

A woman with dark hair is smiling and looking down. A semi-transparent digital face overlay, composed of a network of white dots and lines, is positioned over her face. The background is a soft-focus indoor setting. The bottom half of the image transitions into a solid purple gradient.

ACHIEVING BETTER AML AND KYC WITH MODERN BIOMETRICS

WHITE PAPER

INTRODUCTION

Any business which needs to conform to anti-money-laundering (AML) and know-your-customer (KYC) regulations faces a challenging time. Despite the unsettled economic backdrop, customers are switching from analogue to digital channels in ever greater numbers. And the lower friction of digital means that transaction volumes are rising. On the one hand, it means business growth, new sales channels, new ways to interact with customers and build long-term and high-value relationships.

On the other hand, it means more transactions requiring AML and KYC checks. If companies stay with their legacy ways of working, this inevitably means complexity and delays for customers – delivering a poor customer experience. It could also increase the risk of systems allowing fraudulent or illegal transactions. This comes with potentially high financial, reputational and brand costs. At the same time, compliance costs are rising. Most AML and KYC, CDD (Customer Due Diligence) screening technologies require significant manual effort, making them inefficient and costly. And the average fine for money laundering in 2021 was over US\$34 million¹. The answer is biometrics, driven by the latest in Artificial Intelligence (AI).

Using advanced biometric technology, businesses can onboard customers remotely – capturing all the relevant forms of ID and other documents required for KYC – in just seconds. And once customers have onboarded, they can then login simply by taking a selfie using a mobile device or webcam.

With the right technology and the right approach, biometric-based digital onboarding and authentication combine the rigor and security standards required for compliance with the speed and ease of use which customers demand. In this paper, we explain how biometrics can help to achieve your business goals and how to get started with the integration process.

WHY WE NEED A NEW APPROACH TO AML

The way we do business and consume services is undergoing a massive and rapid change. Between 2020 and 2025, the volume of global digital payments will increase by 80%². The worldwide financial services sector, including the banking industry, grows at a rate of 11% a year³. Nor is this explosive growth confined to financial services. The real-estate sector will grow by 46% between now and 2030⁴. The online global art market will expand by 494% over the next two years to 2024⁵. The worldwide crypto-assets sector is growing at a rate of 11% a year⁶. And so on.

RISING VOLUMES BRING GREATER RISK

With rising transaction volumes comes increased risk of money laundering, terrorism financing, the drugs trade and other illegal activities. Worldwide, criminals launder an estimated US\$800 million to US\$2 trillion every year – representing up to 5% of global GDP⁷. In response to this, states issue ever-tighter politically exposed person (PEP) lists, increased sanctions and stricter standards for the AML and KYC checks institutions are expected to carry out.

Scandals such as the Panama papers and the Pandora papers have brought the issue of money laundering and tax evasion far more into the public eye than ever before. And in a time when the state needs all the revenue it can gather, the realisation that tax evasion alone is costing governments up to US\$600 billion a year is prompting legislators and regulators to look for new ways to clamp down on non-compliance⁸.

2 PWC. (2021). Navigating the payments matrix: Charting a course amidst evolution and revolution. Available online at: <https://www.pwc.com/gx/en/industries/financial-services/publications/financial-services-in-2025/payments-in-2025.html>

3 Yahoo Finance. (2022). Financial services global market report 2022. Available online at: <https://finance.yahoo.com/news/financial-services-global-market-report-084500225.html?guccounter=1>

4 Statista. (2022). Size of the global real estate market in 2021, with forecasts from 2022 to 2030. Available online at: <https://www.statista.com/statistics/1289905/global-real-estate-market-size/>

5 My Art Broker. (2022). The online global art market around the world. Available online at: <https://www.myartbroker.com/investing/articles/online-global-art-market-around-the-world>

6 Fortune Business Insights. (2021). Cryptocurrency market size, share & COVID-19 impact analysis. Available online at: <https://www.fortunebusinessinsights.com/industry-reports/cryptocurrency-market-100149>

7 United Nations. Money laundering. Available online at: <https://www.unodc.org/unodc/en/money-laundering/overview.html>

8 IMF. (2019). Tackling tax havens. Available online at: <https://www.imf.org/en/Publications/fandd/issues/2019/09/tackling-global-tax-havens-shaxon>

THE NEED FOR IMPROVED AND STREAMLINED AML

In most jurisdictions, these industries are all subject to AML regulations. In any fast-growing sector, that is a challenge. Companies need accurate and reliable ways to process ever growing volumes of KYC and AML checks, without introducing delays or difficulties that undermine the customer experience.



And this is particularly challenging now, when jurisdictions around the world tighten AML laws and increase the regulatory burden. In the EU, the latest Sixth Anti-Money-Laundering Directive (AMLD6), which tightens both the definition of money-laundering offences and liability, passed into national law in December 2020. The regulation makes it clear – new customer registration requires PEPs (Politically Exposed Persons) and sanction lists verification and proper risk assessment policies to be in place.

In addition, there are local laws passed as well. In 2020, France passed its new and tougher ordinance (n° 2020-115) into law, applying AML laws to new sectors and enhancing company due diligence obligations⁹. In 2020, the German parliament passed the Draft Act for the Effective Prosecution of Money Laundering, updating and strengthening its 2018 money-laundering law to comply with the terms of AMLD6¹⁰.

⁹ Global Compliance News. France: French ordinance passed to strengthen law combating money laundering and the financing of terrorism. Available online at: <https://www.globalcompliancenes.com/2020/06/20/france-french-ordinance-passed-to-strengthen-law-combating-money-laundering-and-the-financing-of-terrorism-10062020/>

¹⁰ Comply Advantage. Germany Money Laundering and the AML Act. Available online at: <https://complyadvantage.com/insights/anti-money-laundering-germany/>

BALANCING REGULATOR AND CUSTOMER REQUIREMENTS

As the combination of ever higher transaction volumes and tougher laws was not challenging enough, customer requirements have also evolved. According to Experian Global Identity and Fraud Report, 2021, 60% of consumers have higher expectations for their online experience than pre-pandemic, while 55% still say security is a top priority, 74% of consumers chose physical biometrics as their preferred security method¹¹. And that's a challenge for financial services institutions.

The more complicated KYC and AML checks become, the more they impact the customer experience. This is particularly true during the onboarding process, with its often-cumbersome KYC checks. As a result, during the last six years, financial-services abandonment rates during onboarding rose from 40% to 68%¹².

The question then, is how to process ever-greater volumes of AML and KYC checks, in a way that is compliant, easy for the customer to follow and provides a better customer experience. It's precisely this challenge which today's industry-leading biometric-based identification and authentication technologies are designed to address.



¹¹ Experian. (2021). 2021 Global Identity and Fraud Report: The impact of COVID-19 on digital customer experience and fraud prevention. Available online at: <https://www.experian.com/decision-analytics/global-fraud-report>

¹² Signicat. (2021). Why are users continuously abandoning onboarding to financial services year upon year? Available online at: <https://www.signicat.com/the-battle-to-onboard-2022/abandonment-to-financial-service-onboarding-over-the-years>

WHY BIOMETRICS WITH FACIAL RECOGNITION IS THE FUTURE OF AML

SIMPLE AND CUSTOMER-FRIENDLY IDENTITY VERIFICATION PROCESS

The pandemic has changed the way businesses are conducted. Due to social contact or distancing restrictions many were not able to undergo an in-person onboarding process or present their ID documents in person. With AI-driven biometric technology, remote customer onboarding is possible in just three steps, taking only seconds. The customer takes a photo of her approved form of ID and then takes a selfie.

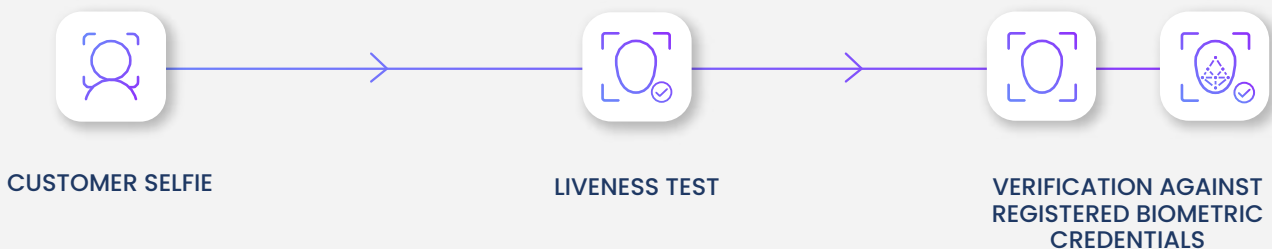
CUSTOMER ONBOARDING AND VERIFICATION STEPS



The customer gets a quick and seamless onboarding experience while the business gets assurance of the genuine legitimate customer, protection against fraud and money laundering with robust KYC and AML processes in place. In addition, it reduces the time and cost involved in onboarding new customers by replacing inefficient manual workload while adhering to compliance and security.

From this point on, the customer uses her own device to access a service instantly, no password is required.

CUSTOMER AUTHENTICATION PROCESS



NO TRADE-OFF WITH SECURITY

Biometric technology offers multiple security layers for a robust, fraud-proof digital onboarding and compliance:

NEAR FIELD COMMUNICATION (NFC) READING

Most identity documents and electronic passports follow international standards and have an NFC chip that stores the holder's data in digital format, including the signature or the photograph printed in the document. Smart phones and tablet devices are equipped with robust cameras and NFC readers which enable customers to easily scan their ID document NFC chips. Once scanned, the data from the ID document is matched to the NFC one, confirming the identity. In cases where security is critical, NFC reading provides assurance for an accurate customer identity verification.

VIDEO ONBOARDING

In some countries such as Germany, Spain, Mexico, etc. video onboarding is a requirement. It can be performed using assisted and unassisted video onboarding. In the first case the call will be taken with an online agent and in the latter the customer is required to take a short video of herself. Video onboarding can provide more confidence in new customers.

DOCUMENT VERIFICATION

Biometric technology can verify the authenticity of documents presented by a customer. Biometric algorithms analyse and compare the security features on ID documents (which are hard to spot with manual checking) against the stored templates, ensuring higher level of accuracy and protection against fraudulent IDs.

CONNECTION TO GOVERNMENT AND OTHER DATABASES

ID document data can also be matched against government data sources to ensure accuracy and validity of records.

AML SCREENING

Biometric digital identity verification can incorporate a real-time AML/PEP risk screening for due diligence and risk mitigation ensuring compliance with KYC and AML regulations. Businesses can securely reduce dependence on inefficient and costly manual review processes. In addition, as a part of the continuous customer due diligence, biometric technology can run recurring screening in the background and raise notification alerts.



ELECTRONIC SIGNATURE AND DOCUMENT SUPPORT

Digital onboarding and identity verification processes can support additional document uploads – such as visas, marriage certificate, applications, contracts, etc. They also provide e-signature functionality to facilitate legal or financial consent with agreements.

MULTIPLE BIOMETRICS

Biometric data is considered the most secure method of identification. It is very challenging to replicate. However, adding a second biometric identifier such as voice or digital fingerprint scan will fortify security providing the highest level of protection against identity fraud or account hacking. It can constitute a component of a two-factor or multi-factor authentication as well.

DATA PRIVACY BY DESIGN

Advanced biometrics provide the most secure way for customer onboarding data to be extracted and analysed. The data is converted and encrypted before being securely transferred to a data holder. This functionality prevents it from being deciphered or reverse engineered. In addition, a unique time stamp token is added which makes it impossible for bad actors to leverage.

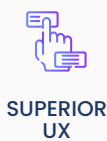
GEOLOCATION

Combining biometrics data with geolocation helps to identify customer location, including the countries that businesses are unable to serve prior to customer onboarding.

LIVENESS TEST

A liveness test determines whether the person in front of the camera is real and present – not a spoof or a presentation attack. It can be performed in two ways – active or passive. An active liveness test involves asking the customer to turn their head, blink or perform some other actions to prove they are both real and present, rather than simply an image or a video recording. It can however cause friction in customer experience and be susceptible to fraud attacks. A system that uses passive liveness doesn't require the customer to carry out any actions. It leverages deep learning techniques to analyse images, can detect involuntary eye or subcutaneous muscle movements – none of which would be detectable in recorded media.

With a limited number of prescribed actions, fraudsters might get an idea of what parameters to attack and how to break or bypass the liveness check. The passive liveness method, however, does not directly identify any security parameters ensuring reliability.



Passive liveness protection is tested with ISO Presentation Attack Detection testing in accordance with 30107-3.

MOBILE DEVICE BIOMETRICS VS. IDENTITY VERIFICATION TECHNOLOGY

Mobile device biometrics eliminate the use of passwords and are contained only within customers' handset. They only serve to unlock a password container and send the saved password to the remote server. It doesn't mean the user's identity is proven. As the remote server never confirms the user, instead it only confirms the use of a correct password. If multiple users register their faces or fingerprint scans on the same device and all biometrics revert to pin codes on failure, they bypass the security and can access personal accounts which leads to serious flaws in account protection.

In contrast, **identity verification biometrics** capture, encrypt and securely transmit customer biometric credentials to a remote server where passive liveness test and recognition occur. This ensures that the remote system or service can confirm the exact identity in front of the camera at the time of capture. The users can access the account only after their identity is confirmed. Even if the device biometrics, PIN code or entire handset get compromised, the remote identity verification technology will ensure account protection and provide secure access to the true enrolled customer.

SUPERIOR CUSTOMER EXPERIENCE

With the growth of fintech companies alongside traditional banks, brokers, funds and other players, the financial-services industry has never been more crowded. The advent of open banking and API-driven business models gives the customer more ways to shop, buy and service their financial needs than ever before. This makes customer experience more important than ever. With competition fiercer than ever, offering an outstanding experience is an important way to differentiate yourself from the competition. According to research by McKinsey, for every 10% uptick in customer satisfaction, a company can increase revenues by 2-3%¹³. Biometric-based identity verification technology guides new customers through the capture process, requires minimal cooperation and provides real-time feedback to maximise the onboarding outcome. By offering simple, seamless, and easy-to-navigate onboarding and identification services, financial institutions deliver a winning customer experience right from the point of first contact. It removes barriers to conversion and retention, helping to elevate the value of each transaction and of each customer. Having the technology and the standard of engineering required to guarantee accuracy and security, a good biometrics system will also fit seamlessly into your customer-experience philosophy. It works with the widest range of devices and operating systems, including mobile devices, desktop browsers, web kiosks and more.

CONCLUSION

With the right approach, the right technology and support, biometric identity verification technology can streamline KYC and AML processes, provide enhanced data security and fraud protection to businesses and their customers. The technology can be deployed in a matter of weeks and delivers robust and accurate KYC, enhanced operational efficiency with customer onboarding and the requisite checks to ensure legal and regulatory obligations. All while providing a first-class customer experience: fast, seamless, secure and reliable.

ABOUT FACEPHI

Facephi works with customers to create more secure, accessible and fraud-free digital experiences and processes.

Established in 2012, the company specialises in secure and user-friendly digital onboarding, identity verification and authentication solutions using cutting-edge biometric technology. Facephi is committed to unlocking the power of digital identity for all in accordance with the principles of flexibility, inclusion, and consent-based ethical use. To do so, the company develops proprietary multi-biometric solutions and is committed to innovation with artificial intelligence, machine learning and blockchain technology.

With more than 250 clients globally, Facephi boasts 300 million users across various industries, including banking and financial services, fintech, crypto, health, travel and transportation, shared mobility and more.

Headquartered in Spain, Facephi has subsidiaries in EMEA, APAC and LATAM.

For more information, please visit www.facephi.com