It only makes sense that businesses will look to create unified identity platforms that can handle any type of data. Further unifying these platforms will simplify infrastructure, create a better user experience (especially for users who are both customers and part of the organization's global workforce) and reduce costs.

With industry-specific flows, you can customize without compromising. Whether that's gaming platforms that require age verification, fintechs that need AML screening, or marketplaces confirming seller and user identities, every industry is full of nuances.

The Ultimate Adaptability Solution

There's one common goal when it comes to international business expansion: expand to your most profitable markets, and be able to verify every target customer. Achieving this goal requires supporting the full spectrum of identity documents, from handwritten documents and tax documents, to unconventional IDs and non-Latin scripts.

Adaptable technology infrastructure

To be truly adaptable, you need a platform that has infinite possibilities and customizations. This can look like:

Integration flexibility: From no-code options for rapid deployment to full API access for custom implementations, businesses need choices like no-code integration for teams with limited technical resources, mobile SDKs (Android, iOS, Flutter, React Native, Cordova) for app-based verification, web-ready solutions that maintain brand consistency, full RESTful API access for complete customization, and on-premise implementations for data-sensitive industries.

Workflow adaptability: The ability to reconfigure customer interaction workflows nearly instantaneously is critical to adapting to new compliance requirements or fraud patterns without disrupting operations. These workflows must account for cultural naming structures that vary dramatically — Ethiopia includes patronymic names, Libya includes tribal affiliations, Japan follows surname-first convention, and Myanmar may include monastic or royal titles.[10]

Scalability: Solutions should support high-volume transactions while maintaining strict security controls, with the ability to handle thousands of types of ID documents spanning hundreds of countries and many languages.

CASE STUDY HIGHLIGHT

Why adaptability matters

A global social media company was concerned over user privacy and the potential for inappropriate use of its live-streaming capabilities, as well as the risks of unauthorized account access.

When users fell victim to account takeovers, it not only led to a loss in trust but also raised accountability issues regarding live-streamed content. Traditional authentication methods, such as passwords and one-time passcodes (OTPs), were not sufficient. The company needed an advanced, IDV-based authentication system that provided a verified, traceable identity for each user session.

To address these concerns, the company turned to Shufti for verification, ensuring that only the registered account owner could access and use the live-streamed capabilities. By implementing Shufti, the company effectively reduced account tampering, strengthened authentication security, and assured content accountability. When this customer needed identity verification for its Buy Now Pay Later business line, Shufti was able to support both use cases from the same platform.

10 | Shufti. (2025). The Top 10 Most Difficult Countries for Identity Verification.

Real-world success From India to the World:
BigCash's Global Expansion

THE CHALLENGE

Scaling identity verification across 50+ countries

When India's leading gaming platform, Witzeal Technologies, decided to expand its BigCash offering beyond India, the company faced a critical challenge: scaling from 40 million domestic users to a global audience — all while maintaining compliance with diverse international regulations. With 1.5 million monthly active users, any unnecessary friction in the onboarding process would be unacceptable.

The gaming industry's regulatory landscape varies dramatically across jurisdictions. Witzeal needed a solution that could adapt to each country's requirements while preventing fraud — without disrupting the user experience.

THE SOLUTION

AI-powered adaptive verification

Witzeal partnered with Shufti to implement an AI-driven identity verification system with three critical capabilities:

Automated perpetual KYC: Continuous monitoring that detects fraud without interrupting gameplay

High-speed processing: Verification within seconds to maintain user flow

Localized compliance: Automatic adaptation to regulatory requirements across 50+ countries

THE RESULTS

95% fraud risk reduction

- Successfully expanded to 50+ countries while meeting each jurisdiction's KYC standards
- Achieved up to 95% reduction in fraud risk
- Maintained compliance with emerging regulations, including India's DPDPA requiring on-premise data storage
- Eliminated manual review bottlenecks, reducing operational costs

"Partners like Shufti have been the backbone of our expansion. We use Shufti IDV across all 50 countries where we operate,"

- Ketan Godkhindi
Chief Strategy Officer,
Witzeal Technologies

Future-proofing your business from fraud threats

Apart from compliance challenges, organizations face a whole other headache: an escalating threat landscape.

Fighting back against AI-powered fraud

According to Forbes, deepfake attacks occur every five minutes, making up 40% of all biometric fraud.[11] Shufti has observed a 244% increase in account takeovers and identity fraud driven by generative AI — and these numbers will only continue to grow.

And when fraudsters encounter barriers, they don't just stop — they evolve their tactics, reusing successful deepfake templates and creating patterns that only AI can detect.

Proactive compliance and fraud controls

Bad actors often exploit gaps between jurisdictions, moving operations to regions with weaker enforcement. In response, regulatory agencies are building stronger cross-border frameworks and secure data-sharing mechanisms. Organizations must not only keep up with individual regulations, but have an eye on the regulations across all of your jurisdictions.

Built-in flexibility for emerging identity paradigms

Besides addressing today's threats, organizations must plan for what they don't know is coming.

Consider cryptocurrency: what began as a fringe technology now requires sophisticated KYC processes that vary dramatically by jurisdiction. To stay ahead, organizations must stay nimble.

11 | Vakulov, A. (2025, March 9). Deepfake scams are stealing millions—How to spot one. Forbes.

Choosing the Right Partner for International Growth

Global expansion demands more than just technology — it requires a partner who understands that identity verification challenges vary by market, industry, and use case.

The world's most sophisticated tools are worthless without the flexibility to respond to changing regulations and evolving threats. The ability to reconfigure workflows by region, product, or service with low or no-code options is key to successful global expansion.

When evaluating global identity verification solutions, here are the key capabilities that support regulatory adaptability:

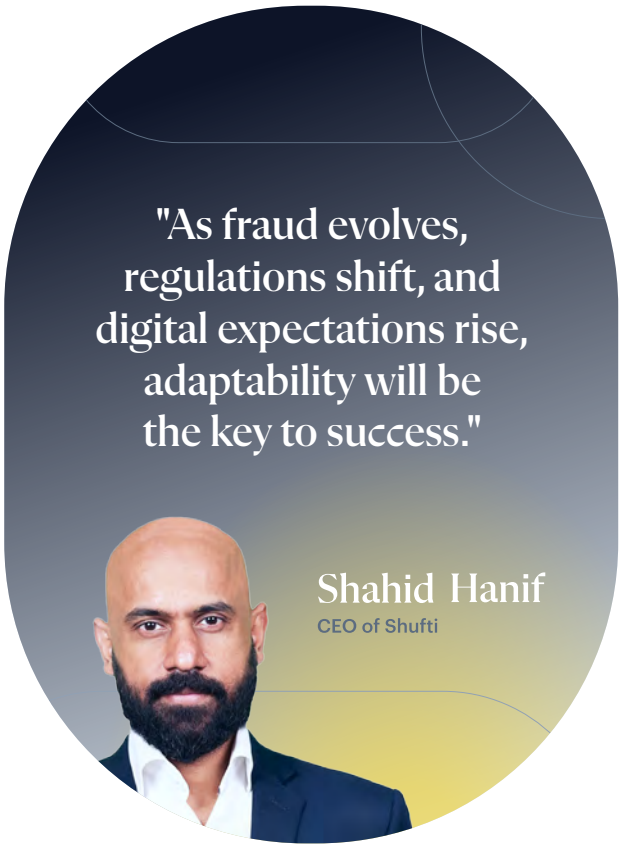
- **True multi-market capabilities** (not just multi-language support) with an emphasis on accepting more good customers and declining more fraud
- **Flexibility** in deployment and integration
- Understanding of **local compliance** requirements
- **Ability to handle** edge cases and unusual documents
- **Track record** of successful international implementations

Build Your Global Expansion Roadmap With Shufti

Your identity verification systems should accelerate growth — not become the bottleneck that costs you customers and revenue.

When organizations work with Shufti outside their home market, they typically see a 30% increase in customer acceptance rates.

This isn't just about technology — it's about understanding that success in Hong Kong requires more than translating your German verification process.



Global expertise

With coverage spanning 240+ countries and territories, supporting 150+ languages and over 10,000 document types, we've built our own OCR technology specifically to handle the world's most challenging documents — from handwritten documents in India to complex naming structures in Ethiopia.

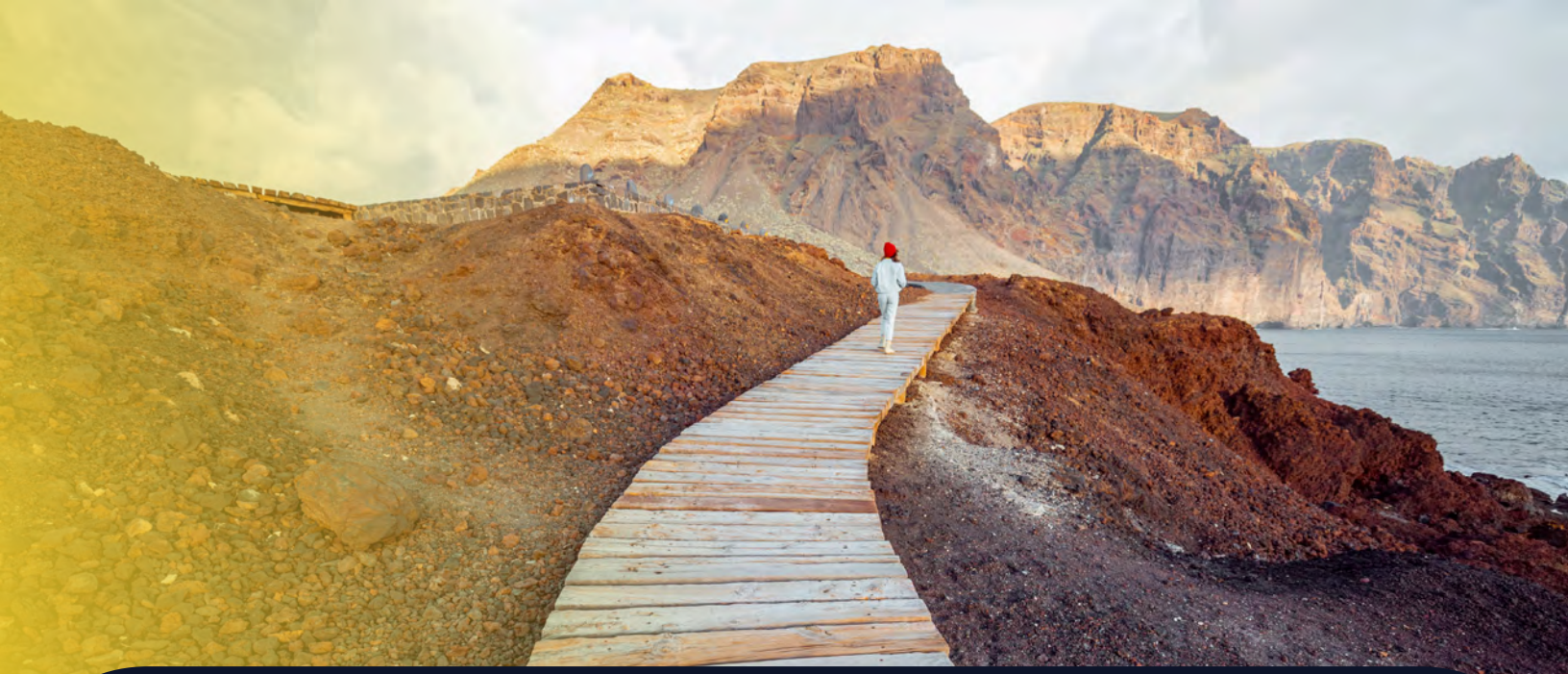
Beyond traditional verification

While legacy vendors remain locked into passport-only verification, Shufti handles unconventional documents, alternative data verification, and industry-specific requirements.

Rapid customization at scale

What typically costs hundreds of thousands with other providers, Shufti delivers at a fraction of the price. Our engineering team works closely with customers, allowing you to adapt to new markets or regulations in days, not months.

Whether it's on-premise deployment for data sovereignty or cloud-based solutions, we'll configure our solution to meet your needs.



The Path Forward

Adaptability is not just a feature — it's a necessity.

From AI-powered fraud detection to evolving regulatory frameworks, we ensure your growth never stalls due to identity verification limitations.

Identity Verification, Your Way

Discover Shufti's full identity platform through interactive demos. No forms, No sales calls. Just the product, on your terms.

Explore the Demo Center

WWW.SHUFTI.COM

Shufti