



How

eKYC

is Streamlining
Digital Banking



An Asia-Pacific
Perspective

JUMIG[®]

Setting the Stage: Understanding the Digital Banking Landscape in APAC

The launch of virtual banks across Asia-Pacific is beginning to disrupt the traditional banking model. At the same time, banks are expected to adopt more technology solutions to manage costs and achieve operational efficiency amid a rapidly evolving and increasingly competitive landscape.

The arrival of virtual banks is expected to have a greater impact on small- and medium-sized enterprises, especially those reaching the unbanked and traditionally underserved markets. Newly licensed digital banks, global and digital-only banks are all vying for their share across the region's lucrative markets. In response, many traditional banks will seek to accelerate their IT and systems transformation, invest in new technologies and upgrade their digital platforms to compete. For example, the CIMB Group launched the all-digital, mobile-first CIMB Bank Philippines in 2019, and nearly 2 million Filipinos signed in via the CIMB Bank PH digital platform in its first year of operations.





Virtual Banking Licenses

Regulatory authorities in Australia, Japan, Hong Kong and Taiwan have already issued virtual bank licenses while Singapore and Malaysia are looking to catch up. The Monetary Authority of Singapore received 21 applicants competing for five virtual banking licenses.



Fintech Riding the Digital Payment Wave

In the EY 2019 Banking in Asia-Pacific Report, Ernst & Young forecasted that APAC emerging markets will see a 7.5% increase in mobile penetration between 2018 and 2022. The rise in mobile digital transactions gave rise to an increase in mobile payment apps which allow banks to transfer funds for purchases. Digital payments transactions reached US\$600 billion in consumer spending, with e-wallets accounting for US\$22 billion.



Increase in Online Fraud

Digital banking has also opened up more opportunities for fraudsters. According to Experian's 2019 Asia-Pacific Global Identity and Fraud Report, 50 percent of businesses surveyed in Asia-Pacific saw an increase in fraud losses over the past 12 months from account originations and account takeovers.



Compliance Remains Painful for Customers and Banks

Ensuring KYC and AML compliance is the most time-consuming and onerous step in the onboarding process. Financial institutions need to ensure compliance with local and regional laws while also ensuring that customers have a smooth onboarding experience which is also financially feasible.

Clearly, virtual banking presents opportunities and access to new markets, but it's also fraught with challenges, from online fraud and technical know-how to compliance hurdles.

Ingredients for a Successful Virtual Bank

Starting a virtual bank (or transforming a traditional bank) is no small task — and many will not make the transition successfully. The banks that are willing to completely change their operational models are the ones that will succeed in making the virtual banking transformation. Let's explore some of the key ingredients that will help separate the winners and the losers.



Targeting

Virtual banks have the ability to not only target markets within their home countries but also quickly reach other markets. Virtual banking also helps many banks reach whole new generations. Millennials, Gen Zers and baby boomers alike are early adopters of new tech products and are comfortable navigating the world through the lens of their smartphone or tablet. So by prioritizing a streamlined, personalized and mobile-optimized experience, virtual banks can satisfy the needs of a new breed of customers.



**3 OUT OF 5
TRANSACTIONS
ON MOBILE**

Mobile Transformation

A recent innovation study found that just over three out of five (61%) consumer banking transactions in 2019 were conducted on mobile phones. Strikingly that figure is up from 52% in 2018 and 28% in 2014.



Digital Transformation

We have seen some efforts at banks to digitally reimagine certain services, such as the onboarding of new customers. But digital transformation goes beyond just digitizing the front end (e.g., the website and the app). Banks need to fully replace their legacy processes and back-end systems with digital technology to build a customer-centric infrastructure.



Onboarding

When customers no longer need to set foot within a branch office, the online experience is everything. Unfortunately, recent research found that over 50% of retail banking customers abandoned their attempt to sign up for new financial services online because of a long and clunky onboarding process. Given the acquisition costs of a new customer, banks cannot afford to squander the opportunity.



Brand Awareness

Virtual banks must quickly establish their brand, raise their awareness and establish their differentiation if they want to compete and gain share. Similarly, traditional banks need to transform their image of being outdated or even irrelevant by investing in the customer experience. This also means exploiting the power of data and advanced analytics to build more personalized communications.



Differentiation

In order to gain share and some level of notoriety, digital banks need to carve out a unique space in the minds of their target markets. Virtual banks are serving as catalysts for innovation and change and eKYC is enabling them to tap into different customer segments and markets. eKYC refers to the process of performing identity verification and due diligence online/electronically. By bringing the KYC process online, businesses have an opportunity to improve the customer onboarding experience by reducing paper-based procedures and time spent on administration. They can also reduce the costs of and time spent on verification, making it more profitable for the organization.



Compliance

Three out of five banks in Asia-Pacific still do not have full digital account opening for new customers, according to a survey of 20 chief risk officers from across Asia-Pacific (FICO, April 2019). Respondents cited the region's changing regulations (28%) and the need to create digital KYC/AML solutions (21%) as the biggest challenges they had in terms of acquiring customers online.



User Experience

At the heart of everything virtual banks do is user experience. From improved customer service and innovative new products, to frictionless onboarding and simple yet effective apps and online banking interfaces, challenger banks have made established financial institutions sit up and take note, especially as they become increasingly popular among younger generations who have grown up in the internet age.



Fraud Detection

Four out of five Asia-Pacific banks (78%) say the introduction of real-time payments platforms in their country has resulted in increased fraud losses, with social engineering named by two in five banks as the top form of attack by fraudsters. Additional identity and authentication technologies are needed.

Optimizing Customer Acquisition

After enjoying double-digit annual revenue growth from 2010-2014, banks in Asia-Pacific are starting to witness tapering growth trends with annual revenue growth slowing to 5% in 2014-2018 and growth in profit pools easing to 3% over the same period, according to McKinsey's annual banking review.

And this puts a tax on customer acquisition costs.

Customer acquisition for the leading digital challenger banks has been accelerated by viral marketing and social media. The average challenger bank's cost of acquisition ranges from £1 to £30, which is significantly less than the cost of acquisition for incumbents. Unfortunately, this trend of low-cost customer acquisition is nearly over. In fact, it has become more difficult and more expensive to cut through the clutter to attract new customers at an affordable cost.

Online abandonment dramatically increases customer acquisition costs.



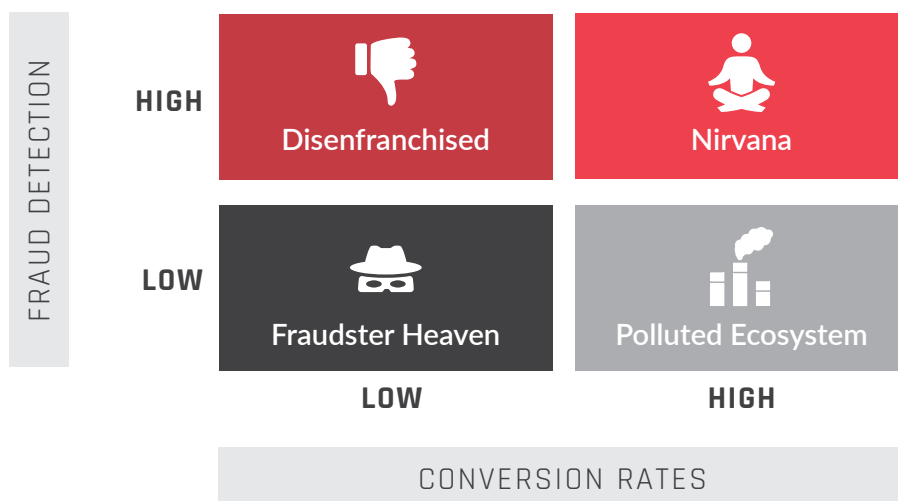
Approximately 40% of online applications never get completed and get abandoned midway by the customers.

SIGNICAT, 2019

Account opening is a tedious job for customers — it's often time-consuming, cumbersome and requires a lot of effort for them to provide their personal information. Today's digitally savvy customers do not wish to spend time and effort in selecting a product and then providing a long trail of information about themselves to get the product.

Balancing Conversion with Fraud Detection

It's a delicate balancing act between friction and the user experience. On one side, prioritizing fraud detection adds incremental friction to attain higher levels of identity assurance. If you have too much friction, conversion rates drop off and you're left with disenfranchised prospects. On the other side, focusing on conversions often means reducing the friction during the account creation process. This translates to lower levels of assurance and fraud detection, which means more bad actors access (and pollute) your organization's ecosystem.



Successful Asia-Pacific banks in the digital world need to strive for continuous improvement and renewal. That means getting much faster in the way they learn, act and react. An increasing number of modern banks are deploying high-powered machine-learning algorithms and AI-powered fintechs to streamline onboarding, reduce manual labor and increase accuracy in support functions, including fraud prevention, KYC reviews, loan processing and credit underwriting, among others.

It's no longer an either/or situation. Banks can now have high levels of fraud detection and conversion rates with the right technology stack.

True Measures of Fraud Detection: FAR & FRR

Most eKYC vendors position their offering as a comprehensive eKYC solution. This necessarily means calculating the effectiveness of fraud detection, which can be objectively measured via two statistics:

False Acceptance Rate (FAR):	False Rejection Rate (FRR):
The percentage of identification instances in which imposters are incorrectly accepted .	The percentage of identification instances in which legitimate users are incorrectly rejected .

Verification providers will sometimes speak about false positives and false negatives and they are parallel concepts. Legitimate users who are incorrectly rejected are considered false positives while incorrectly accepting fraudulent users are considered false negatives.

Unfortunately, most eKYC solutions often lack the requisite knowledge, experience and best practices to deliver optimal performance. This means having the means and business intelligence to handle blurry images, provide end users the ability to course correct (e.g., when their images are dimly lit or key parts of the ID are obscured by a finger), and a systematic way to continually tune the AI algorithms that inform the biometrics system.

Ultimately, modern enterprises want a definitive verification decision — a yes or a no — not a risk score in order to more quickly convert new users into customers.

KYC & Customer Due Diligence

Consumers increasingly expect that their online banking experience should be as simple, secure and convenient as their everyday apps, and this starts with the onboarding experience – anything less than an accurate, fast, seamless experience will be rejected by consumers who often have plenty of immediate alternatives.

It's not as simple as making it easy for a consumer to open a new bank account whenever and wherever they want. The current regulatory landscape in Asia-Pacific adds a layer of complexity, and financial institutions must comply with stringent anti-money laundering (AML) and know your customer (KYC) regulations that typically send new customers out of their preferred (digital) channel for identity verification.

1.



Online Form

Applicant provides name, address and other relevant data.

2.



Government ID

Picture of driver's license, passport or ID card is captured with smartphone or webcam.

3.



Selfie

User takes a corroborating selfie to ensure picture in selfie matches picture on ID document.

4.



Database Check

Organization pings a variety of third-party databases to ensure that the individual exists (usually based on name and date of birth checks).

5.



Fraud Signals

Organization may check a variety of fraud signals, including the IP address of the phone, email address verification and even the speed at which the online forms are completed by users.

6.



AML Screening

User is screened against regional government-issued watchlists and politically exposed person lists as part of anti-money laundering compliance mandates.

7.



Proof of Address

Since the address is often not included on the ID document, the organization may need to capture proof of address (e.g., copy of bank statement or utility bill).

8.



Risk Pools

Based on these checks, screening and fraud signals, users are assigned to risk pools and those flagged as high risk may be reviewed manually to make a final determination.

9.



Ongoing Monitoring

After the customer has been onboarded, customers are monitored on an ongoing basis. This includes transaction monitoring, AML monitoring and behavioral monitoring (anomaly detection).

Streamlining the Onboarding Process in APAC

For established banks and up-and-coming digital banks, it's become a business imperative to streamline the digital onboarding experience and dramatically cut abandonment rates. And so much of this comes down to common sense processes and technologies that enable a better experience.



1. Cover All of APAC, Not Just Part of It

No matter where your customers are in the world, your identity verification solution should be able to support them whether they're in Singapore, Malaysia, the Philippines, Hong Kong or Australia. Banks can convert more accounts with a solution that gives users the most possible options when it comes to ID documentation including passports, driver's licenses, ID cards — and older versions of these too.

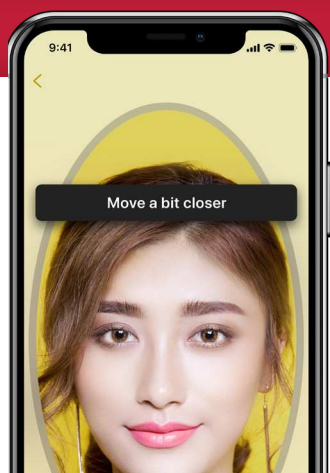
2. Enable Auto-ID Capture

Eliminate extra steps and increase accuracy with a solution that automatically captures the user ID once it is clear and properly positioned in the camera frame. This simple functionality can yield as much as 30% higher acceptance rate compared to manual ID capture.



3. More Capture Channels

Let your users complete the account opening process via API, mobile SDK (apps) and mobile web. This is especially important if you're trying to reach different demographics who gravitate to different channels.

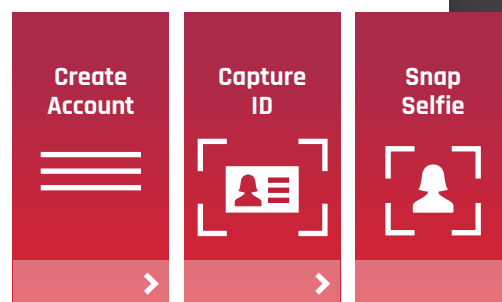


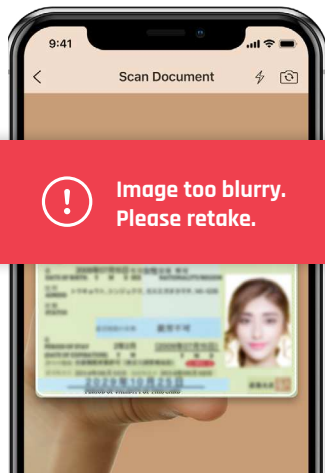
4. Provide Clear Instructions

Provide context and rationale to users as to why they must go through the identity verification process. Frame it in a positive light and don't use jargon.

5. Eliminate Unnecessary Screens

Simplify the user journey as much as possible. Fewer screens translates to higher conversions. "The most fundamental attribute of an exceptional account opening experience is speed – the faster an account is opened, the less likely the customer is to want improvement." (Deloitte)



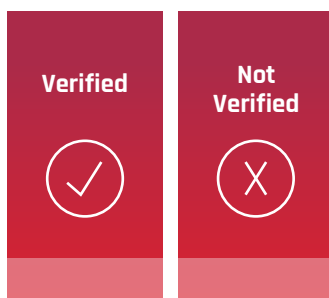


6. Provide Instant Feedback

Look for an identity verification solution that returns specific rejection codes when an ID or identity is rejected. This allows the user to course correct, retake the photo and resubmit their ID right on the spot. **In fact, offering detailed feedback in real time can boost onboarding conversion rates by 15%.**

7. Utilize Intuitive Liveness Detections

Liveness detection is the process of determining if someone is physically present during the transaction. If you can prove liveness, it establishes the chain of trust and anchors the digital identity of a real person. Plus, it helps keep fraudsters, spoofs, deepfakes and bots from opening bogus accounts.



8. Reduce the Need for Manual Review

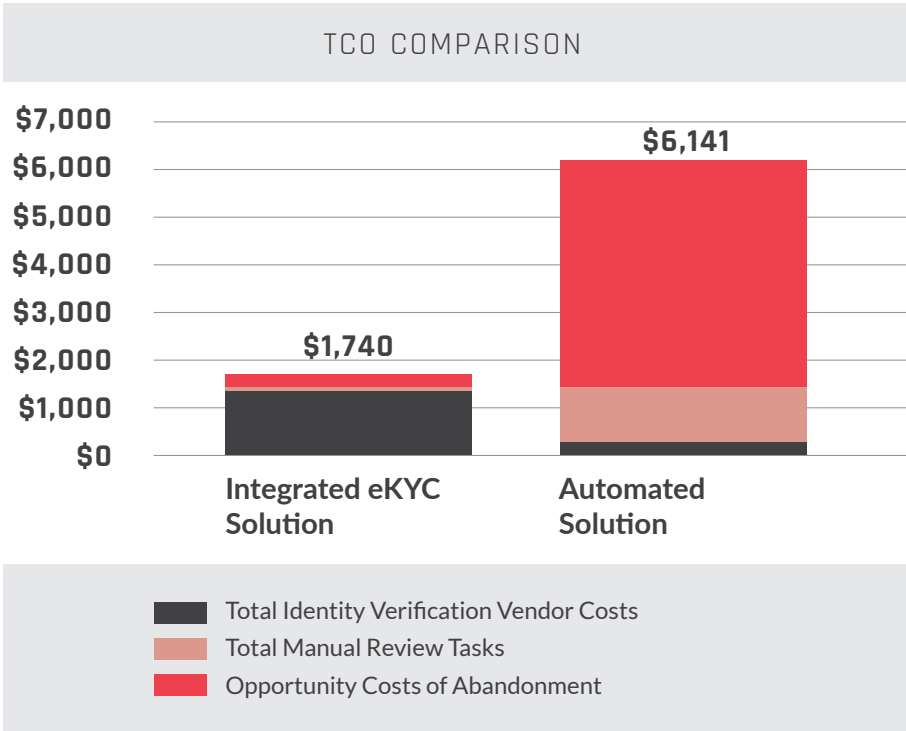
Make sure the identity verification solution you use delivers definitive yes or no answers. “Maybes” lead to costly manual reviews on your part to determine if the customer is fraudulent or legitimate.

Understanding the Full Costs of Onboarding

Asia-Pacific is home to over 40 different regulators and varying complex approaches to AML regulation and customer due diligence obligations. The increasing costs of client onboarding and KYC and AML compliance is reflected in the enhanced regulatory frameworks introduced by the Hong Kong Monetary Authority, Australian Securities and Investments Commission, the Monetary Authority of Singapore and the Bank Negara Malaysia. Moreover, the introduction of beneficial ownership registries in certain jurisdictions adds an additional layer of regulatory and reputational risk for financial institutions.

Labor represents a sizable portion of the KYC and AML compliance spend, which drives higher costs at larger firms. As a result, these firms are implementing labor-related steps to address the impact of non-bank payment providers and systemic risks, including enhanced training and controlling operations screening hours. Despite the labor-intensive nature of the AML/KYC function within financial firms, few institutions are capitalising on AI-based technologies across the region.

Unfortunately, financial institutions in Asia-Pacific often make short-sighted business decisions based purely on the total vendor costs. When it comes to identity verification, for example, there are really three drivers of cost: **the cost per verification, the cost of manual review and the cost of customer abandonment (which can be caused by an identity verification process that is too time-consuming, onerous or invasive).**



The graph above shows a Total Cost of Ownership (TCO) estimate for 1,000 verifications.

Even if the initial identity verification vendor cost is higher, the total TCO is lower since it minimizes the cost for additional manual review and the cost of lost opportunities due to low accuracy of the automated solution.

Traditional identity verification solutions are often, slow, inaccurate and unable to catch or deter more sophisticated forms of online fraud. The high inaccuracy rates often translates into more manual reviews (performed by in-house teams) which further slows down the process which leads to greater abandonment and high opportunity costs. Modern identity verification solutions can often help tick many of the AML and KYC compliance requirements, deter fraud and deliver a much faster and intuitive user experience.

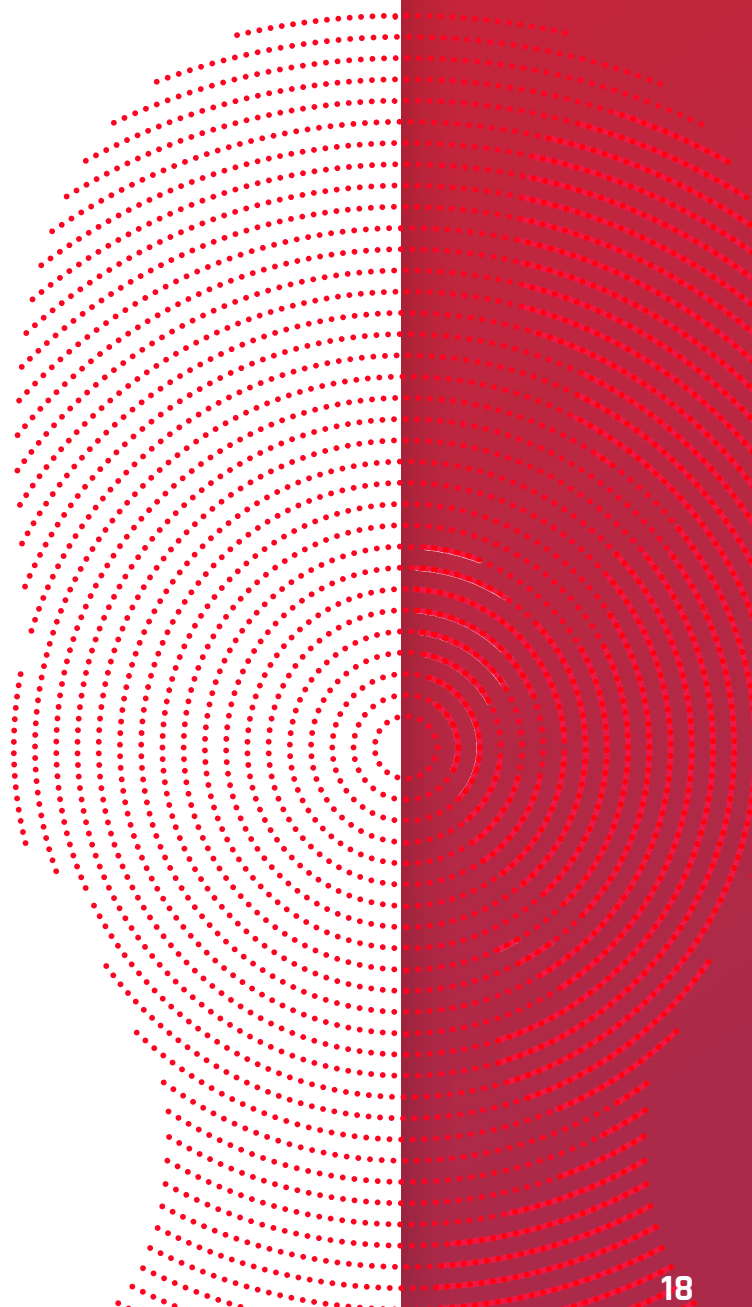


The Role of Biometric-Based Authentication

When it comes to identity proofing, many traditional banks still rely on database look-ups — what Gartner refers to as “static data corroboration” (e.g., knowledge-based verification). These methods rely on public records for real-world activity and on credit bureau data to confirm or deny that the information provided by an individual matches the information on record.

While popular, these methods are relatively ineffective at detecting both synthetic identity and identity theft. They also have been poorly equipped to corroborate the identity of individuals with an absence of credit history due to the use of alternative financial services, age or recent immigration to the country whose records are being interrogated. In light of recent data breaches which have exposed much of this data to the dark web, Gartner strongly recommends that modern FIs move away from this method as their sole method of corroborating the identity of individuals.

Biometrics is now starting to fill this void by delivering a more reliable, secure, and intuitive user experience through the use of unique biological characteristics. Biometrics allows a person to be identified and authenticated based on a set of recognizable and verifiable data, which are unique and specific to them. Biometric authentication is the process of comparing data for the person’s characteristics to that person’s biometric “template” to determine resemblance.



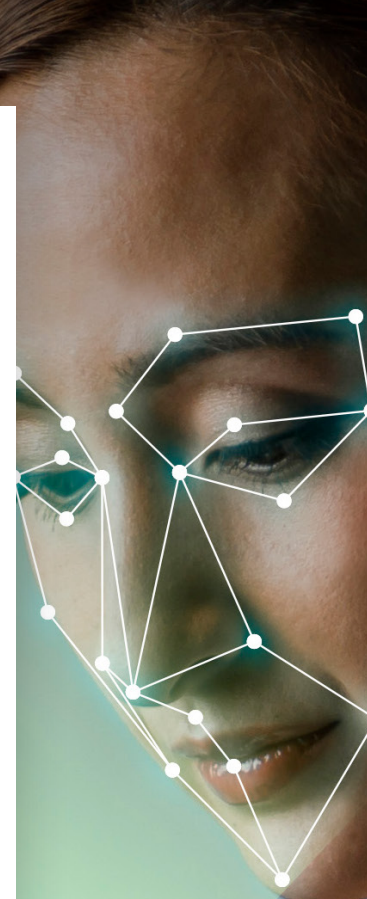


Three-quarters of APAC consumers have more confidence in banks that have integrated biometric online security.

EXPERIAN, 2019

But up until recently, the only security customers in the region had was the use of their personal identification number, which made it easy for hackers to take over their accounts.

According to [Banking CIO Outlook](#), the new strategy involves multi-factor authentication that consists in a mix of biometric identification, most likely in the form of 3D face maps, fingerprint scanning, passwords and personal identification numbers. By deploying biometric-based verification and authentication, APAC banks can simultaneously reduce costs, deliver an enhanced user experience, provide higher levels of identity assurance and boost security.



Deepfakes & Other Emerging Threats

A deepfake superimposes existing video footage of a face onto a source head and body using advanced neural network powered AI. In other words, a deepfake looks to be a real person's recorded face and voice, but the words they appear to be speaking were never really uttered by them, at least not in that particular order.



Not surprisingly, deepfake technology is also being weaponized for political misinformation and cybercrime.

Many modern identity verification solutions now require new users to take a picture of their driver's license (or some other government-issued ID) and then take a corroborating selfie. The face in the selfie is then matched to the face on the ID document and a yes/no decision as to whether the person in the selfie is also shown on the ID is rendered.

A number of years ago, cybercriminals started using photos and pre-recorded videos to bypass biometric-based verification systems. In response, identity verification providers introduced different types of liveness detection to attempt to differentiate between real human users and spoof artifacts. The goal is to know if the biometric data being matched is from the live, physically present person at the time of capture.



Put simply, liveness detection prevents bots and bad actors from using photos, videos, masks or other biometric data (stolen or otherwise) to create or access online accounts. Liveness ensures only real humans can create and access accounts. Sometimes liveness detection methodologies ask users to blink, smile, turn/nod, watch colored flashing lights, make random faces, speak random numbers and much more. Sadly, most of these legacy techniques are easily spoofed by deepfakes.

More and more identity verification providers are unveiling passive “liveness detection” based on a single static image. Unfortunately, this form of basic liveness detection can be easily spoofed since it does not detect the physical presence of the end user. That’s why it’s imperative to leverage stronger and more robust forms of liveness detection.

In the world of liveness detection, there is a large distinction between certified and uncertified methods. Certification testing is performed by iBeta, a NIST/NVLAP-accredited lab, based in the United States. They are currently the only lab performing presentation attack detection (PAD) testing guided by the all-important ISO 30107 global standard. This certification is key when it comes to detecting and thwarting deepfakes.

At their core deepfakes are 2D videos, not 3D human faces, so they become relatively easy to discern for a certified 3D liveness detection provider like FaceTec. The computer monitor used to play back the video emits light – it doesn’t reflect it – and certified liveness detection can tell the difference. And, if a criminal attempts to use the deepfake video with a projector onto a 3D head, then the skin texture won’t be quite right, and the advanced certified liveness solution will detect the generation loss, a surefire tipoff.



Stitching Together eKYC Modules

Today, many APAC fintechs and financial institutions are looking to deploy and stitch together OCR and facial recognition solutions, in combination with their own manual processes and review teams as part of a homegrown KYC solution.

Cobbling together disparate piecemeal solutions may not be the quickest path to better compliance, improved fraud detection and increased verification accuracy. Although point solutions are great for functions like accounting, project management or document management, relying on multiple software solutions for eKYC and AML screening can lead to greater organizational roadblocks down the line and dramatically less accuracy.

For example, many enterprises may develop separate modules for different parts of the identity proofing process, including:



OCR

To extract key parts of data from the ID document in order to compare to the ID's barcode or MRZ (passports)



Liveness Detection

To prevent spoofing and presentation attacks when a fraudster uses a photo or video (deepfake) instead of a genuine selfie



Face Matching

To compare the image on the ID document to the selfie which ensures that the person presenting the ID is the same as the ID owner



Fraud Detection

To ensure that the ID document and the selfie are genuine, contain the correct security features (e.g., watermarks, microprint) and have not been manipulated



AML Screening

To check the user against regional watchlists, politically exposed persons (PEPs), sanctions and adverse media in order to limit money laundering schemes



Risk Engines

To better assess the risk profile of would-be customers using a variety of fraud signals to corroborate the digital identities of your users.

When organisations take a module-based approach, they generally need either manual labor (or engineering resources) to make sure that they interoperate. This human element not only adds cost to the process but it introduces other challenges that are often underappreciated, including:



Expensive

Each module requires human capital to manage the software, interpret the results and move the eKYC process forward.



Error Prone

The more human resources required, the greater the likelihood of error. While automated solutions can make verification mistakes as well, the decisions will be consistent and can be course-corrected.



Slow

Unfortunately, when more humans are involved in more verification processes, it's likely that the verification times will take minutes, hours or days (instead of seconds). Here again, manual processes will result in inconsistent verification times based on staffing and time of day or week.

A New Dawn

Instead of building your own solution, piece by piece, increasingly it makes more practical and economic sense to buy a full-stack eKYC solution. Benefits of this approach include:



Orchestration

Better verification vendors take care of the orchestration layer between all of these separate components and deliver a definitive yes/no answer, in a matter of seconds or minutes.



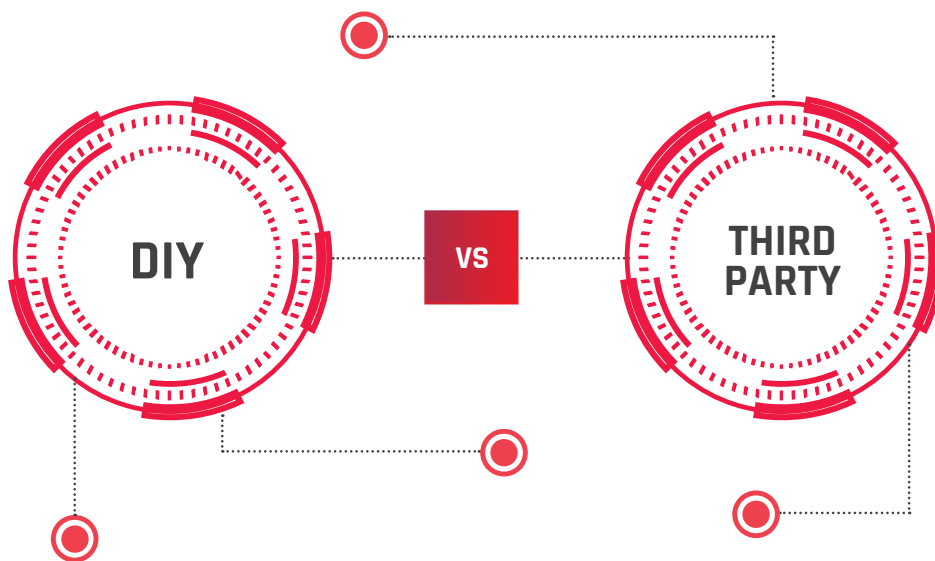
Informed AI

Leading identity verification providers enrich the entire eKYC process flow through the use of AI to minimize the need of human review in the intermediate stages to detect fraud, streamline the user journey and develop predictive risk scores. Some vendors go a step further providing an “informed AI” — developing AI algorithms that are supported by machine learning based on hundreds of millions of historical verification decisions and informed by human review who tag verification transactions which help the algorithms get iteratively better.

While many vendors boast about their use of AI, it's important to understand how much data has been leveraged to create those algorithms and how have they been tagged to assist the learning process. Taking a DIY approach often neglects the power of AI and is inherently limited in its ability to get iteratively better over time.

As a result, homegrown solutions are limited and often struggle to efficiently extract key details from ID documents, perform security checks, compare the selfie image to the image on the ID, ensure liveness of the user and deliver accurate and rapid verification results. Because of that, these solutions are usually inaccurate and often necessitate extra manual review as a result of environmental factors such as bad lighting, blur and glare. The more manual review required, the more time required to render a yes or no decision. The longer the process, the higher the user abandonment. Based on recent research, online abandonment can be as high as 50%. And this abandonment translates into user frustration, brand damage and lost revenues.

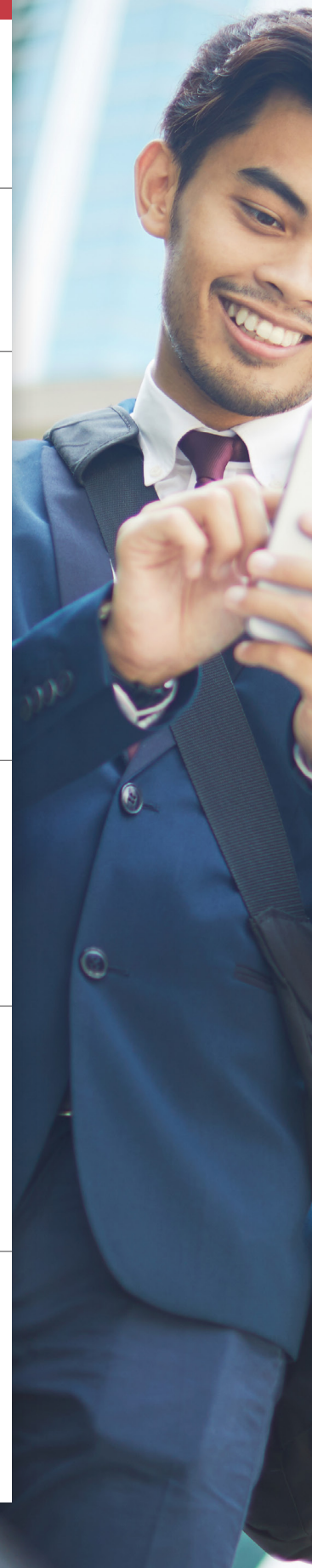
If you're evaluating whether to DIY or utilize a third-party eKYC solution for your organization, you should understand some of the key evaluation criteria in the perennial build vs. buy question. It's critical to address all the components that need to be built in order to make an apples-to-apples comparison.

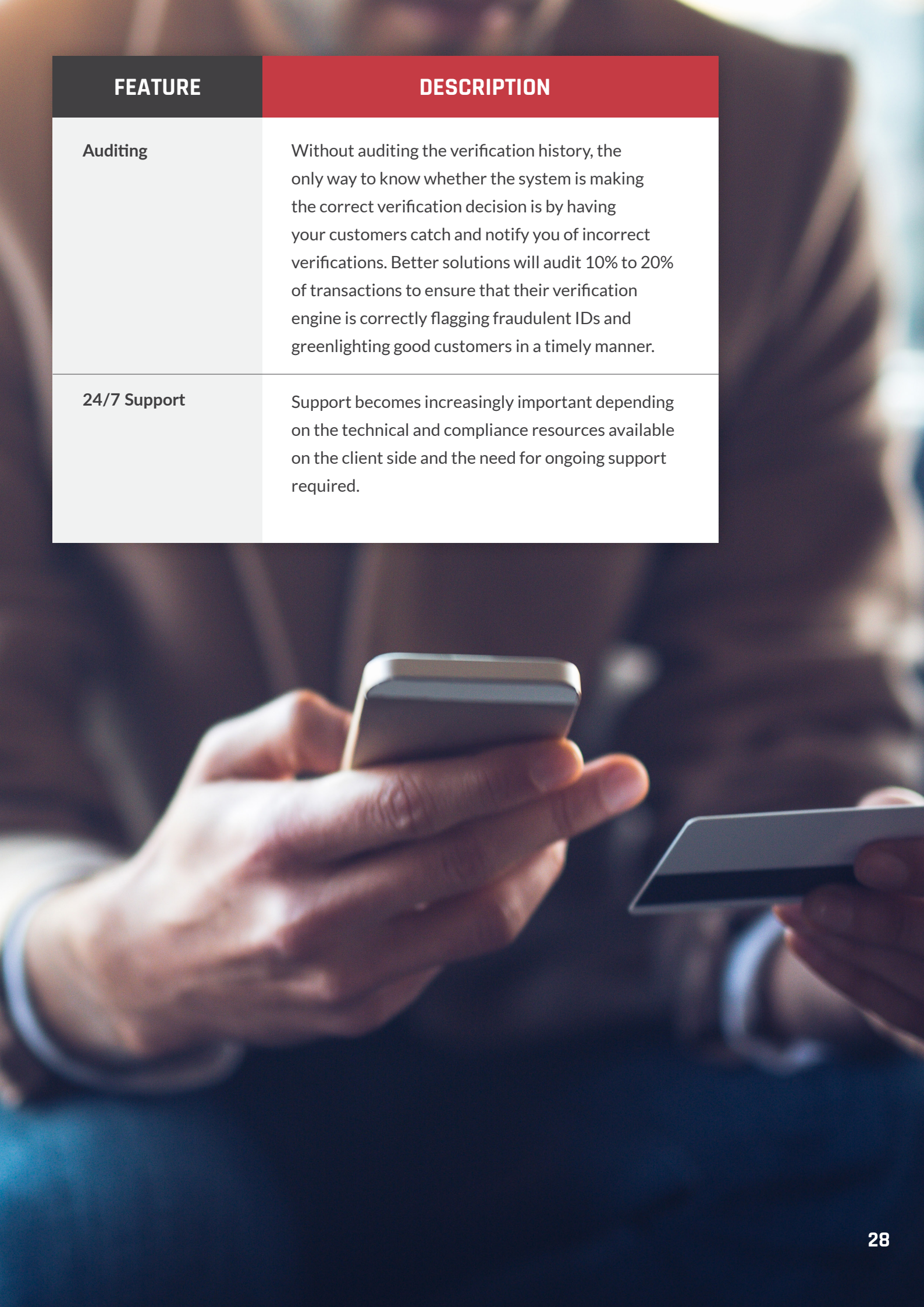


FEATURE	DESCRIPTION
Price	Point solutions are generally more affordable than fully integrated KYC solutions, but often offer significantly less functionality and deliver more inaccurate results (which often lead to more manual review and higher abandonment rates).
Approval Rate	The number of online transactions initially approved by the identity verification supplier. More integrated solutions typically generate higher approval rates because of the use of AI/machine learning, the ability to process verifications with blur and glare, and the ability to provide detailed rejection codes that enable end users to course correct (e.g., the ID image is obscured by a finger).
Optical Character Recognition (OCR)	OCR is used to extract data key information from the ID document which is imperative for age verification and performing data lookups (e.g., AML screening).
AI/Machine Learning	Leveraged in a broad number of areas from auto-aligning (rectifying ID images) to fraud detection to risk scoring. AI/ML algorithms can also help to identify which type of identity document is being presented.
Mobile SDK	With a homegrown solution, it's difficult to package it up as an SDK that can be embedded within an app. Having a SDK enables some incremental functionality. For example, some SDKs enable the app to automatically snap a picture when the image is framed under optimal conditions, with minimal blur/glare. Some SDKs can capture multiple frames and select the best frame to be submitted for identity verification.
Face Comparison	Comparing the picture on the ID document to the selfie image to ensure the person presenting the ID is the same as the ID owner.



FEATURE	DESCRIPTION
Blur/Glare Detection	Better solutions will be able to detect and make verification decisions when there is some level of blur or glare.
Fraud Detection	Can the solution detect whether the ID has been manipulated and check against a variety of security features embedded within the ID document?
Verification Speed	One of the key determinants of successful online conversions is the speed of verification. It's critical to measure the end-to-end verification speed from image capture to verification decision. The verification speed may vary from seconds to minutes to hours based on the vendor. NOTE: Several automated solutions exist in the market, but their verification accuracy is quite low because of their inability to address environmental factors.
Certified Liveness Detection	Liveness detection has become a business necessity for any biometric-based identity verification solution that needs to thwart sophisticated spoofing attacks (e.g., a fraudster uses a deepfake video instead of a selfie).
IDV System Tuning	Online identity verification is a process that includes multiple steps and processes. Whether it's a single integration or customized solution (built by the organization), the processes need to be regularly tuned and tweaked to ensure verification accuracy.
FAR & FRR Tuning	Balancing FAR and FRR is difficult work to achieve an optimal user conversion. For many eKYC vendors, this type of FAR and FRR tuning becomes the business customer's responsibility.





FEATURE	DESCRIPTION
Auditing	Without auditing the verification history, the only way to know whether the system is making the correct verification decision is by having your customers catch and notify you of incorrect verifications. Better solutions will audit 10% to 20% of transactions to ensure that their verification engine is correctly flagging fraudulent IDs and greenlighting good customers in a timely manner.
24/7 Support	Support becomes increasingly important depending on the technical and compliance resources available on the client side and the need for ongoing support required.

Getting What You Pay For

Given these criteria, it's important to understand the tradeoffs of different types of solutions and the degree of product integration (including OCR, facial recognition, fraud detection and AML screening).

The chart below compares three different service offerings options:

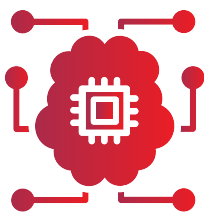
Full Stack eKYC Service	This solution has integrated eKYC, AML and fraud detection functionalities.
Automated IDV Solutions	This category of solution relies heavily on AI and back office agents to perform manual reviews.
OCR Solutions	These solutions rely on OCR to extract key data fields off the ID document. Because these solutions do not include any fraud checks, liveness detection or face matching functionality, they can fall short of compliance mandates and put an extra tax on manual resources.

CRITERIA	Full Stack eKYC Service	Automated IDV Solution	OCR Solution
Approval Rate	95%+	50%	varies
OCR/Data Extraction	automated	automated	automated
AI/Machine Learning	✓	✓	✗
Face Comparison	✓	✓	✗
Blur/Glare Detection	✓	✗	✗
Fraud Detection	✓	◐	✗
Verification Speed	< 2 minutes	< 30 minutes	varies
Certified Liveness Detection	✓	◐	✗
IDV System Tuning	✓	✗	✗
FAR/FRR Tuning	✓	✗	✗
Auditing	✓	✗	✗
24/7 Support	✓	✗	✗

These are important considerations for any modern enterprise exploring the build option. The cost of purchasing multiple point solutions on a need-by-need basis can quickly add up. In addition to purchasing a number of point solutions, including OCR, facial recognition and AML watchlist screening, businesses are forced to deal with incremental payments for user licenses and other fees associated with each individual software.

The build-or-buy decision is not an easy one, especially in Asia-Pacific where labor costs are low. For some applications, organizations can just suck it up and build a new, modern application from scratch. But with many other complex applications – most, in fact – it's a much more difficult decision. Either because of their complexity or because they are essential to the organization, but not necessarily delivering competitive value, it simply does not make sense for the organization to spend precious resources and capital immediately rebuilding these applications in a cloud-native fashion.

We would argue that today's identity verification solutions are too complex, involving myriad technologies (e.g., AI, OCR, liveness detection and biometrics) and processes, that it's far more practical to buy a more fully integrated KYC solution for onboarding new customers.



Bottom Line:

There's a very steep learning curve involved when stitching together point solutions which is too often underestimated and underappreciated.

A More Sensible Approach

Less than a third of banking executives in Asia-Pacific are equipped to handle the changing regulatory landscape, compared to 46% of their peers in North America and Europe, according to new research developed by Asia Risk and Oracle. In Asia-Pacific, banks and the regulatory bodies that govern them are behind their counterparts in modernizing their finance and risk processes and their use of data.

Modern eKYC, AML and identity verification technologies can transform many of the manual processes banks rely on today, particularly those related to meeting regulatory requests and gaining useful data insights to meet business objectives.

Jumio's identity verification process uses machine learning, face-based biometrics and verification experts to ensure the person behind a transaction is present and who they say are. Identity verification goes well beyond traditional authentication methods to deliver a significantly higher level of assurance and establish a trusted digital identity.



ID Proofing Check

Is the ID document authentic and valid?



Similarity Check

Is the person holding the ID the same person shown in the ID photo?



Liveness Check

Is the person holding the ID physically present during the transaction?



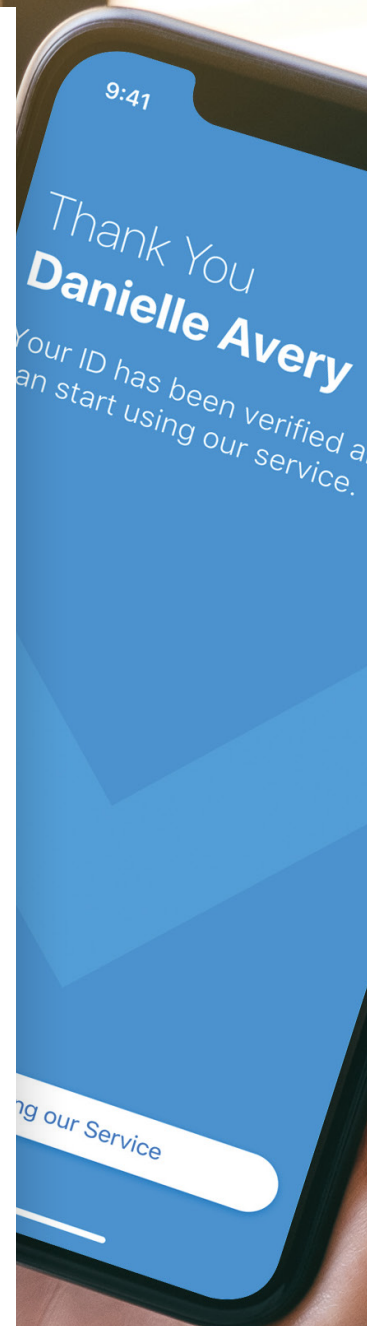
Definitive Answer

Jumio Identity Verification delivers a definitive yes or no answers in seconds.



Jumio helps global institutions streamline the onboarding process with an integrated eKYC, verification and AML solution that leverages a wide variety of technologies including informed AI, OCR, computer vision, biometrics, automated watchlists and human review. Collectively, these technologies deliver better, more robust solutions for fraud detection and watchlist monitoring, and provide a more fully compliant solution for regional regulators.

At Jumio, we deliver a full stack eKYC service, which builds upon our 10 years of eKYC knowledge in creating the balance between friction and user experience to achieve optimal user conversion outcome. To date, Jumio has verified more than 225 million digital identities which has fueled its leading informed AI algorithms. For Jumio, FAR and FRR rates are being optimized through a combination of informed AI, biometrics, OCR and biometrics, leveraging our global experience. Unlike other providers in this space, Jumio provides a binary response to our eKYC verification (i.e., a definitive pass or fail decision). As a result, Jumio continues to deliver better fraud detection, a more intuitive user experience and stronger conversion rates.



About Jumio

When identity matters, trust Jumio. Jumio's mission is to make the internet a safer place by protecting the ecosystems of businesses through cutting-edge online identity verification and authentication services that quickly and accurately connect a person's online and real-world identities. Jumio's end-to-end identity verification solutions fight fraud, maintain compliance and onboard good customers faster.

Leveraging advanced technology including informed AI, biometrics, machine learning, certified 3D liveness detection and human review, Jumio helps organizations meet regulatory compliance including KYC, AML and GDPR and definitively establish the digital identity of their customers. Jumio has verified more than 225 million identities issued by over 200 countries and territories from real-time web and mobile transactions.

Jumio's solutions are used by leading companies in the financial services, sharing economy, digital currency, retail, travel and online gaming sectors. Based in Palo Alto, Jumio operates globally with offices in North America, Latin America, Europe and Asia Pacific and has been the recipient of numerous awards for innovation.

For more information,
visit www.jumio.com



**Loved by users.
Loathed by fraudsters.**

Identity verification through informed AI.

JUMIO[®]