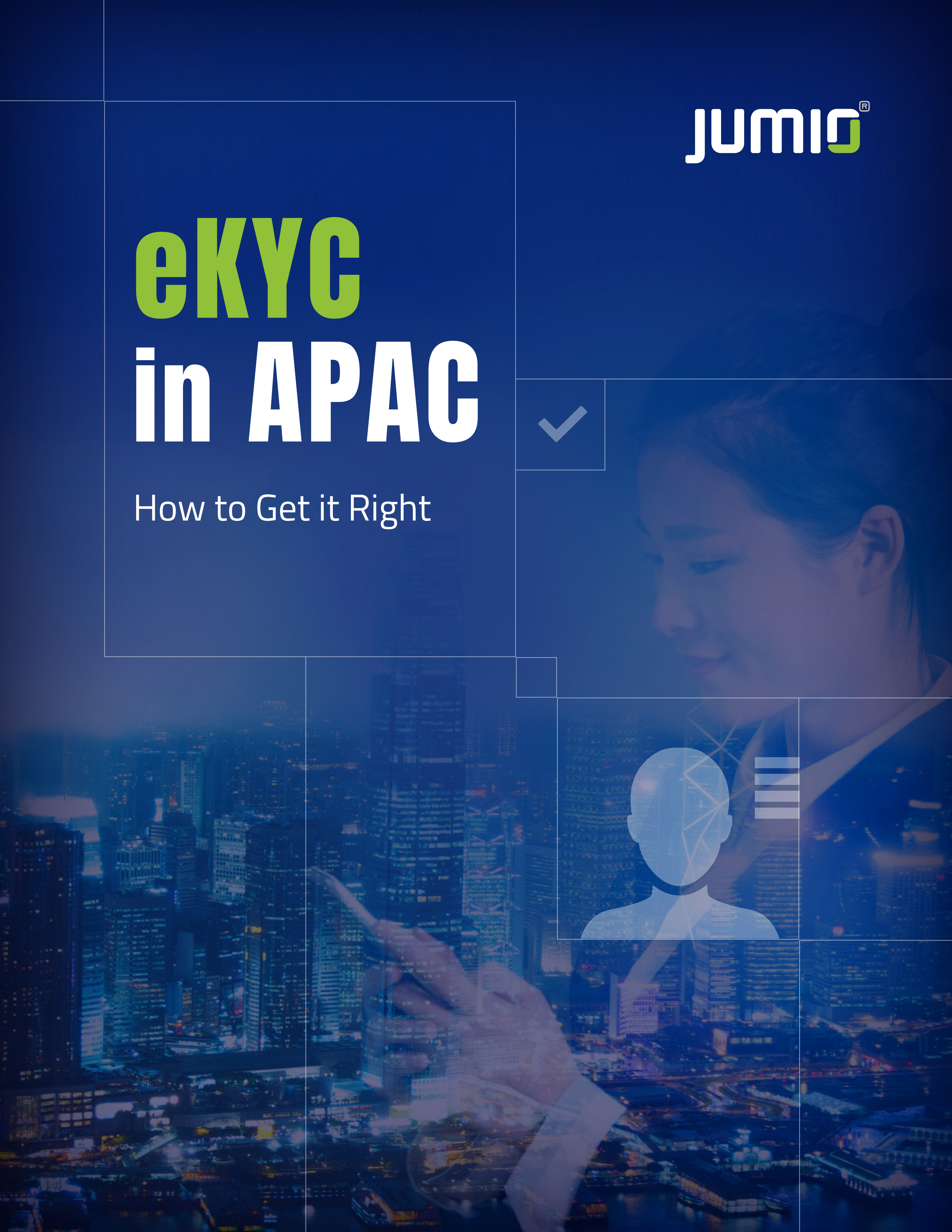
# eKYC in APAC

How to Get it Right



# Introduction

These are heady times for banks and fintechs in the Asia-Pacific region.

The central banks are loosening the reins on electronic Know Your Customer (eKYC) pilots in select regional sandboxes, but the pace of innovation and acceptance are increasing. eKYC is the online process of verifying the identity of customers, and assessing the risks or illegal intentions, during each transaction, whether they're opening or logging into an account, applying for a loan or making a payment.

The eKYC requirement imposed on financial institutions and certain financial reporting entities under increasingly stringent anti-money laundering (AML) laws is a key consideration for new and existing players getting into this space.

This new openness to eKYC makes sense given the skyrocketing adoption of mobile devices. For decades, Asia-Pacific marketers have looked to the U.S. to shape how we think of the online world, but we're on the cusp of a seismic shift. India recently surpassed the U.S. to become the second-largest online population behind China. In fact, the region has four of the world's top 10 markets for smartphone adoption. Singapore and South Korea are tied for fourth place at 91 percent, and nine countries in Asia already have the same or a higher smartphone ownership rate than the U.S.

Skyrocketing mobile device adoption is a positive step for APAC when it comes to eKYC and customer onboarding but it has also introduced significant new threats.

While 58 percent of all digital transactions now originate from mobile devices worldwide, one-third of all fraud attempts now target this channel.

## Cybercrime in APAC

Asia-Pacific companies receive **six cyber threats every minute**

(Cisco)

The potential economic loss across Asia-Pacific due to cybersecurity incidents could hit a staggering **$1.7 trillion (USD)**

(Frost & Sullivan)

Southeast Asia saw a **78% growth in attacks** year-on-year overall, and 105% growth on mobile new account creation transactions, highlighting the influence of breached identity data on the region. (ThreatMetrix H2 2018 Cybercrime Report)

**In this guide, you'll learn:**

- ✓ The benefits of biometric-based identity verification
- ✓ The dangers of taking a DIY approach to eKYC, especially when it comes to optical character recognition (OCR) and facial recognition software
- ✓ The challenges and opportunities of modern OCR and facial recognition technologies
- ✓ How OCR and facial recognition impact verification accuracy when used in isolation or when cobbled together in a piecemeal fashion
- ✓ How modern digital identity verification and automated AML screening solutions can help financial institutions meet eKYC requirements while protecting against online fraud and account takeovers with speed, accuracy and a streamlined user experience

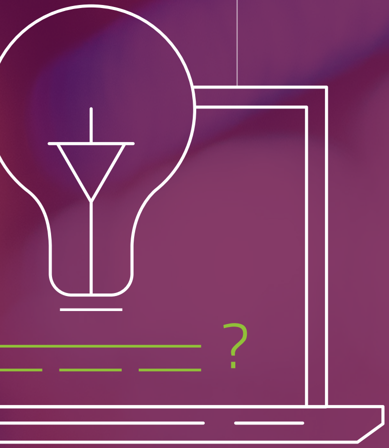
# The Old Way

Before we explore the promise of eKYC and automated AML screening, let's review how banks currently verify the identities of their customers.

The most traditional form of verifying customer identities is having a new customer visit a branch location to have their personal identification documents verified by a branch employee. Unfortunately, branch employees are not experts in identity document verification and are simply not trained to spot sophisticated forgeries. In addition to physically checking a new customer's ID documents in the branch, banks commonly employ other KYC technologies and techniques, including:

## Knowledge-Based Verification (KBV)

This type of identity verification relies 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. Typically, the user is asked several proofing multiple-choice questions such as "Which of the following ZIP codes have you resided in during the last five years?" which is then corroborated against public records databases. Questions are often created on the fly based on the user's public records or financial records history.



Knowledge-based verification has proven problematic as legitimate customers frequently fail these questions, and the frustration introduces a high rate of friction and abandonment. This method has also become ineffective due to the large troves of personally identifiable information (PII) captured by criminals in several security breaches over the last few years, and the large amounts of PII that can be found volunteered by users on social networks.

## PEPs & Sanctions

Domestic regulatory changes will increasingly require banks to monitor and flag suspicious transactions, incorporate more due diligence into the customer onboarding process (such as cross-checking of personal details against international watchlists) and report more activity to regulators. Unfortunately for many financial institutions, AML screening is still a manual, tedious process. The process requires bank staff to determine whether new customers are listed on any sanctions or watchlists of people with criminal track records. They must also determine if a customer is a politically exposed person entrusted with a prominent public function who, therefore, might be at higher risk for potential involvement with bribery or corruption.

## Credit Data

Many identity verification systems call out to one of the big three credit bureaus — Experian, Equifax, and TransUnion — who then search for an identity match within their vast repositories of consumer credit data. These tools analyze a customer's credit data and calculate the amount of risk they represent.

## Analytics Solutions

Behavioral analytics solutions can analyze customer transaction data and flag unusual behavior patterns such as atypical location. However, these tools are not perfect and can often make customers' lives more difficult. For example, if a customer is traveling and didn't notify their bank in advance, their transaction might be declined because it is deemed fraudulent even though it wasn't.

## Database Solutions

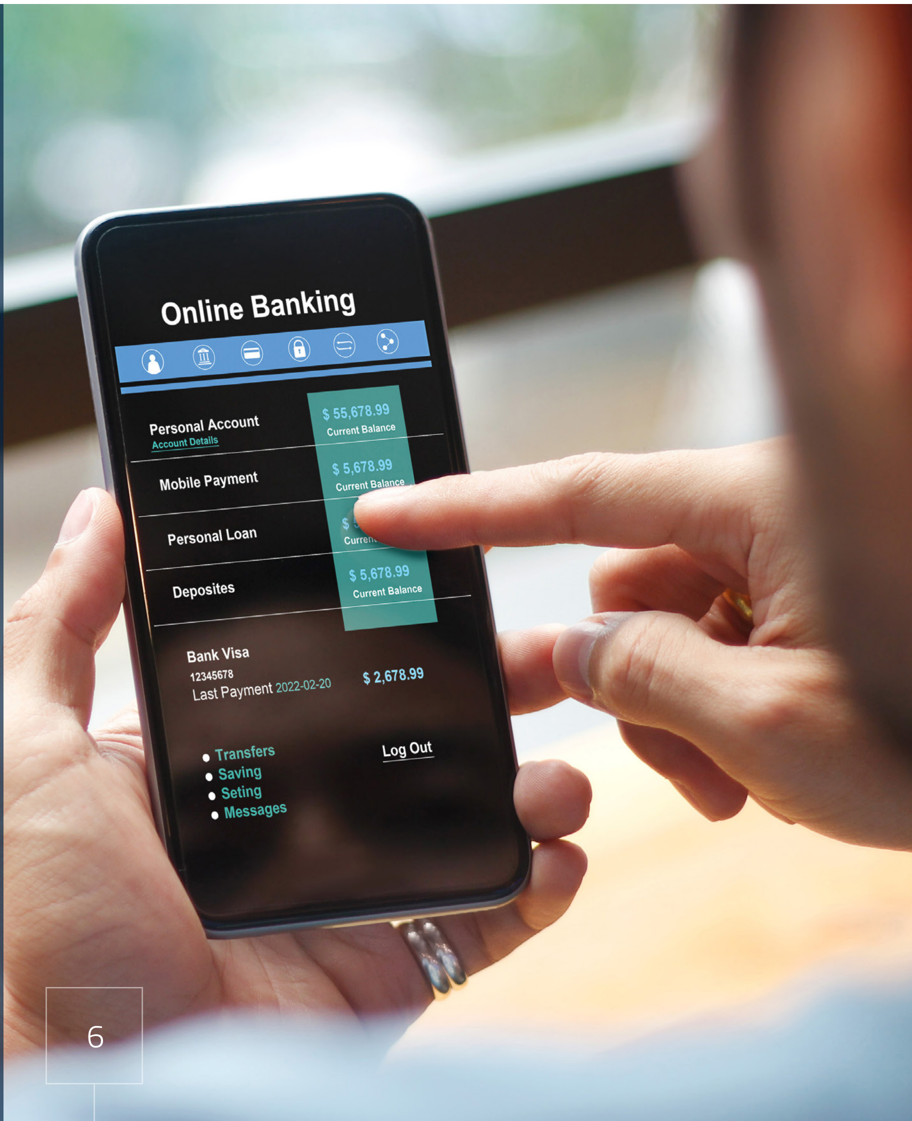
These solutions leverage online, social media and offline data (and sometimes behavioral patterns) to detect if an online ID is authentic, a fraudster or a bot. It is highly unlikely that even the most stringent of social media verification tools would pass regulatory scrutiny, making such methods impractical for financial services.

# Searching for a Better Way

More than ever before, banks are striving to increase new account enrollments through faster, easier and lower-cost digital channels. Yet, the current regulatory and cybersecurity landscape creates a layer of complexity. Consumers want the convenience of signing up through digital channels, but financial institutions must comply with stringent AML and KYC regulations that typically send new customers out of their preferred (digital) channel for identity verification.

Current estimates suggest that banks are closing hundreds of branch locations and consumers expect to be able to conduct their transactions — from beginning to end — through digital channels, expecting them to journey to the branch is not realistic. In fact, consumer visits to retail bank branches are set to drop 36 percent between 2017 and 2022, with mobile transactions rising 121 percent during the same period.

Consumer visits to retail bank branches are set to
drop 36 percent
between 2017 and 2022



# The Customer Experience is Sacrosanct

A 2019 Signicat survey found that more than 50 percent of EU consumers abandoned their attempt to sign up for new financial services and 72 percent said they wanted an all-digital onboarding system. Meanwhile, consumers who were able to successfully onboard digitally were more likely to remain loyal and tend to apply for additional products and services.

Another report (IDology's Consumer Digital Identity Study, May 2019) discovered that for the first time, consumers opened more new accounts on mobile phones than on computers. The study also uncovered a 19 percent increase in abandonment during account openings compared to last year, due to high consumer expectations for convenience and a low tolerance for friction.

**Online identity verification and AML screening are two crucial steps in the onboarding process and often the steps with the most friction, where many would-be customers bail out because of the time and effort it takes. But this friction has been viewed as a necessary evil, not only for compliance reasons, but to ensure that online customers are who they claim to be.**

Consumers increasingly expect that their online banking experience should be as simple, secure and convenient as their everyday apps. Today, consumers have so many choices when it comes to their banking needs that banks need to deliver a great online experience —"good" is no longer good enough. 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.

So how do financial institutions find a balance between fighting fraud, meeting compliance mandates and ensuring new customers have a seamless and compliant experience when opening an account?

☆☆☆☆☆

# The Advent of the Do It Yourself Movement

There are several ways and technologies that can be brought to bear to perform eKYC, AML screening and online identity verification. For financial institutions that rely on a government-issued ID document and biometric verification, the online identity verification process generally consists of a few key ingredients:

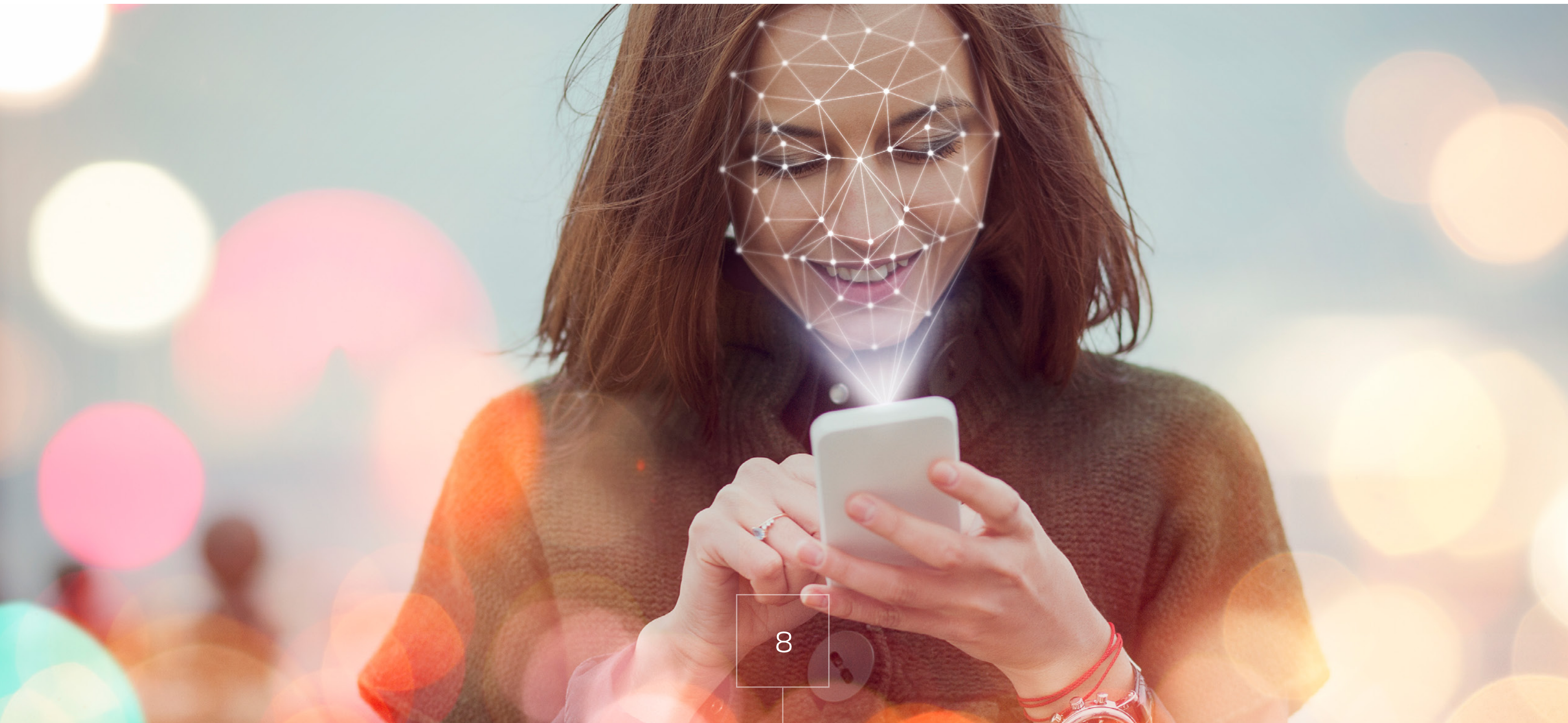
**Optical character recognition** (OCR) to extract data from the ID document

**ID verification** to ensure the ID is valid and undoctored

**Selfie capture and comparison to ID document** to increase identity assurance

Some 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.

Let's explore some of the challenges with this approach.



# Optical Character Recognition (OCR)

OCR is used for scanning and extracting the data from images of ID documents (e.g., driver's licenses, passports, etc.) captured via smartphones or webcams. This will generally include a person's name, address, photos, date of birth, height and weight. The data extraction process is usually fast and reduces or removes the need for manual data input.

But, OCR is not without its own set of challenges.

The better the quality of the source image, the easier it is for the OCR to extract and structure the (correct) data. But OCR was originally intended for reading black text against a white background, not for extracting key data fields from ID documents using small fonts and different colored backgrounds that may include holograms, watermarks and printing on glossy surfaces.

Adding to the complexity, when users take a picture of their ID document with their smartphone or webcam, multiple steps are required to extract and structure the information. The first step is to precisely recognize what kind of ID document is present. This enables the engine to properly structure the information read with the OCR, which means figuring out the first name, last name, date of birth and any other field of interest.

中华人民共和国驾驶执照
Driving License of the People's Republic of China
数 342600078654564

名称 Name 林徽因　性别 Sex 女　国籍 Nationality 中国

地址 Address 香港旺角爱油街2号

上海市公安局交通警察总队

出生日期 Date of Birth 1991-07-26

首次发行日期 Date of First Issue 2014-09-21

Class C1

有效期 Valid Period 2014-09-21 至 2021-09-21

Now, layer in the challenge of rectification. When people take pictures of their ID documents using their smartphones or webcams (versus using a flatbed scanner), these images usually need to be de-skewed if the image was not aligned properly and reoriented a few degrees clockwise or counterclockwise to make it readable. It often must take a color/greyscale photo and convert it to plain black and white to reduce blurred text and better separate black and white text from its background. These requirements often go well beyond the original design (and limitations) of OCR. When there is glare or blurriness in the ID image, the probability of data extraction mistakes is significantly higher.

OCR poses another challenge for financial institutions looking to offer an omnichannel experience by enabling customers to capture ID documents via mobile SDK, webcam or API. Unfortunately, not all channels produce the same quality image of the ID document. For example, webcam quality varies which means the quality and clarity of the pictures they take is not always as sharp as those taken by most modern smartphones. And the camera quality will impact the OCR's system ability to correctly extract the data from the image of the ID document — garbage in, garbage out. That's why native or mobile apps that take advantage of the smartphone's camera quality and auto-focus functionality provide better OCR data extraction compared to API or webcam channels.

Lastly, the number and variety of ID documents and subtypes makes the OCR job even more difficult. OCR is based, in part, on an extensive learning of the patterns that characterize a specific ID type, and this can make for a challenging learning task given the variety of ID subtypes (e.g. some printed in landscape, some in portrait mode). OCR is only fully usable if the data extracted is correctly structured and that requires the software to understand all the nuances and subtleties of different ID types around the globe.

There's clearly a great deal of science and technology behind the best OCR engines and even then, financial institutions are reliant on the image quality submitted by the user. If your financial institution is looking to expand geographically, it's imperative that your chosen OCR solution be able to correctly read the data from the ID documents issued in those countries.

## eKYC without Boundaries

Many large and growing Asia-Pacific banks have global aspirations. This means that their eKYC solution must naturally be able to scale across geographies. If you're leveraging a third-party eKYC solution provider, they need to support the countries, languages and ID types of your user community. It's not just a matter of supporting driver's licenses, ID cards and passports — these solutions must also support all the possible versions and permutations of each country's ID documents. In some cases, there may be as many as 15 versions of a particular driver's license — some issued 5 years ago, some issued 10 years ago, some printed in landscape, some in portrait, some for commercial drivers and some for driver's permits — each with their own unique set of security features.

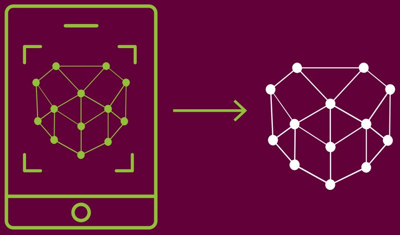
**At Jumio, we support more than 3,000 ID types across more than 200 countries and territories, enabling Asia-Pacific banks to more easily expand their geographic coverage.**

In some territories such as Singapore and Hong Kong, regulated financial organizations who deploy non face-to-face account onboarding technologies (eKYC) must engage a third-party auditor to assess the eKYC framework to determine that it is as effective and reliable as face-to-face. That's why it's imperative that your choice of eKYC technologies is crucial to ensure that it can withstand regulatory scrutiny.

## Facial Recognition Software

A number of facial recognition technologies and solution providers have emerged over the last few years, many of which are being considered and trialed in pilots or regulatory sandboxes as we speak. But, it's important to understand how these facial recognition solutions work, know their limitations and explore how they differ from face-based biometrics.

Facial recognition software can automatically identify an individual from a database of digital images or videos through a combination of AI and machine learning algorithms.



**Most facial recognition solutions start with a user uploading a simple photo of themselves when they enroll with an online banking service. If a user is successfully onboarded, facial recognition can be used to compare a recent selfie with the original selfie captured during the onboarding process, but there are some limitations.**

Facial recognition is ideal for matching a photo against a large database of other photos or videos, or comparing a high-quality selfie against another high-quality selfie. What's considerably more difficult is matching a recent selfie to a low-quality photo on a driver's license or passport. Pictures on ID documents are of notoriously poor quality and often small, greyscale and overexposed. The physical characteristics of people change over time — they may gain weight, lose their hair, grow a beard or start wearing glasses — which makes comparing a recent selfie to an older low-resolution ID picture difficult. This type of image comparison goes beyond the capabilities of most facial recognition software and requires a combination of technologies, including AI, machine learning and even human review.

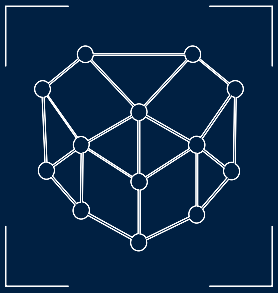
Another shortcoming of facial recognition software when applied to identity verification is that it cannot definitively assess the digital identity of an online user or assess whether they're physically present or spoofing the system. Sadly, cybercriminals are using spoofing attacks to outsmart such systems by using a photo, video or a different substitute for an authorized person's face. Given the fraud landscape, real-time liveness detection is absolutely critical for today's eKYC solutions — whether it's for initial customer onboarding or ongoing user authentication.

Reliably assessing the digital identity of an online user (and knowing with some assurance that they are who they claim to be) is the providence of identity proofing and unfortunately, a very real shortcoming of facial recognition.

## Identity Proofing versus Authentication

Identity proofing is the process an organization uses to collect and verify information about a person for the purpose of opening an account or issuing credentials (i.e. username and password) to that person. This typically involves three distinct steps: collection (capture evidence of identity), validation (confirm identity exists) and corroboration (ensure the digital identity belongs to a person).

Simply requiring a government-issued ID, such as a Singapore driver's license, does not mean that the person presenting the ID is the actual owner of the ID. This is why a selfie is often required as part of the identity proofing process to corroborate that the person holding the ID document is the same person behind the online transaction. Identity proofing is usually the first step in establishing your online account or profile. Unfortunately, facial recognition is really useful for one-to-many comparison of pictures, but not for binding a digital identity to a trust anchor, such as a government-issued ID.



**With biometric-based authentication, a biometric, such as a fingerprint or a 3D face map is captured, stored and bound to the new customer's identity during the initial enrollment process. This same biometric can then be leveraged for authentication events in the future (e.g., logging into your account or performing a high-risk transaction such as a wire transfer or password reset) by simply recapturing the biometric and comparing it to the baseline captured during enrollment.**

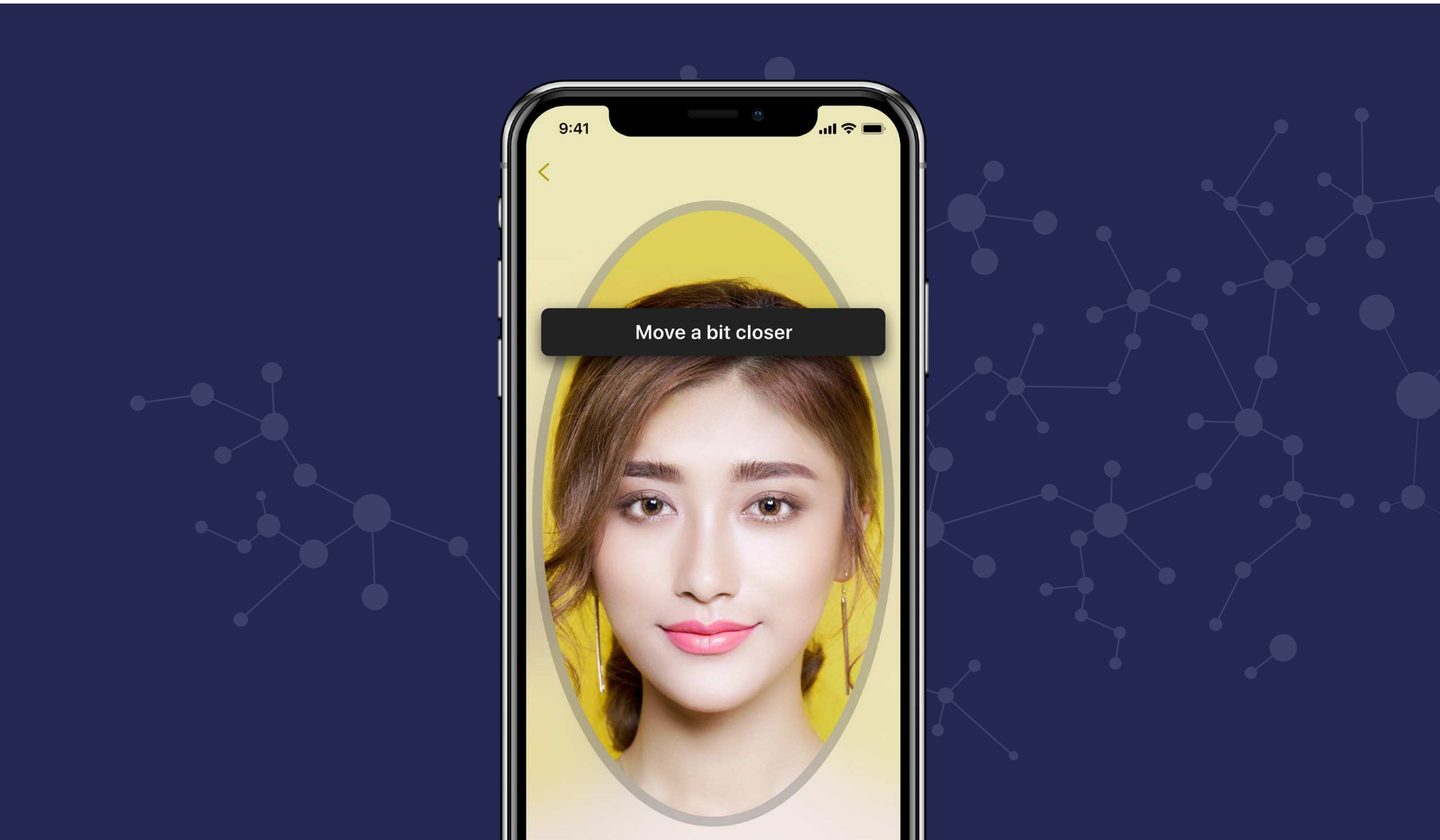
The biometric comparison takes seconds to perform and is significantly more secure and reliable than traditional forms of remote authentication, including knowledge-based authentication and SMS-based two-factor authentication. The elegance of this solution is that the user is not required to repeat the identity proofing process — they just need to take a new selfie.

This type of authentication is fundamentally different and outside the scope of what facial recognition software solutions can currently offer.

## A Word About Liveness Detection

Identity verification providers, such as Jumio, have embedded 3D liveness detection into the identity proofing process to better thwart fraudsters who are increasingly using spoofing attacks by using a photo, video or a different substitute for an authorized person's face to acquire someone else's privileges or access rights. A 3D face map is created based on up to 100 frames (images) from the smartphone. In addition to checking the authenticity of the ID document and ensuring that the image in the selfie matches the person pictured on the ID, Jumio is ensuring that the new customer is physically present without relying on any special hardware in the phone itself.

Until recently, there has not been a NIST-certified third-party test guided by the International Organization for Standardization (ISO) presentation attack detection (PAD) standard that can verify the abilities of liveness detection vendors to detect and repel spoofing attacks. For years this lack of oversight allowed biometric vendors to exaggerate their security claims and resulted in a false sense of security that many criminals took advantage of. Thankfully, objective spoof detection testing from iBeta/NIST is now in place and today's technology providers can be comprehensively evaluated, bringing much-needed transparency to the industry.

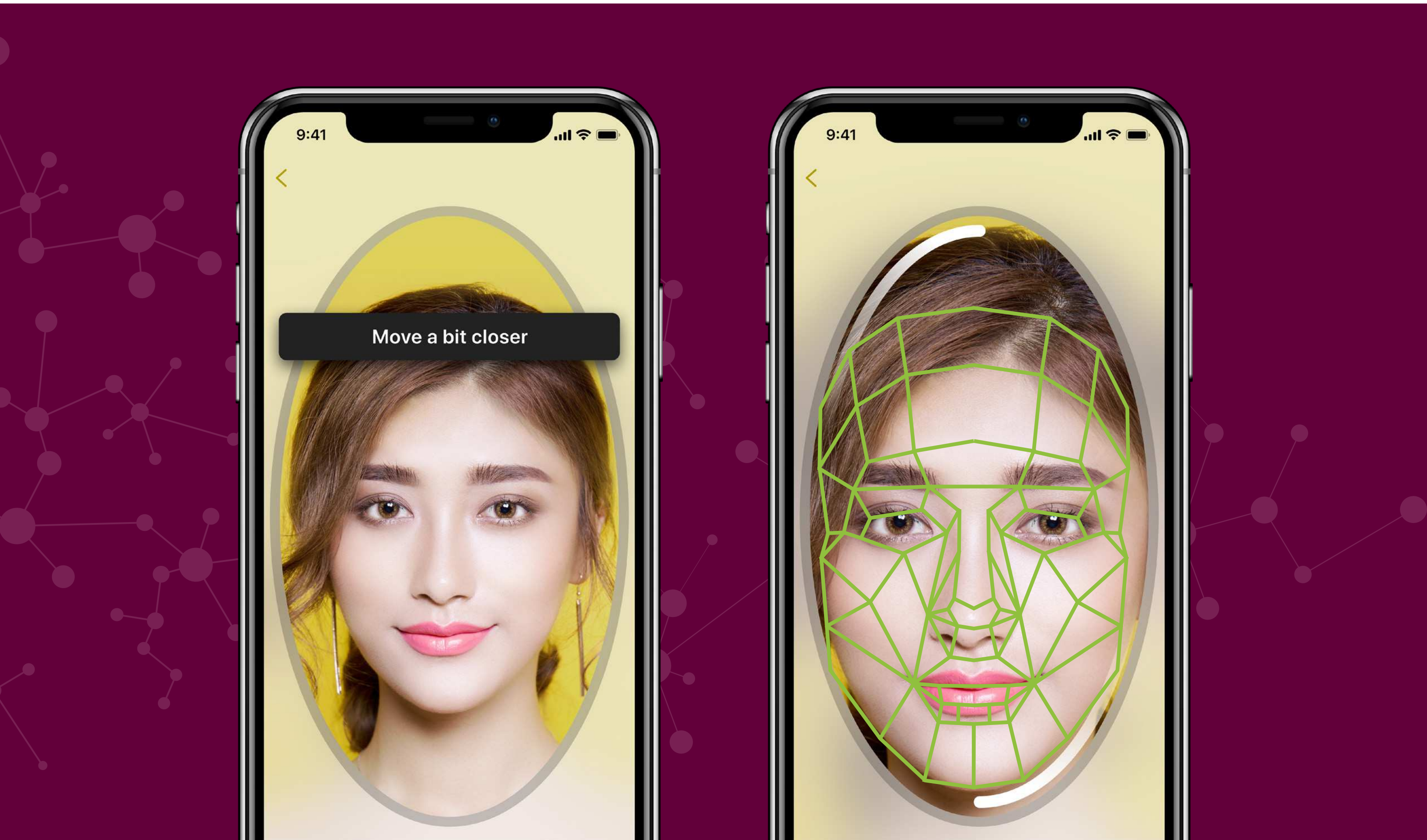


## The Rise of Biometric Authentication

According to Research & Markets, the global biometric authentication and identification market is expected to witness significant growth during the forecast period (2018-2023) registering a compound annual growth rate of 22.5 percent.

The increasing risk of data breaches, coupled with the explosive growth of handheld devices, increased mobile banking penetration and security concerns among customers, is expected to propel future global growth, especially in APAC. Within the biometrics space, face-based biometrics is gaining in popularity thanks to Apple and Samsung's face-based logins. Apple's Face ID is now the sole means of biometric authentication on Apple's iPhones, and it looks like the company will stick with this system for the foreseeable future.

**All of Apple's new mobile devices have abandoned Touch ID fingerprint authentication in favor of Face ID, an infrared, 3D face authentication system. In fact, estimates by Counterpoint Research suggest that more than one billion smartphones will have some form of a face unlock solution in 2020.**



Move a bit closer

## FAR & FRR: The Biometrics Scorecard Metrics

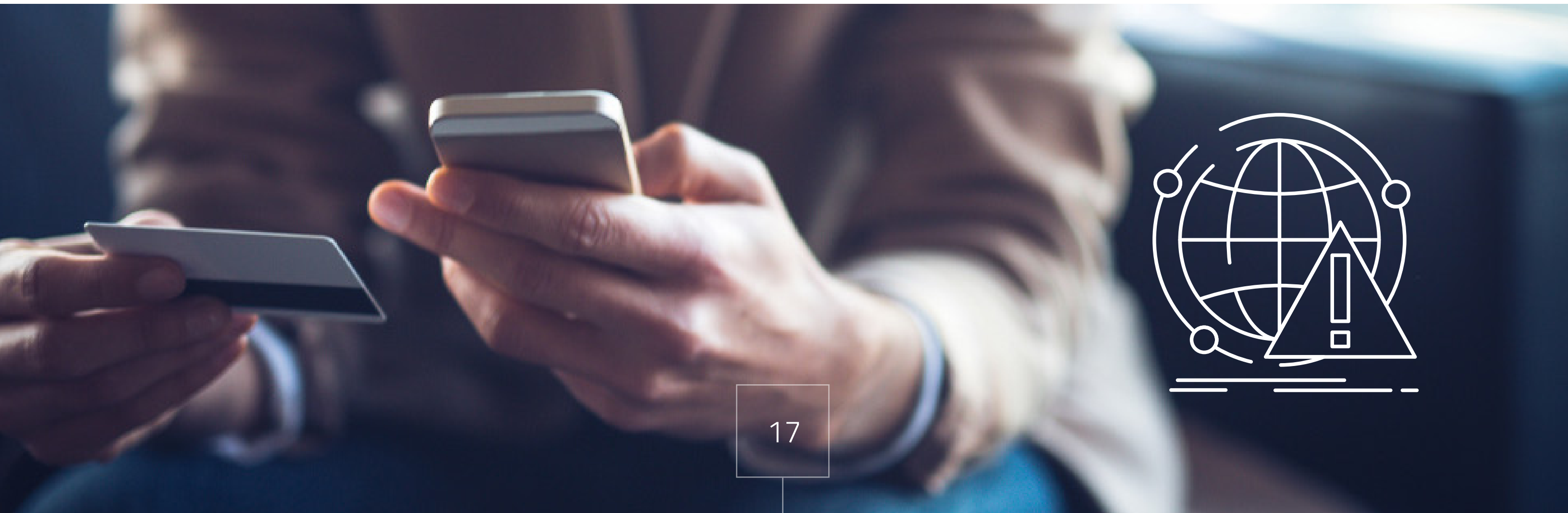
Whether you deploy facial recognition or biometric-based authentication, it becomes increasingly important to measure just how accurate these biometric systems are — and that's where metrics such as FAR and FRR fit in:

**False  Acceptance Rate (FAR)**
the percentage of identification instances in which imposters are incorrectly accepted.

**False Rejection Rate (FRR)**
The percentage of identification instances in which legitimate users are incorrectly rejected.

Any biometric-based verification or authentication solution that regularly rejects legitimate users would not only be inconvenient for the user — it would stop being a practical method on a day-to-day basis. On the other hand, biometric systems with a high false acceptance rate would compromise the security of the verification process and leave financial institutions vulnerable to fraud and non-compliance.

Each financial institution needs to evaluate whether the FAR and FRR ratio is acceptable for the application. Generally speaking, it's important to aim for a low FAR as those are usually judged as high-severity mistakes. Letting bad actors into your online ecosystem can often be more expensive and reputation-damaging than rejecting a few good users. This is especially true if a good user only needs to retake a selfie (or recapture some other biometric) to reapply as part of the onboarding experience. This means that companies may need to accept a non-zero percentage of FRR if they want to have a near-zero  FAR.



## AML Screening: PEPS, Sanctions & Adverse Media

Asia-Pacific is home to over 40 different regulators and varying complex approaches to AML regulation and client due diligence obligations. The increasing costs of client onboarding and AML compliance is reflected in the enhanced regulatory frameworks introduced by the Australian Securities and Investments Commission, Monetary Authority of Singapore, and the Hong Kong Monetary Authority. In China, regulators have made it clearer than ever that AML is a major priority, with the People's Bank of China recently posting on its website a notice from the State Council — the government's main executive body — that elevates AML to a key part of the national strategy on financial regulation.

As AML rules evolve, compliance remains a significant challenge for Asia-Pacific financial institutions. They need to ensure they stay consistently compliant with AML regulations or face severe reputational and financial penalties. This has been especially evident when some of the larger APAC-based lenders have ventured overseas, where regulations have traditionally been more stringent. China's state banks, for example, have faced sanctions from authorities in Europe and the U.S. for apparent AML violations.

Resource-constrained banks that fail to get it right with AML face severe consequences. Beyond the possible financial and reputational losses, the penalties for enforcement lapses under the region's various AML regulations range from hefty fines to full-scale business suspensions. Compared to the bigger corporations, many fintech startups might not have the resources and manpower to address KYC compliance requirements effectively, but technology can help reduce costs.

**Forward-thinking financial organizations must adopt a rigorous approach to AML compliance to future-proof against evolving regulatory requirements.**

The sheer number of online transactions that both authorities and banks are grappling with is placing an outsized toll on human resources and capacity constraints will struggle to adequately monitor.

Technology can be transformative and play a leading role in a robust and effective AML strategy. Regulators are actively encouraging institutions to apply new technologies such as big data and automated watchlist screening and ongoing monitoring to enhance AML supervision. Banks are also being urged to expand AML inspections and encourage information-sharing between various departments to get a more holistic picture of associated risks.

# A More Sensible, Integrated Approach to eKYC and AML

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 verification accuracy.

The chart below compares and contrasts point solutions with integrated eKYC and AML solutions, focusing on six key factors.

| **Factors to Compare** | **Point Solutions** (OCR+eKYC+AML) | **Integrated eKYC & AML Solutions** |
|---|---|---|
| **Price** | 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, businesses are forced to deal with incremental payments for user licenses and other fees associated with each individual software. | When purchasing an integrated software solution, prices are often given up front. With this in mind, a single solution with a scheduled payment system helps your company better budget, plan and predict any future payments. From a financial perspective, this is a much more efficient and flexible system. |

| Factors to Compare | Point Solutions (OCR+eKYC+AML) | Integrated eKYC & AML Solutions |
|---|---|---|
| **Usability** | Data is only able to interface across each system. This means that when information is entered into one system, it does not automatically sync with other point products you are using, increasing the need for double entry, or the monotonous task of rekeying information. Because point solutions only serve one function, the lack of integration often hinders the productivity of other areas in the business. | Data is integrated and is accessible across multiple areas of the business. More importantly, an integrated solution ensures that data only needs to be entered once. In addition, it is also much easier to learn how to operate one system, rather than learning a number of different interfaces, buttons and icons as each point solution is different. |
| **Implementation and Training** | Learning how to operate a software can be time-consuming and difficult. Multiplying this process can only lead to greater challenges and frustrations. By investing in a variety of point solutions, staff members are forced to take time away from day-to-day tasks, only to learn how to use another software. In addition, onboarding new staff becomes an extremely lengthy and complex process. | Although implementation and training for construction software can be a long process, it is much more efficient to learn one system well, than struggle through various ones. With a successful implementation, businesses can maximize their use of the single software, making the most out of their investment. With a number of staff familiar with one software, training and onboarding new staff is a simpler process. |

| **Factors to Compare** | **Point Solutions** (OCR+eKYC+AML) | **Integrated eKYC & AML Solutions** |
|---|---|---|
| **Verification Accuracy and Speed** | Point solutions for OCR and facial recognition are focused on specific parts of the identity verification process. OCR solutions require pictures of ID documents captured under ideal conditions. Most facial recognition solutions are not tethered to a government-issued ID so they assume that the person creating the account and capturing the initial (enrollment) picture is a legitimate user. | Integrated eKYC and AML solutions include OCR and face-based authentication but also leverage AI, machine learning, computer vision and human expertise to yield a much lower FAR and FRR. These solutions generally connect a government-issued ID to a selfie. OCR is just one of many technologies that are brought to bear to determine the legitimacy of an ID document. These solutions also leverage computer vision and AI to determine whether an ID is fraudulent. Plus, they will combine identity verification with face-based authentication which rely on 3D face maps created during the selfie capture process and based on up to100 frames (images) from the smartphone. |
| **User Experience** | When financial institutions take a DIY approach they personally need to ensure that the component point solutions work together to deliver a positive user experience. | Integrated solutions ensure that the end-to-end experience, from initial ID capture to final verification decision, is delivered quickly and simply within the app or online. |

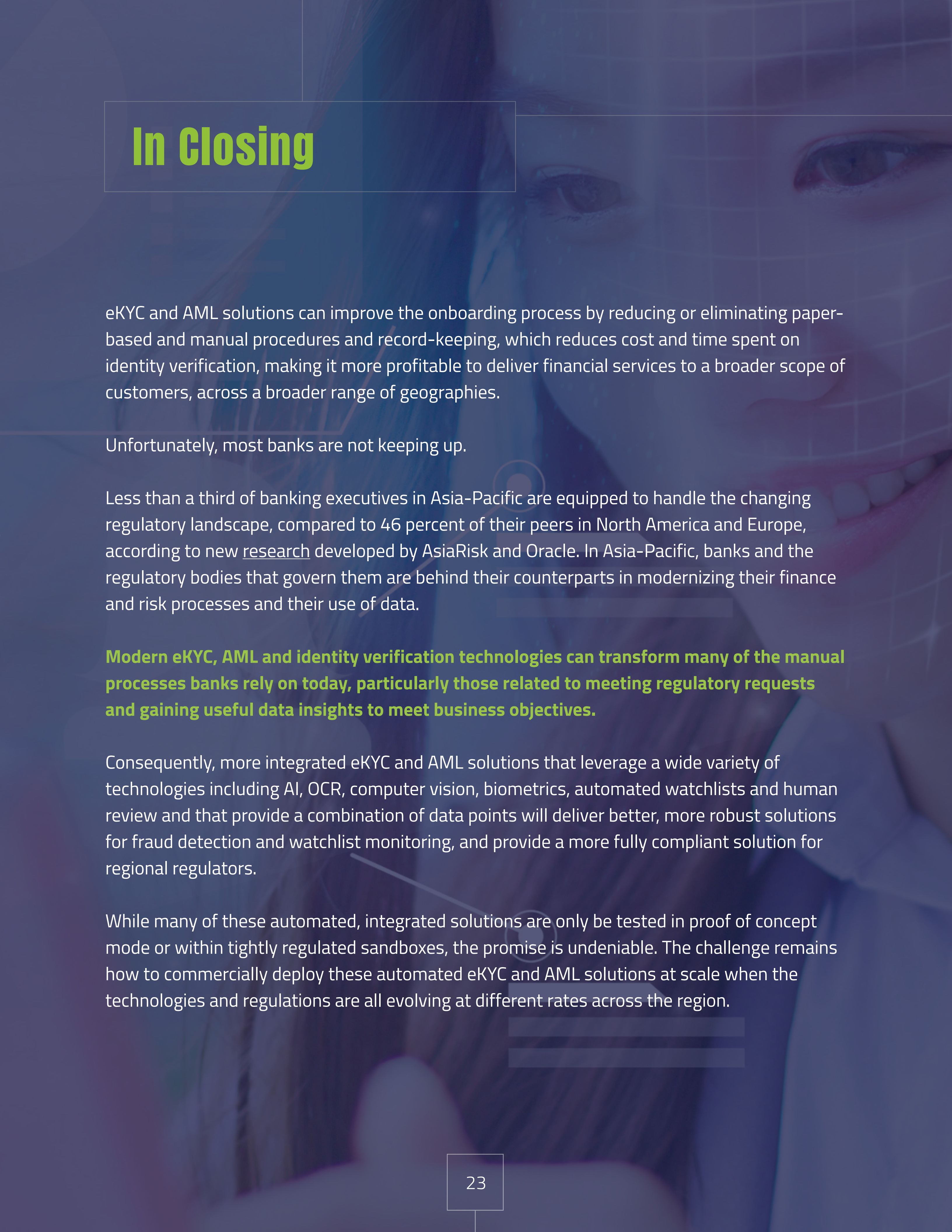
| Factors to Compare | Point Solutions (OCR+eKYC+AML) | Integrated eKYC & AML Solutions |
|---|---|---|
| **Customer Support** | Relying on multiple software vendors for customer support can easily become a messy and disorganized process. By cobbling together a variety of software, diagnosing problems and the origin of issues becomes a more difficult task. Rather than getting work done, financial institutions are forced to investigate problems or call various support teams even for the simplest of resolutions. | With an integrated software solution, dealing with the same support team can provide a great deal of comfort. Furthermore, support from just one vendor can save time and effort by allowing businesses to address multiple issues at once. By having one dedicated support team, representatives become more familiar with your business. With this added experience, support teams have more data to help you find resolutions much quicker. |

Cobbling together various software can lead to a lack of integration, ultimately leaving financial institutions disjointed, disorganized and out of compliance.

To address these shortcomings, the better long-term solution is to partner with experienced integrated software solutions. More seasoned solution providers have had more time and experience to develop and refine the processes and the technologies that often result in higher accuracy and faster verification speed.

Some solution providers, for example, employ human review to tune their AI algorithms, and this expertise is not easily replicated by hiring your own team of manual reviewers. Companies often understate the challenge and complexity of developing in-house systems and processes from scratch. They also don’t properly account for the time it takes 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. Another important consideration with point solutions is the time, costs and bandwidth associated with maintaining and upgrading these solutions over time.

**Bottom Line: There’s a very steep learning curve involved when stitching together point solutions which is too often underestimated and underappreciated.**



# In Closing

eKYC and AML solutions can improve the onboarding process by reducing or eliminating paper-based and manual procedures and record-keeping, which reduces cost and time spent on identity verification, making it more profitable to deliver financial services to a broader scope of customers, across a broader range of geographies.

Unfortunately, most banks are not keeping up.

Less than a third of banking executives in Asia-Pacific are equipped to handle the changing regulatory landscape, compared to 46 percent of their peers in North America and Europe, according to new research developed by AsiaRisk 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.**

Consequently, more integrated eKYC and AML solutions that leverage a wide variety of technologies including AI, OCR, computer vision, biometrics, automated watchlists and human review and that provide a combination of data points will deliver better, more robust solutions for fraud detection and watchlist monitoring, and provide a more fully compliant solution for regional regulators.

While many of these automated, integrated solutions are only be tested in proof of concept mode or within tightly regulated sandboxes, the promise is undeniable. The challenge remains how to commercially deploy these automated eKYC and AML solutions at scale when the technologies and regulations are all evolving at different rates across the region.

# 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 augmented intelligence, 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 helped companies verify nearly 200 million identities worldwide and we'd love to help yours be the next. Contact us to learn more about our eKYC and AML solutions.

JUMIO®

Jumio.com