Shufti

WHITEPAPER

The KYC Compliance Challenge Across APAC

Identity Verification for Changing Fraud and regulatory landscape

Table Of Contents

The Shape Of The Problem

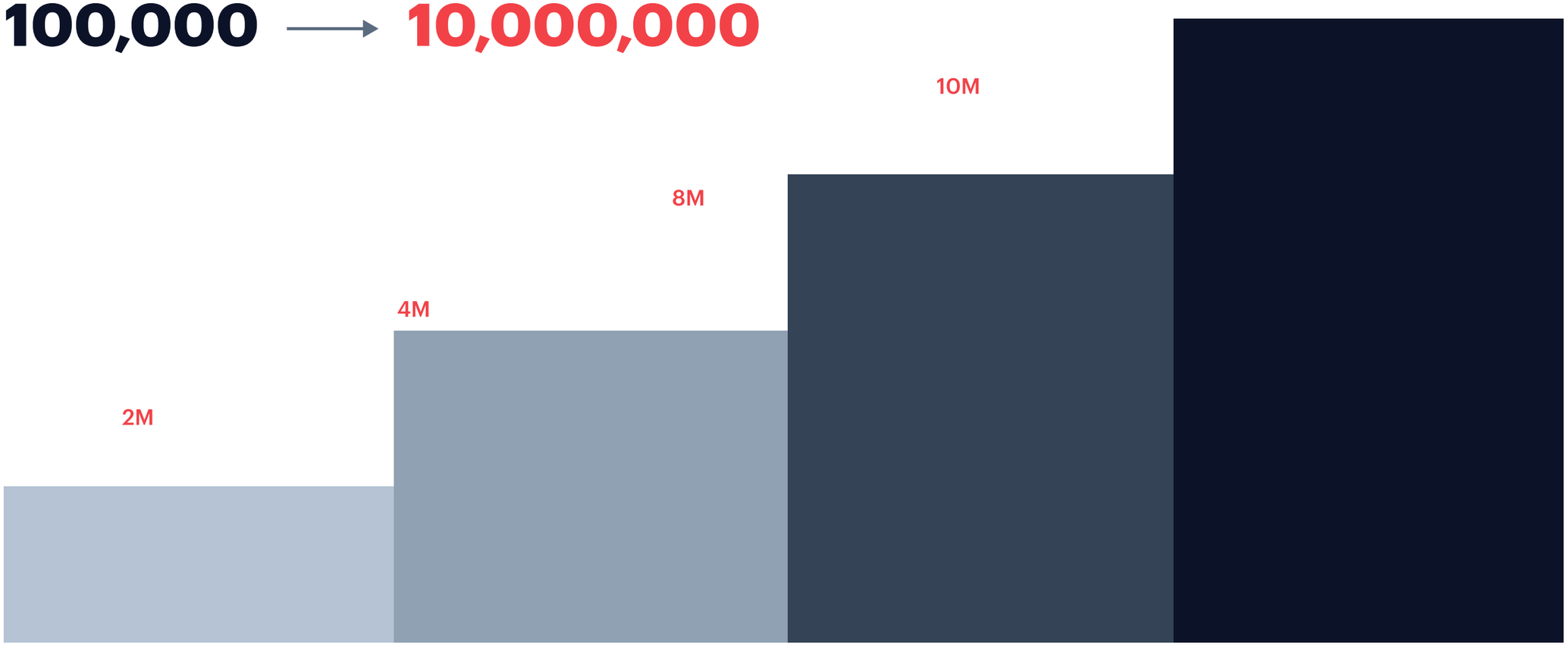
Asia-Pacific Is Generating More Of The World's Economic Growth Than Any Other Region, And The Faster Its Digital-First Businesses Scale, The More Identity Fraud They Attract And The Harder Regulators Scrutinise Them. Most Of Them, Though, Run On Identity Verification Infrastructure That Cannot Keep Pace With That Growth Or Verification Volume, Leaving New Acquisition And Customer Retention Exposed To Mounting Fraud And Compliance Pressure.

APAC continues to contribute nearly 60% of global growth, reinforcing its role as a key driver of the global economy.[1] Social commerce is becoming mainstream across the region, with influencer-driven purchasing2 behaviour and in-app shopping adoption accelerating across its mobile-first, creator-led commerce ecosystem. UPI in India now accounts for roughly half of all global real-time payment transactions.[3] Digital public infrastructure adoption across Asia continues to accelerate at population scale. Singapore's Singpass facilitates over 41 million digital transactions each month,[4] and India's DigiLocker supports more than 620 million users with over 9.5 billion issued digital documents.[5]

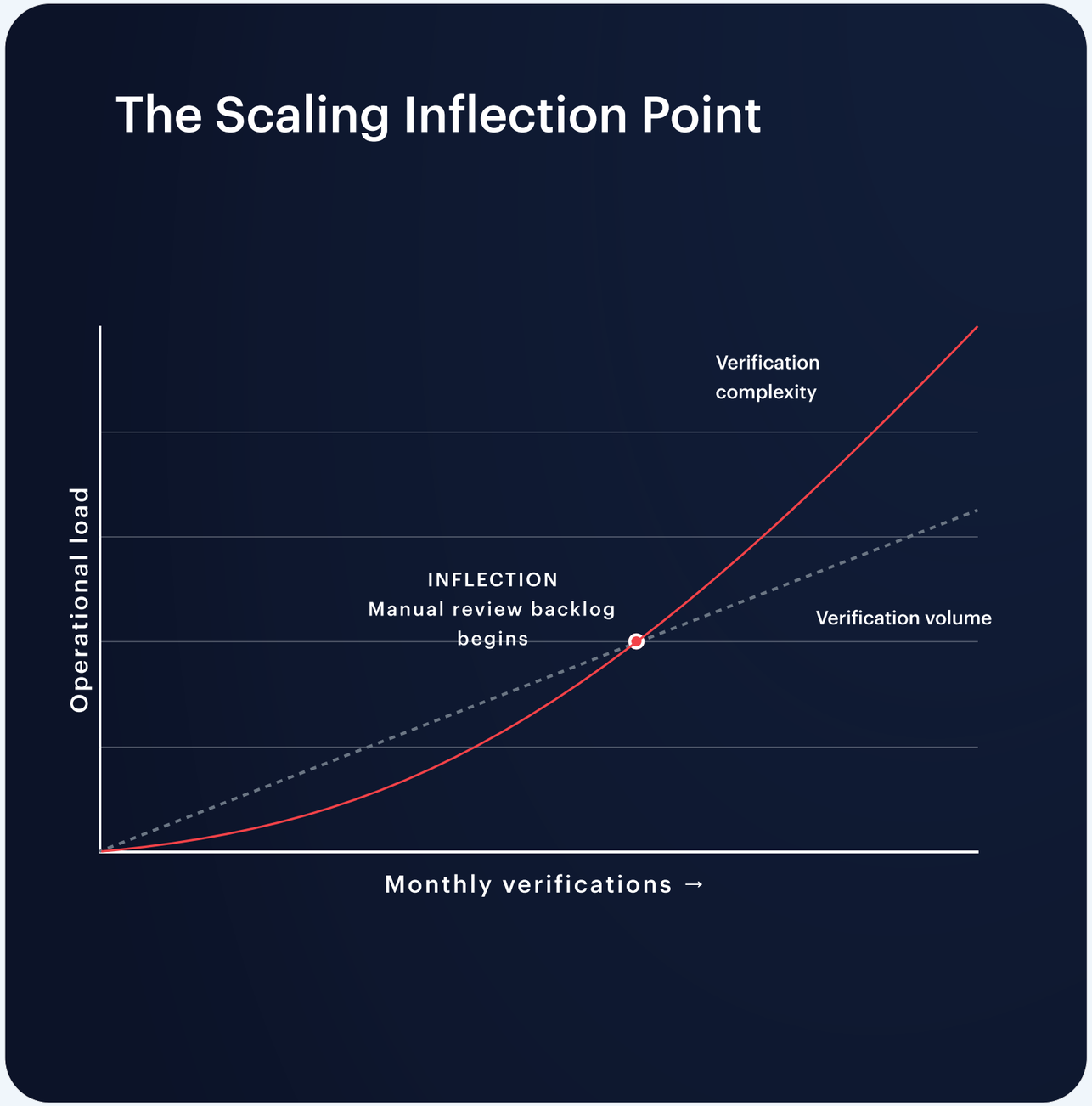
Every one of those numbers is a verification moment that strengthens the foundation of trust in the digital-first world: account openings, KYC refreshes, age-gated purchases, payment authentication, lending decisions, marketplace seller onboarding. Each one is a place where a business has to decide, in milliseconds, whether the person on the other end is who they claim to be — and increasingly, whether they are a person at all.

SCALING ACOSS MARKET

100,000 → **10,000,000**



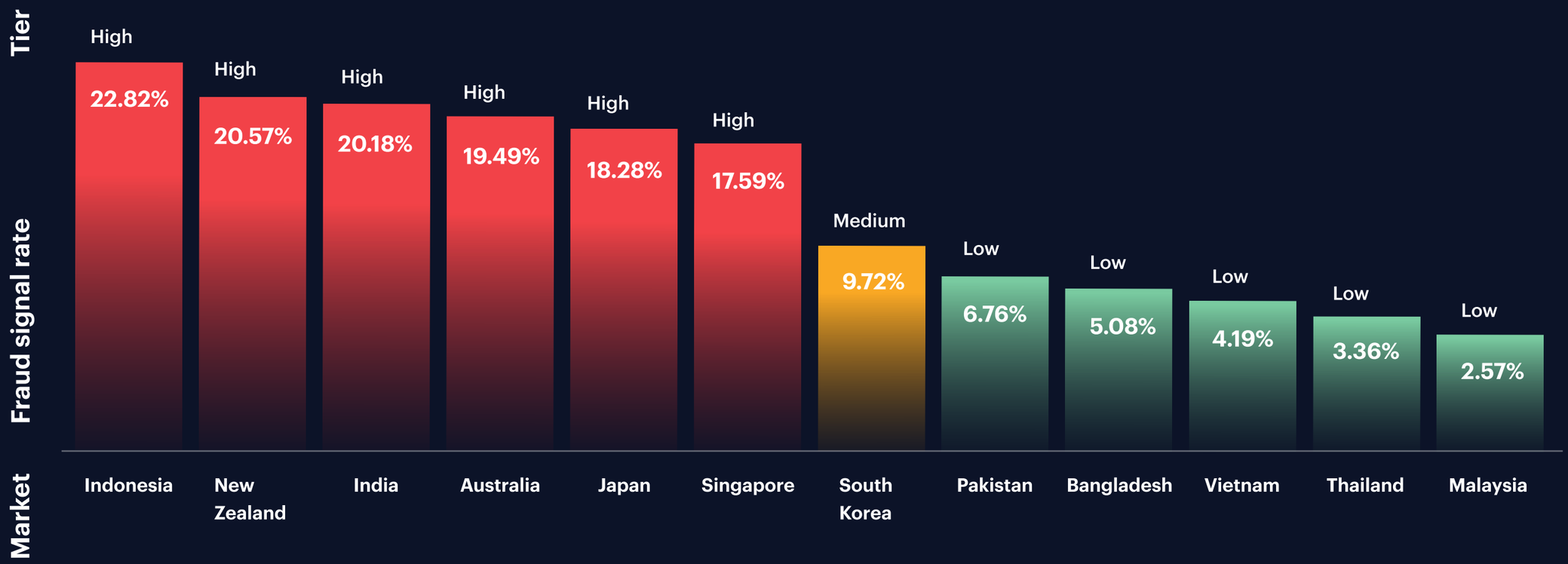
Verifications a business may need to handle within a year as it scales across three or four APAC markets. An identity verification solution used for low-volume onboarding environments is unlikely to meet the performance, accuracy, or compliance demands of high-volume markets at scale.



As a digital first business grows, the number of identities it has to verify keeps rising. But growth does not only mean more checks. It also means more kinds of fraud. The bigger and more visible a business becomes, the more fraudsters try to get through, and they keep finding new ways to do it. At the same time, regulators start to expect more. The rules for onboarding customers remotely become stricter and harder to meet, and they often differ from one market to the next. So the business is not just doing more verifications. It is doing harder ones, against more threats, under tougher rules. This is where a rigid IDV vendor begins to hold the business back. A fixed system can handle the checks it was built for, but it cannot easily adjust when new fraud patterns appear or when a regulator changes what is required.

Digital Maturity And Fraud Exposure In APAC Markets

According to Shufti's internal verification data fraud across APAC is not evenly distributed, and this is evident from the pattern which emerges from the data. In a sample of identity verification data spanning APAC countries, the highest fraud-rates per 1000 verifications appear in some of the region's most digitally mature economies, not in the markets most readers would intuitively expect.[6]



Methodology

How the fraud rate is defined here

The fraud rate represents the proportion of verification requests where the submitted identity documents failed authenticity, originality, or integrity validation checks and were consequently declined by the verification system. A document is flagged as fraudulent when at least one of three checks fails: Authenticity asks whether the document appears to be a genuine issuance from a legitimate authority; security features, layout, fonts, MRZ checksums, document-number formats, and visual design are checked against known specimens for that issuing country and document type.

Originality asks whether the submission is a first-generation document presented to the camera, rather than a photo-of-a-photo, a screen recapture, a printed scan, or a digitally re-rendered version. Integrity asks whether the document has been tampered with after issuance, field-level edits, photo substitution, font inconsistencies, compression artefacts inconsistent with single-pass capture, and metadata anomalies.

Figures are aggregated by country of document issue across multiple client businesses operating in different sectors. They are not directly comparable to payment-fraud rates, scam-loss statistics, or confirmed-fraud disclosures published by other vendors, which use different definitions. Patterns in this sample may not generalise to other vendors' books of business.

The pattern is notable. Several highly digitised APAC economies, including Singapore, which ranks among the world's leading economies on the IMD World Digital Competitiveness Ranking, alongside Japan, also appeared toward the upper range of fraud-signal activity within this sample.[7] Thailand, Malaysia, Vietnam, and Bangladesh, with less developed digital infrastructure, sit at the bottom. The most likely explanation is not that mature economies are uniquely vulnerable, but that digital maturity and the density of digital-first businesses doing identity verification scale together. More businesses running remote KYC means more attack surface, more attempts, and a higher share of fraudulent attempts captured at the verification step. The relationship in this sample is likely to hold for similar verification businesses in similar segments, but may not generalise to consumer-payment fraud, scam losses, or other fraud categories with different dynamics.

Why Businesses In APAC Face Challenges With Identity Verification As They Scale

Most identity verification stacks were built around assumptions that hold in markets with a single national alphabet, two or three primary document formats, and one or two regulators per country. APAC breaks all of those assumptions simultaneously.

Consider the challenges for remote identity verification in the region. Names appear in Latin script, in Devanagari, in Khmer, in Burmese, in Tagalog with Spanish-influenced spellings, in Vietnamese with full diacritics, in Thai with tone markers, in Korean Hangul, in simplified Chinese characters, in traditional Chinese characters, in Japanese with three concurrent scripts (kanji, hiragana, katakana), in Urdu for Pakistani populations, and in Cyrillic for Mongolian and Kazakh contexts.

Address conventions vary fundamentally, with Japan and Korea running addresses largest-unit-first, unlike Western conventions where the street name appears first, while Vietnam's addresses have just been restructured wholesale by a 2025 provincial reform.

Non-Latin Scripts Create CRM And Sanctions Database Mismatches

Thai And Khmer Scripts:

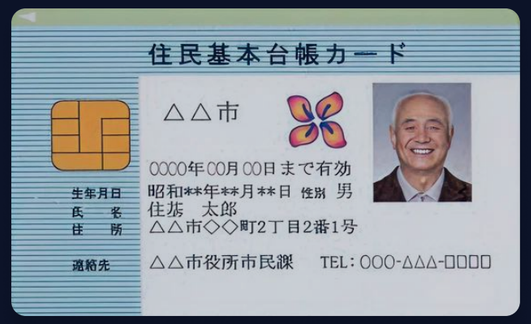
written without spaces between words, which makes segmentation hard for OCR and entity-matching, so platforms struggle to extract names and addresses cleanly for comparison against CRM, AML, or sanctions databases.

Japan:

documents mix kanji with phonetic scripts (hiragana, katakana), and dates may use imperial eras such as Showa, Heisei, or Reiwa rather than the Gregorian calendar. Without proper normalisation, OCR can misread date-of-birth fields or generate inconsistent records downstream.

Japanese Documents In Three Different Scripts:

Hiragana



Katakana

Kanji

Korea:

names romanise inconsistently across systems, appearing as Park, Pak, or Bak depending on the standard used by passports, regulators, or sanctions lists, which raises both false positives and false negatives during watchlist screening.

Cambodia And Myanmar:

Cambodian IDs may carry dates and numerals in Khmer script, while Myanmar IDs use Burmese script with handwritten or semi-structured fields and vary by region in format, print quality, and field placement, so Latin-first OCR struggles to extract and normalise them.

India:

KYC is anchored on Aadhaar and PAN, with Passport, Voter ID, Driving Licence, and the NREGA job card also accepted, and Aadhaar is issued bilingually, pairing English with a regional script (Hindi, Tamil, Bengali, Telugu, and others) by the holder's state and language.

The Diversity In Identity Documents Cascaded Into Business Problem

A verification engine that cannot reliably process the diversity of APAC documents, scripts, and address formats does not just produce friction at the verification step, it caps the markets a business can credibly serve. Compliance teams cannot sign off on onboarding flows that reject legitimate customers at scale or pass forgeries through; product teams cannot launch in markets where the verification stack fails on a meaningful share of real applicants.

Most vendors respond by stitching together a patchwork of regional add-ons: document verification for the first market, say Vietnam, licensed from one vendor, the second market, say Japan, from another, and the third from someone else again. Every new geography means onboarding yet another supplier, and that dependency creates bottlenecks in expansion The resulting "frankenstack" carries its own compliance hazards. Customer data routed through multiple sub-processors expands the surface area for a security breach, multiplies the privacy notices and data-processing agreements a business must maintain, and complicates data-residency and cross-border transfer obligations that vary significantly market by market.

The business consequence is structural: not just friction on real customers or gaps for attackers, but a hard ceiling on regional expansion.

Evolving KYC Regulations Across APAC

India:

RBI's Master Direction on KYC, updated in August 2025, significantly strengthened V-CIP expectations around spoof detection, liveness verification, and fraudulent-manipulation detection, raising the bar beyond basic blink-and-smile liveness checks toward more robust presentation-attack and deepfake-resistant controls.[8]

Singapore:

MAS' September 2025 Information Paper, Cyber Risks Associated with Deepfakes, raises supervisory expectations around AI-generated identity fraud, synthetic media, and remote-onboarding integrity. It places particular emphasis on securing non-face-to-face verification workflows against manipulated video, impersonation, and deepfake-enabled attacks.[9]

Malaysia:

Bank Negara's e-KYC Policy Document, revised in April 2024, legally mandates liveness detection within the digital onboarding framework, with prescribed FAR/FRR thresholds and independent assessment of document verification, biometric matching, and liveness modules.[10]

Philippines:

BSP's eKYC framework (Circular 1170) has accelerated remote-onboarding adoption, with biometric liveness verification and PhilSys integration becoming central to higher-assurance digital identity workflows.[11]

Hong Kong:

In a 30 May 2025 circular, the SFC expanded acceptable non-face-to-face onboarding approaches by formally recognising iAM Smart, broadening digital certification mechanisms, and supporting biometric ePassport verification for overseas onboarding.[12]

China:

The amended Anti-Money Laundering Law, effective 1 January 2025, introduces mandatory beneficial-ownership identification, with the regulatory perimeter widened to additional non-financial sectors.[13]

Australia:

The AML/CTF Amendment Act 2024 (Royal Assent 10 December 2024) brings lawyers, accountants, and real-estate professionals into mandatory IDV from 1 July 2026, with existing reporting entities required to comply from 31 March 2026.[14]

Administrative reforms move just as quickly and create entirely separate operational headaches. Vietnam's 1 July 2025 restructuring, formalised through Resolution 60-NQ/TW and Resolution 125/NQ-CP, merged 63 provinces into 34 first-level subdivisions and eliminated the district tier entirely, invalidating address fields across millions of existing identity documents overnight.[15] Legacy and current formats coexisted during the transition. Verification systems built around fixed templates could not process the new structure; legitimate customers were rejected at onboarding while fraudulent documents went unchecked during the operational gap.

The detailed implications are covered in the case study at the end of this paper. The pace and prescription combined mean that any vendor running on third-party engines it does not fully control, will perpetually be a quarter or two behind what regulators in the region actually require.

The Evolving Fraud Threat In APAC

Regulation is moving fast because the attacks are moving faster. The fraud environment APAC verification systems operate in now is unlike anything they were originally designed for.

+600%

Increase in deepfake-related content tied to criminal activity in Southeast Asia, H1 2024, per UNODC.[16]

USD 25M

Hong Kong Arup deepfake video-call fraud loss.[17]

USD 4B+

Estimated laundered via Cambodia-based Huione Group, Aug 2021–Jan 2025 (FinCEN).[18]

Deepfakes And Synthetic Identity Fraud:

The APAC Threat Landscape

Deepfakes have moved well beyond experimental novelty into operational fraud infrastructure, and nowhere is that shift more alarming than in Asia-Pacific, now one of the hardest-hit regions globally.

AI-Enabled Fraud Is Scaling Rapidly Across The Region

UNODC's reporting on AI-enabled cybercrime in Southeast Asia documented a major increase in the use of synthetic media and AI-driven fraud tooling during 2024[19] Dark-web marketplaces now advertise synthetic identity kits containing AI-generated avatars, cloned voices, forged identity templates, and biometric artefacts designed specifically to target onboarding and authentication workflows.

High-Profile Cases Signal A Wider Pattern

The Hong Kong Arup case, in which an employee transferred approximately USD 25 million following a deepfake-enabled video call impersonating senior executives, remains one of the most widely publicised examples.[20] Chinese authorities have also reported AI face-swap and manipulated-video fraud incidents involving substantial losses, including a police-disclosed case in which a victim was defrauded of 4.3 million yuan (around USD 610,000) through a single deepfake video call.[21]

Malware And Evolving Attack Techniques Compound The Risk

Researchers across parts of Southeast Asia have identified malware campaigns capable of harvesting video, audio, and biometric information later repurposed for onboarding fraud and authentication-bypass attempts. Fraud techniques are evolving rapidly enough that liveness models considered state-of-the-art only a short time ago may now perform inadequately against newer presentation-attack and deepfake variants.

Synthetic Identity Fraud Is Becoming Industrialised

UNODC has identified AI-generated documents and synthetic identity tooling as major enablers of cyber-enabled fraud across the region, particularly as these methods challenge template-based verification and legacy fraud-detection systems.[22] FATF's report on illicit financial flows from cyber-enabled fraud similarly highlighted forged and altered identity documents as significant facilitators of laundering activity globally.[23]

Scam Compounds Are Sustaining Organised Fraud Ecosystems

Pig-butchering operations and cyber-scam compounds remain heavily concentrated across parts of Southeast Asia. UNODC's April 2025 report, Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia, documented the continued industrialisation of cyber-enabled fraud ecosystems spanning Cambodia, Myanmar, and Laos, where large organised scam networks have been linked to romance scams, fake investment platforms, identity-construction services, and large-scale social-engineering operations targeting victims worldwide.[24]

Different Sectors, Same Point Of Origin

Different sectors absorb different parts of this threat surface. Fintechs and digital banks face mule-account creation and SIM-swap-enabled account takeover at scale; crypto exchanges encounter synthetic identity construction and Travel Rule evasion; digital lenders face forged income proofs and ghost-lending schemes; dating platforms become origination points for romance scams; forex platforms encounter investment-scam mule accounts; iGaming operators face multi-account abuse and underage onboarding; and social-commerce marketplaces deal with fraudulent seller onboarding. The common thread is that many of these risks originate at the verification layer itself.

Why Identity Verification Vendors Fall Short In The APAC Market

Digital-first businesses across Asia-Pacific feel this environment of script complexity, regulatory volatility, and industrial-scale fraud most through their identity verification vendor, the one thing that should be enabling growth but often constrains it instead, unable to keep pace with evolving fraud or to support a clean move into new markets. It usually comes back to three problems that feed into each other:

They Don't Actually Own The Core Of What They Sell

A lot of vendors license their OCR from one company, their face match from another, and advanced deepfake detection from another. When a regulator pushes through a new reform, a fresh deepfake typology appears, or presentation attack detection needs hardening, the vendor without in-house tech and R&D teams available at its disposal. It has to go back to whichever supplier owns that piece, wait for them to act, and stitch the update in afterwards while the market keeps moving and it is still assembling the parts it does not control.

Their Engines Were Never Built For The Documents People Actually Carry Here

Most OCR systems are trained on Roman alphabets and standardised Western identity documents, making them less effective in Asia's multilingual environment. Scripts such as Devanagari, Bengali, Thai, Khmer, Chinese, Hangul, Urdu Nastaliq, and Vietnamese behave very differently from Latin text. Combined with the region's vast variety of IDs, passports, and residence permits, many verification vendors still rely on third-party providers to process unsupported documents

They Can't Adapt Fast Enough To Keep Up With The Fraud

Threats in Asia don't stand still. Deepfake injection, synthetic identities, and forged document templates keep evolving, yet many vendors run static detection engines they rarely retrain or meaningfully update. A model tuned for last year quietly goes blind to this year's attacks. By the time anyone gets around to refreshing it, the fraud has already changed shape, leaving the business to defend against a threat the system was simply never taught to recognise.

The Cost Of Getting KYC Wrong

01

Onboarding Friction Functions As A Structural Tax On Growth

The customer who never completes the verification flow represents the largest revenue impact in digital financial ecosystems, yet it is the one most businesses fail to measure. Friction at the verification stage drives customer abandonment, delays activation, and weakens institutional trust, compounding quietly as a recurring drag on acquisition and lifetime value rather than appearing as a single, visible loss event.

02

Trust Loss Is The Least Measurable Consequence, But The Most Strategically Damaging

A digital bank whose customers discover their identities have been cloned and used to open fraudulent accounts loses something no compliance budget can recover. Trust does not respond to remediation the way a regulatory penalty does. Critically, the corollary is equally measurable: frictionless onboarding correlates with materially higher customer acquisition and retention, making a smooth verification flow a growth asset, not merely a compliance overhead.

03

Regulatory Penalties Are Rising Across APAC, And Financial Exposure Is Significant

Singapore's 2023 money-laundering case, involving more than SGD 3 billion in seized or frozen assets, triggered MAS supervisory action and composition penalties totalling S$27.45 million against nine financial institutions in 2025. Across APAC, Australia's expanded AML/CTF regime has materially increased potential exposure, while RBI, MAS, BSP, and BNM have all strengthened onboarding governance expectations , simultaneously driving up the operational cost of compliance.

04

Operational Fraud Losses Are Less Visible, But Often Larger In Aggregate

Mule accounts opened under failed verification feed pig-butchering schemes, investment scams, and large-scale laundering operations. Synthetic identities are used to take out loans that default, while deepfake-impersonated accounts trigger emergency wire transfers that cannot be recalled. Every dollar of fraud that passes through a failed verification checkpoint typically costs multiples in downstream investigation, restitution, and regulatory engagement.

Choosing The Right IDV Vendor For APAC

The right identity verification vendor for businesses in APAC is one that adapts continuously to the region's regulatory velocity, evolving fraud landscape, and the new market requirements that come with every stage of growth.

The APAC IDV Vendor Checklist

- Does the vendor own its tech stack so it can customize quickly for new regulations, risks and fraud without bottlenecking your growth?
- Does the vendor efficiently supports expansion to new markets?
- Can the vendor hold accuracy, speed and automation steady as verification volumes and fraud pressure both rise?
- Can the vendor's OCR accurately extract and verify diverse APAC documents and non-Latin scripts, and normalise transliterated data for CRM consistency?
- Does the vendor offer doc-less and eIDV coverage across APAC that delivers higher conversion in regional flows?
- Does the vendor catch synthetic identity and organised fraud through multiple tools without blocking legitimate customers?
- Does the vendor own its tech stack so it can customize quickly for new regulations, risks and fraud without bottlenecking your growth?
- Does the vendor provide a higher level of assurance in authentication for high-risk and step-up scenarios?
- Does the vendor continuously adapt as threat typologies evolve?
- Does the vendor offer continuous identity verification to prevent fraud across the customer lifecycle?

Shufti's Approach

Shufti was built on this architectural principle. The OCR, document authentication, biometric matching, liveness, and deepfake-detection engines are all developed and maintained in-house. The document library covers over 10,000 documents across more than 240 countries and territories, including the regional variants that determine whether APAC verification flows actually work. Because the technology is in-house, the solution can verify the edge cases businesses meet during expansion. The fraud-detection layer is trained continuously on the attack patterns the platform sees across its global client base, and APAC-specific fraud signals feed back into the same models. The solution balances verification accuracy with response time through continuous collaboration with clients, while actively monitoring the threat landscape and evolving regulations.

What this means operationally is best illustrated by two recent examples.

Case study

Vietnam

administrative restructuring and the address-logic problem

In April 2025, Resolution 60-NQ/TW approved a shift to a simplified two-tier administrative structure. The district level was abolished entirely, leaving Province/City to Commune/Ward as the official hierarchy. Resolution 125/NQ-CP then reduced the number of provincial-level units from 63 to 34. Regions were merged, renamed, and reorganised, and new administrative codes were issued. These changes became effective nationwide on 1 July 2025. However, Vietnamese identity documents still frequently display the old three-tier structure, while government databases now follow the new system. KYC vendors that have not updated their address logic continue to check customer data against obsolete hierarchies. The result is systematic address mismatching: legitimate addresses fail validation because the system treats them as inconsistent, even though they are technically correct within Vietnam's evolving framework. This is exactly the kind of adaptation that demands an in-house verification stack evolving on a single roadmap.

During the transition period, Shufti's OCR engine sustained 96.79% field-level accuracy on the new chip-based citizen ID format, while a comparable third-party engine benchmark in the same window measured 82.36%. The 14-point gap matters: at typical regional onboarding volumes, that delta translates to thousands of additional rejected legitimate customers per month for the lagging vendor, alongside corresponding gaps for fraudulent documents that template-mismatched engines failed to flag.

96.79%

82.36%

Shufti OCR Accuracy Versus A Comparable Third-Party Engine Benchmark On Vietnam's New Chip-Based Citizen ID Format

Case study

Japan

multi-layer fraud detection breaking a coordinated network

A criminal network targeting a leading Japan-based crypto exchange submitted multiple slightly altered originals of the same underlying identity documents, presenting each submission as a distinct customer onboarding. The pattern reflects how fraud now arrives in the region: not as isolated single applications, but as coordinated waves engineered to look independent at the document layer.

Shufti verifies the diversity of documents the region actually carries, across non-Latin scripts and fast-changing national formats, and routes verification through eIDV and doc-less flows wherever national digital identity rails exist, already supporting Aadhaar via DigiLocker in India, Singpass in Singapore, ConnectID in Australia, and PhilSys in the Philippines, with coverage widening as new rails come online.

As deepfake attacks on remote identity verification systems evolve, the fraud-detection layer is retrained continuously rather than left static, while device fingerprinting and IP intelligence link coordinated attempts that look independent at the document layer. Age verification runs through the same platform, so businesses entering age-gated markets add a control without adding a vendor. Because every layer is in-house and on a single roadmap, a business can move into new markets, meet new regulatory mandates, and absorb new fraud typologies without re-architecting or stitching in third parties.

Seamless Verification And Fraud Prevention Across APAC

So how does a digital-first business in APAC stay on its growth trajectory while keeping pace with a fraud and regulatory landscape that shifts by the quarter? It is because in-house tech and R&D teams give it an edge to do quick customization as fraud evolves and the new regulatory requirements emerge.

Shufti verifies the diversity of documents the region actually carries, across non-Latin scripts and fast-changing national formats, and routes verification through eIDV and doc-less flows wherever national digital identity rails exist, already supporting Aadhaar via DigiLocker in India, Singpass in Singapore, ConnectID in Australia, and PhilSys in the Philippines, with coverage widening as new rails come online.

As deepfake attacks on remote identity verification systems evolve, the fraud-detection layer is retrained continuously rather than left static, while device fingerprinting and IP intelligence link coordinated attempts that look independent at the document layer. Age verification runs through the same platform, so businesses entering age-gated markets add a control without adding a vendor. Because every layer is in-house and on a single roadmap, a business can move into new markets, meet new regulatory mandates, and absorb new fraud typologies without re-architecting or stitching in third parties.

Shufti, By The Numbers

The operational baseline Shufti delivers in APAC production today.

230+

Countries and territories covered

10,000+

Document types verified without manual template creation

150+

Languages processed with native accuracy

< 30s

Average verification speed

98.67%

Accuracy rate across document types and languages

1. IMF, Regional Economic Outlook: Asia and Pacific, October 2025.
2. PayPal, “The Rise of Social Commerce: Trends to Watch”
3. Government of India / PIB, citing ACI Worldwide (“Prime Time for Real-Time”) and IMF, June 2025: UPI holds roughly a 49% share of global real-time payment volume. pib.gov.in
4. GovTech Singapore, Singpass product page (over 41 million transactions per month). Figure as published by GovTech
5. DigiLocker / Ministry of Electronics and IT (India).
6. Shufti internal dataset — aggregated identity-verification fraud-signal data across client businesses (methodology as described). Internal source; not directly comparable to other vendors’ published figures.
7. IMD, World Digital Competitiveness Ranking 2025 (Singapore among global leaders). imd.org
8. Reserve Bank of India, (Know Your Customer) (2nd Amendment) Directions, 2025, dated 14 August 2025. rbi.org.in
9. Monetary Authority of Singapore, Cyber Risks Associated with Deepfakes (Information Paper), 18 September 2025. mas.gov.sg`
10. Bank Negara Malaysia, Policy Document on Electronic Know-Your-Customer (e-KYC), revised 15 April 2024. bnm.gov.my
11. Bangko Sentral ng Pilipinas, Circular No. 1170 (e-KYC; PhilSys-enabled verification). bsp.gov.ph
12. Securities and Futures Commission (Hong Kong), “Updates to acceptable account opening approaches”, 30 May 2025 (iAM Smart; ICAO-compliant ePassport onboarding). sfc.hk
13. PRC amended Anti-Money Laundering Law, effective 1 January 2025 (extends obligations to specified non-financial institutions; beneficial-ownership verification).
14. Australian Government, AML/CTF Amendment Act 2024 (Royal Assent 10 December 2024; Tranche 2 from 1 July 2026; existing reporting entities from 31 March 2026). homeaffairs.gov.au
15. Government of Vietnam, Resolution 60-NQ/TW (April 2025) and Resolution 125/NQ-CP (9 May 2025): 63→34 provinces, district tier abolished, effective 1 July 2025. vietnamnews.vn
16. UNODC, Transnational Organized Crime … A Shifting Threat Landscape (October 2024) — 600%+ rise in deepfake-related content in Southeast Asia, H1 2024. unodc.org
17. CNN, “Arup revealed as victim of $25 million deepfake scam”, May 2024. cnn.com
18. US Treasury / FinCEN, Section 311 action on Huione Group (1 May 2025) — at least USD 4 billion laundered, Aug 2021–Jan 2025; analysis via Elliptic. elliptic.co
19. United Nations Office on Drugs and Crime (UNODC), Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape, October 2024
20. Arup revealed as victim of $25 million deepfake scam involving Hong Kong employee, CNN, 16 May 2024.
21. China uncovers country’s largest AI face-swap scam, Yicai Global, 23 May 2023 (reporting a police briefing on a Fuzhou businessman defrauded of CNY 4.3 million via an AI face-swap and voice-mimicking video call).
22. United Nations Office on Drugs and Crime (UNODC), Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape, October 2024.
23. Financial Action Task Force (FATF), INTERPOL and Egmont Group, Illicit Financial Flows from Cyber-Enabled Fraud, FATF, Paris, 9 November 2023.

Shufti

The Trust Foundation

In APAC's digital-first economy, identity verification is not a compliance checkbox. It is the foundation on which customer trust is built, maintained, and scaled. Every business in this region, from a fintech onboarding its first million users in Indonesia to a crypto exchange expanding from Seoul into Singapore, faces the same fundamental question: can we verify who our customers are, keep pace with the regulations governing how we do it, and stay ahead of the fraud that targets every trust moment we create?

Shufti was built to answer that question with confidence for every market, every regulation, and every growth stage that APAC's digital economy will demand.

Book a Demo →