TRANSFORMING FINANCIAL CRIME COMPLIANCE: THE ROLE OF DIGITAL IDENTITIES

FINTRAIL

REFINITIV®

An LSEG Business

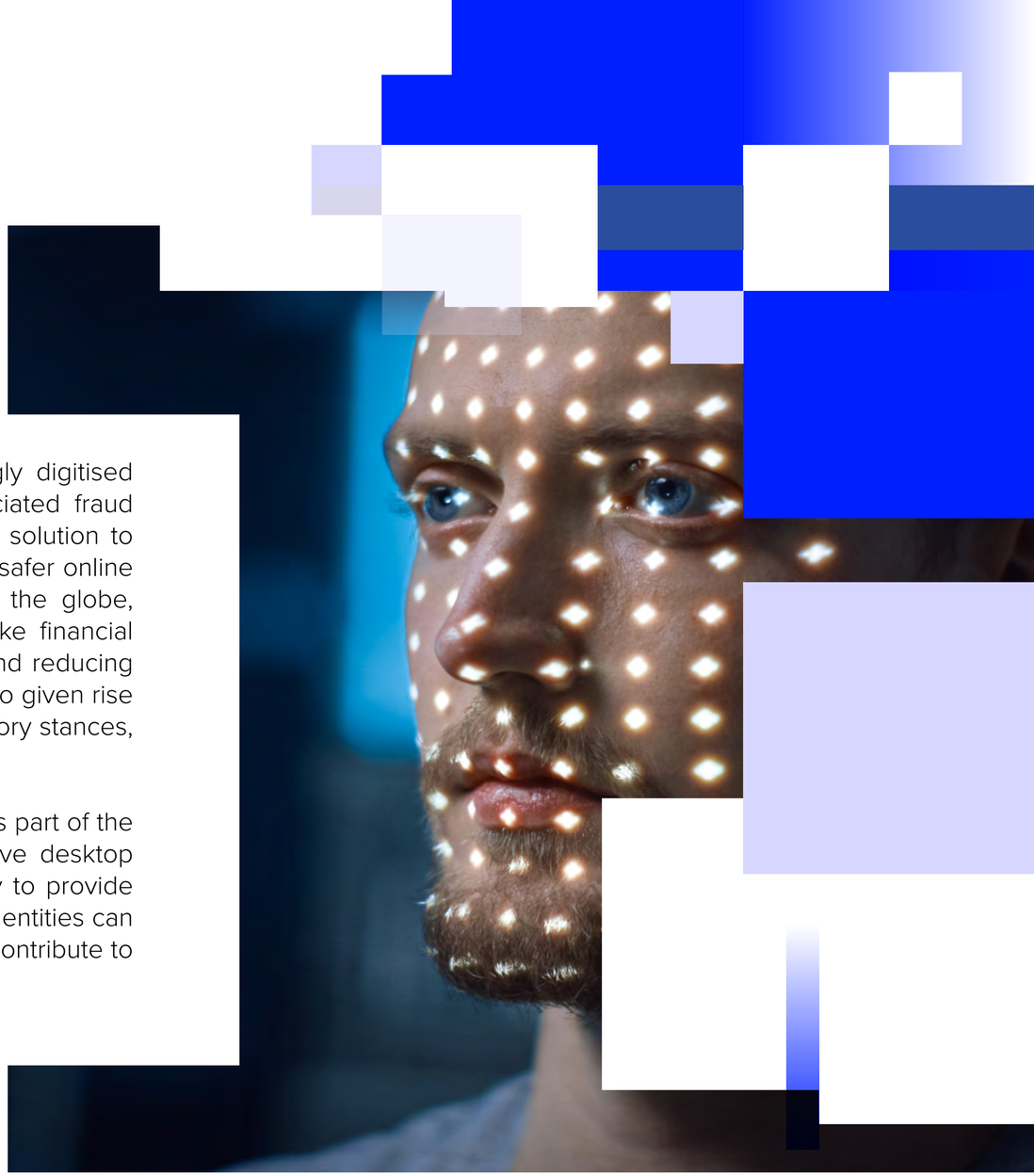
CONTENTS

INTRODUCTION

Digital transformation has reshaped the financial services industry, bringing benefits to consumers, such as convenience, multi-channel banking services and reduced time to access new products. Whilst the customer experience has benefited, criminals have adapted their processes to take advantage of digital banking and circumvent traditional controls. Today, fraud is one of the biggest threats facing financial institutions, with global rates remaining high post-pandemic, making it a key area of focus for regulators and governments. As financial services become more digitalised, remote onboarding processes open the way for fraudsters to impersonate individuals with stolen, fake or synthetic identities. Financial institutions must respond to these new threats by leveraging more innovative, robust and technology-driven Know Your Customer (KYC) processes.

Against the background of an increasingly digitised financial services industry and the associated fraud threats, digital identity has emerged as a solution to verifying identity and creating trusted and safer online spaces. With promising initiatives across the globe, such schemes boast powerful benefits like financial inclusion, streamlining banking services and reducing fraud. Conversely, these schemes have also given rise to concerns about implementation, regulatory stances, and security and privacy.

This white paper explores digital identity as part of the digital KYC journey, incorporating extensive desktop research with expert industry commentary to provide an in-depth understanding of how digital identities can best serve anti-financial crime efforts and contribute to the evolution of financial services.



USE CASE FOR DIGITAL IDENTITIES AND DIGITAL KYC

As defined by the UK's Department for Science, Innovation and Technology[1], a digital identity is a digital representation of identity information, like name and age. It can also contain other static information, like address, or biometric information, like a fingerprint or face scan. It enables individuals to prove who they are during interactions and transactions without presenting physical documents.

Unlike traditional paper-based sources of ID like passports, digital IDs use digital channels to remotely authenticate identity. Digital IDs can be issued by various bodies, such as national governments, and individual firms or consortiums of firms.

[1] UK Department for Science, Innovation and Technology

Technology adoption has altered onboarding processes dramatically in the last few years, with financial services increasingly seeing customer demand for multi-channel journeys. The number of smartphone mobile network subscriptions worldwide reached almost 6.6 billion in 2022 and is forecast to exceed 7.8 billion by 2028 – an estimated 75% penetration rate globally[2]. The unprecedented worldwide events of the pandemic brought both rapid and unexpected digitisation, which in turn opened the way to sky-high levels of fraud. Whilst fraud levels have diminished slightly since the pandemic, they remain a key concern for profit-driven financial institutions that may bear fraud losses. Customer expectations of quick and easy onboarding experiences must reconcile with compliance obligations in all phases of the end-to-end customer onboarding journey.

Within this customer journey, upholding a positive customer experience is more important than ever. Users ranging from Generation Z to technology-savvy older cohorts are accustomed to using technology for their financial services with minimal friction. A recent study has shown that 68% of consumers abandoned a financial services onboarding journey in 2022, up 5% on the previous year. A third of these abandoned applications were due to not having the right identity credentials[3].

In a competitive landscape, offering a quick and straightforward onboarding process is paramount to obtaining and keeping business — directly impacting a firm's survival.

"I think we're at a point where some elements of the customer journey may get worse for customers because of what financial institutions are required to do from a fraud perspective. It will be interesting to see if consumers are willing to have that friction in for added protection. It's a really challenging time for firms to get that balance right. Providing good experience, meeting regulatory expectations, but also the pressures to add more friction to reduce fraud."

KATHRYN WESTMORE,
Senior Research Fellow,
Centre for Financial Crime and Security Studies

As the appetite and expectations for frictionless onboarding grow, onboarding drop off rates suffer. According to a report by Forrester[4], over 64% of banks reported lost revenue due to problems with their current onboarding processes. Issues such as the process taking too long or too much information being requested in the process are the primary drivers for consumers leaving an application.

Whilst customer identification occurs at the first point of onboarding, it is also required during trigger events, change management, and during payments and disbursements. Given that it has the most commercial incentive, many firms concentrate on a good customer experience at the initial onboarding stage, potentially neglecting areas further along the journey. This may include instances where ongoing monitoring may flag and stop payments or transactions, requiring more information from the customer, or periodic reviews which require a refresh of the client information held on file. These other points of contact may lead to frustrated or unsatisfied customers who may decide to discontinue banking with a financial institution.

[2] Statista
[3] Signicat – Battle to Onboard
[4] The State Of Digital Banking, 2022

Organisations want to enable legitimate customers to update their information with minimal friction, whilst at the same time making sure there are robust tools and procedures in place to detect genuinely high-risk changes and stop fraudsters in their tracks. One interviewee explained this difficulty, describing how at onboarding, firms collect basic and often straightforward KYC information, but may require more information as customers start transacting.

> **"If a customer has just been onboarded via selfie check, then often requesting that additional information is when firms also see attrition happening, as it's either too difficult to provide or it is not readily available."**

According to one head of AML interviewed for this report, abandonment can appear differently depending on the jurisdiction. In regions with high levels of digital technology, people might be reluctant to share extra information due to privacy concerns. In other areas where there is low technology adoption and more individuals are unbanked, customers may be onboarded quickly with a selfie taken from their mobile phone, but may fall off at the latter stages of the onboarding process when more inaccessible information such as proof of address is required.

Cost is a prevalent consideration throughout the journey, including both the opportunity cost of losing potential customers due to cumbersome onboarding procedures, and compliance resource drain. For firms that require more information from customers, the burdensome and time-consuming back-and-forth is not only a deterrent from a customer's viewpoint, but also an expensive exercise. Funnelling human resources into manually sourcing extra documentation or clarifying specific details is laborious, clunky and expensive. One survey of banks from 2022 found that a single KYC review costs between $1,501 and $3,500 for two-thirds of respondents. For 41% of respondents, around 31-50% of KYC review tasks are conducted manually, in a siloed environment that requires significant human intervention[5]. Another report puts the average cost of working through an alert at around £20 (approximately $25) each time, with 25% of alerts being reviewed by level-two senior analysts[6].

Beyond gaining new customers and optimising the onboarding process, digital identities can provide revenue-generating opportunities for financial institutions through cross-selling. One interviewee used the example of an individual taking out a mortgage with a bank where they already have an account, requiring them to visit a branch with specific paperwork. Using digital identity verification for cross-selling, eliminating the need to go to a physical branch, can hugely benefit the customer journey, reducing onboarding and operational costs, and capturing new business from existing customers. These use cases exemplify the need for firms to prioritise identity verification as a prominent feature of their overall business strategy.

[5] International Banker
[6] False positives: a growing headache – The Global Treasurer

The Global Data Consortium paper, 'Winning the Financial Services Onboarding Battle by Repositioning eIDV ROI'[7] states that the return on investment for technology to support digital identity is worth the outlay: "A dollar spent on onboarding in electronic ID verification (eIDV) is worth $412 in Customer Lifetime Value (CLTV)." The higher the CLTV, the better the revenue and thus the growth of an organisation. Recognising that one of the greatest challenges in onboarding is identity verification, where chances of abandonment are high, the report highlights the need to rethink the approach to onboarding in terms of customer acquisition costs (CAC). Firms must consider eIDV as a critical CAC, because even a small investment in identity verification technology provides significant returns. Adopting identity verification in a digital customer journey will help reduce the cost of onboarding customers whilst also creating a more streamlined process.

Furthermore, the market looks at identity verification checks as price per check as opposed to per match. Whilst price per check is cheaper, it can return zero matches if it is not checking against the right data set. Conversely, price per match might be higher, but will always return a match, as it searches in many data sources within a country. A single data source in a country will not always return a match, there must be subsequent checks for maximum coverage, leading to better conversion, reduced abandonment and better CLTV.

Use cases for digital identities:

- **Age verification:** providing access to online services or products that are age restricted, such as gambling
- **Anti-money laundering compliant onboarding:** allowing regulated firms to verify identity as part of their onboarding process and keeping them compliant with regulations
- **Fraud prevention:** combating fraud by using identity signals to verify that an individual is who they say they are, reducing the risk of identity theft
- **Employment:** timeframes for right to work checks and verifying employees' identities can be dramatically reduced, improving the time to onboard new employees
- **Public services:** digital ID is a key enabler for modernising public services such as healthcare, welfare payments, certifications and licences
- **Government and business:** digital ID can streamline interactions between governments and the private sector in areas including corporate registrations, taxes, economic support, permits and authorisations

[7] GDC Report

CURRENT STATE: DIGITAL IDENTITY AND DIGITAL KYC

As remote onboarding is now a standard expectation for many, some regulators have responded by publishing guidelines for financial institutions. The European Banking Authority (EBA) has produced comprehensive guidelines for remote customer onboarding, touching on document authenticity, ongoing monitoring and outsourcing customer due diligence[8]. The Hong Kong Monetary Authority (HKMA) has released information on best practices for remote onboarding initiatives[9], highlighting the risk-based approach and details of ongoing monitoring and the use of technology.

[8] EBA
[9] HKMA

The consensus is that remote onboarding is the way forward, and that finding ways to verify and authenticate customers online requires some form of digital identity verification. This verification process allows a firm to collect, validate, verify and authenticate an identity of a person digitally. The concept of digital identity has evolved significantly with technological developments, moving from user-generated usernames and passwords to multi-factor authentication to biometrics. More recently, the concept of digital identity has included identity wallets, as featured in a proposal to amend the European Union's electronic Identification, Authentication, and Trust Services (eIDAS). This proposal, known as eIDAS 2.0, focuses on creating a framework for digital identity wallets for both individuals and businesses[10]. As the notion of digital identity further evolves, it moves to encompass interoperable, reusable digital identities. Such schemes have been initiated and implemented with varying degrees of success in a number of jurisdictions.

INDIA

Implemented in 2009, India's Aadhaar card is the world's largest national digital ID programme. Created by the Unique Identification Authority of India (UIDAI), financial institutions can verify a customer's identity under the Aadhaar-based eKYC programme using their Aadhaar number and a fingerprint or iris scan[11]. This programme is a pillar of India's financial inclusion initiative[12]. As part of financial inclusion measures, enrollment accounts for flexible identity evidence requirements, with special measures for marginalised individuals such as children, senior citizens, disabled individuals and others[13].

Whilst India has made significant progress toward financial inclusion, enrolling 1.37 billion residents in the programme[14], concerns have emerged over data breaches. One 2018 media report stated that a billion Aadhaar card holders' details were available for 500 rupees (approximately $6) on WhatsApp within 10 minutes[15]. To combat security concerns, the UIDAI introduced the concept of a virtual identity, where Aadhaar-card holders can generate a random 16-digit number online. When combined with biometrics, individuals can use their credentials at various outlets, such as mobile companies, limiting the sensitive data details shared[16]. More recently, there have been reports of cyber scammers using silicon fingerprints and biometric machines with Aadhaar numbers to steal money[17]. In response to these new types of fraud attacks, UIDAI continues to launch new security systems[18].

[10] European Commission
[11] World BankCommission proposes a trusted and secure Digital Identity for all Europeans
[12] Government of India
[13] FATF
[14] UIDAI
[15] The Tribune
[16] Economic Times
[17] DNAIndia
[18] IndiaToday

THE UK

A digital identity scheme is currently underway in the UK as part of the government's strategy to enable innovation, support the digital economy and protect against fraud. A revised Digital Identity and Attributes Trust Framework (DIATF) is in circulation, which outlines robust standards that ensure privacy and security. In March 2023, the Data Protection and Digital Information (No.2) Bill, which underpins the trust framework and its governance and allows identity and eligibility checks to be made against government-held data, had its first reading in Parliament. The government has also released guidance, such as the Good Practice Guide 45 (GPG 45), designed to help companies understand different identity verification methodologies so they can select the most suitable one for their organisation.

Findings generated by the Financial Conduct Authority (FCA) regulatory sandbox[19] support a move to digital identity, identifying benefits for financial institutions such as reducing human error, improving audit trails, lowering costs and reducing friction. However, potential challenges include a lack of interoperable digital identification systems, protocols and processes; and insufficient management buy-in, meaning scarce resources for developers and frontline staff to create the infrastructure needed. One interviewee called out the need to make money laundering regulations clearer and more explicit on the acceptability of digital identities, noting HM Treasury's commitment to doing that as part of its most recent consultation.

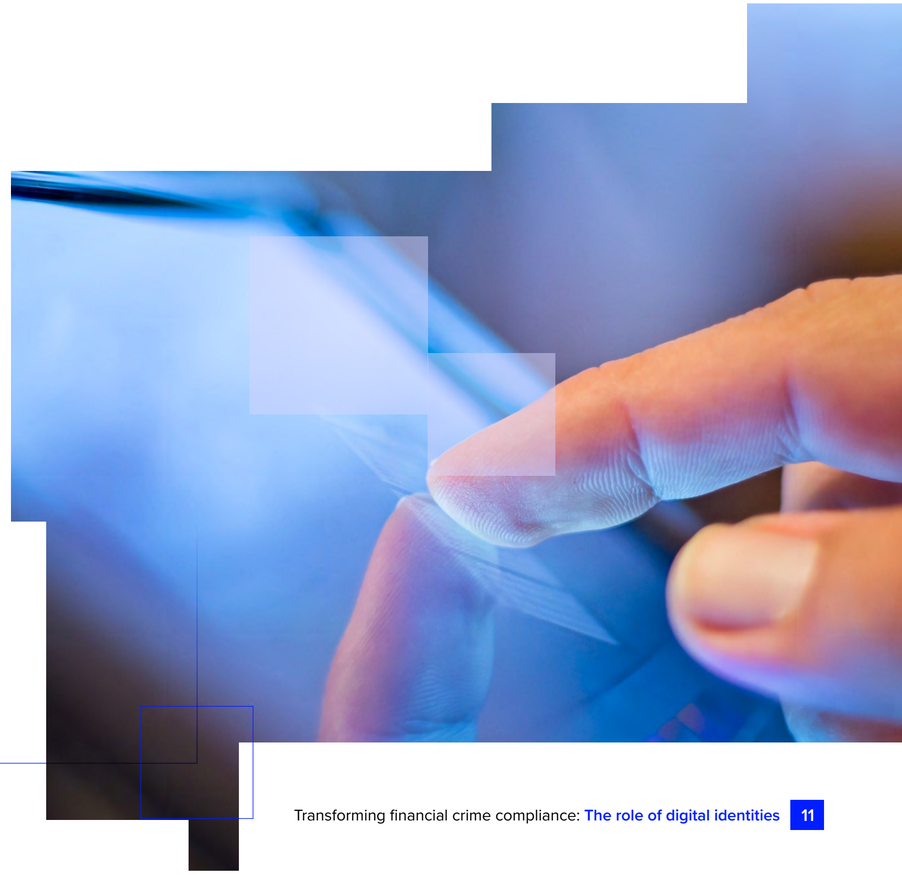
[19] FCA

BAHRAIN

The Central Bank of Bahrain (CBB) has launched an eKYC platform, first announced in 2019[20]. The project is the first of its kind in the region and is part of a broader national strategy of moving towards a digital economy. The eKYC platform supplies a national digital identity database that financial institutions can use to securely verify customers' identities, validate their information and share data digitally. The solution supports sectors including retail and corporate banking, asset management and insurance, with plans to move to telecommunications in the future. The platform verifies customer identity via biometric identity and verification technology, which links to Bahrain national identity card data before instantly connecting to the eKYC platform.

SINGAPORE

Singapore's national digital identity, SingPass, is the product of collaboration between the Monetary Authority of Singapore (MAS), Smart Nation and Digital Government Office, and the Government Technology Agency. As part of SingPass, users can consent to share their information through the MyInfo digital platform, allowing for non-face-to-face customer identification by financial institutions. Firms do not need to obtain physical documents or a photograph of the customer, making KYC a more streamlined process[21]. SingPass serves approximately 97% of citizens and permanent residents older than 15 years of age, making it one of the most widely adopted national digital identity systems globally[22].



[20] Central Bank of Bahrain
[21] MAS
[22] GovTech

MAJOR CHALLENGES

Despite these advancements, challenges surrounding digital identity and digital KYC remain. One prevalent concern is security and privacy. Because digital identity schemes require collecting and storing personal information, including sensitive details, understanding how data is stored and protected and who has access to it is paramount.

These factors can be a significant deterrent,, as seen with the rejection of Switzerland's proposed electronic identity system over data privacy concerns in 2021[23]. In an era of fraud, the infrastructure protecting sensitive details must be robust to guard against cyberattacks. Data breaches may compromise users' information and lead to identity theft, undermining the use of digital identities in the first place and deterring consumer acceptance of them more generally. Building confidence in digital identities application in both the public and private sectors is vital for them to work optimally. Currently, digital identities are most prominently used in the public domain, as seen with new schemes such as Canada's federal digital identity plan that targets government services[24].

Another concern is interoperability. Ideally, digital identities should be seamless and work across different digital identity systems. Fragmented digital identities within one jurisdiction create frustrating user experiences and detract from their key benefit. Jurisdictions must find a framework that allows for the interoperability and universal application of their digital identity schemes, from government services to financial services to business services. On a global level, this poses new challenges as interoperability must be understood between jurisdictions. Since digital identities operate nationally, bilateral frameworks and agreements must eventually be established between countries. This raises questions about defining criteria to determine which jurisdictions have sufficiently robust frameworks.

From an anti-financial crime perspective, the lack of endorsement and certification schemes by regulators is problematic for financial institutions. Without specific guidance or regulatory changes that explicitly address the use of digital identities in KYC, it is unlikely that firms will undergo an overhaul of their onboarding process to include them. Such an undertaking would be massively expensive and lead to regulatory fines amidst the ambiguity of regulatory expectations for digital identities.

[23] SwissInfo
[24] Government of Canada

THE POWER OF DIGITAL TRANSFORMATION IN KYC

Identity triangulation methods help financial institutions gain a fuller picture of their customers and the risks they pose. By looking at different aspects of a customer and cross-verifying across multiple sources, firms can ensure the accuracy of customer data, enhance fraud detection and uphold their anti-financial crime obligations.

The three sides to identity triangulation:

1. **Standard address and identification checks:** authenticating residential addresses and essential identity documents like passports, national ID cards or licences.
2. **Watchlist checks:** cross-checking names against international watchlists, sanctions lists and government or regulator-owned databases.
3. **Bank or finance checks:** corroborating an individual's bank account details, credit history and transactional behaviour to understand financial risk.

> “Verifying an identity is not just verifying that Customer X is a natural person who is opening an account. It is also verifying that Customer X is someone who works in Company Y doing a specific kind of work, because verifying an identity is also about assessing who you are and what you do or have done previously. How a person earns their income can be a big part of their identity and knowing this information helps us understand not just their source of funds but also their transactional profile and behavioural patterns.”

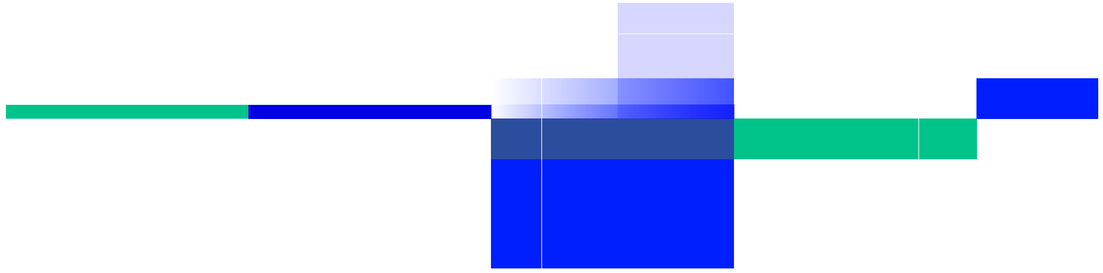
AAMIR HANIF,
Regional Vice President,
AML Compliance, Western Union

A successful and optimal digital KYC process includes triangulating identity without inconveniencing the customer. Checking an individual's or entity's identity will involve validating their supplied personally identifiable details, for example, name, date of birth or address, against a trusted data source. Real-time watchlist checks are also conducted against sanctions and adverse media data sources, connecting to the customer’s bank account through open banking or a database and cross-verifying the retrieved information. All these checks can be completed with zero friction for the customer.

Digital KYC processes benefit the onboarding process by improving the user experience and expediting the customer journey to give firms a competitive advantage. Since using digital identity verification techniques or, even better, using a digital onboarding platform, can reduce human error and increase accuracy, they also improve overall compliance processes. These factors, combined with enhanced capabilities to detect fraud and other illicit activities, more effectively keep bad actors off a firm's platform. The operational efficiencies, reduction of manual burden and increased accuracy mean financial crime risks are more easily identified, minimising overall financial crime risk.

"I absolutely believe that compliance is a competitive advantage. The challenge, though, is that it's a competitive advantage for a problem that is not easily identifiable. It's not understood to be a competitive advantage because the problem isn't accepted until there is adverse media or a fine — and by that time it may be too late."

AAMIR HANIF,
Regional Vice President,
AML Compliance, Western Union



Financial inclusion is one of the most widely understood benefits of digital identity schemes, when globally an estimated 1.4 billion adults are unbanked[25]. One interviewee noted that "the whole package of an effective digital identity ecosystem should improve financial inclusion", extending services to marginalised communities like refugees or immigrants, people experiencing homelessness, older adults or those with disabilities. Referencing HSBC's UK No Fixed Address programme that allows homeless individuals to open a bank account if someone from a participating shelter vouches for them[26], the UK's trust framework also includes provisions on vouching. The Bill and Melinda Gates Foundation has noted that "ID platforms such as the Aadhaar system in India are promising models for providing safe, efficient, and widely beneficial identification services that support financial inclusion across a country."[27]

Benefits are felt beyond marginalised individuals and could include those who have undergone a name change. One interviewee cited the example of a divorcee who might incur difficulty proving their identity with a maiden name, despite building credit under their spouse's last name and being perfectly solvent.

[25] World Bank
[26] HSBC
[27] Bill and Melinda Gates Foundation

HORIZON SCANNING

As part of adapting to a digital economy, it seems clear digital identities are set to eventually be widely adopted. This is demonstrated by progressive government policies and pilots with varying degrees of maturity that look to implement related schemes. The European Commission has stated its aim to have 80% of people using digital identities to access key public services across EU borders by 2030, effectively mandating the availability of digital identity for member states under eIDAS 2.0[28]. Creating a single European digital identity in the form of a digital wallet will allow EU citizens to identify themselves via eIDs, but also store and make available identity data, credentials and other personal attributes, most likely through a smartphone or computer. The proposal aims to make it mandatory for each EU member state to provide EU digital identity wallets to all citizens free of charge, as opposed to the voluntary eID schemes that operate today.

[28] European Parliament

By establishing common standards and requirements, the regulation makes it easier for businesses and individuals to use electronic identification and trust services across the EU, with some positive use cases for consumers and financial services. This framework will allow users to open a bank account in another country with their eID, creating an easier and safer way for consumers to access cross-border services and streamline the onboarding checks needed for financial institutions. Increased security through proposed secure authentication and certification systems could help reduce the risk of fraud and identity theft and make it easier for individuals and businesses to access online services and conduct transactions securely. Another use case being explored is for payments – currently, two consortia have engaged in large-scale pilots to explore the payment use case[29].

In the Philippines, the Bangko Sentral ng Pilipinas (BSP) published a circular stipulating rules on electronic KYC and using digital IDs during customer onboarding[30]. Looking ahead, South Korea plans to launch a blockchain-backed digital identity by 2024 that users can operate with a smartphone[31].

As different countries adopt digital identity schemes, financial institutions must create a framework for determining which programmes have a higher degree of confidence. Countries with a robust digital identity framework may be weighed differently than those with less robust ones. Firms will need to decide which digital identity frameworks they trust and which will require further scrutiny, outlining and defining the criteria. As Kathryn Westmore of RUSI stated, assessing and making risk-based decisions on different digital identity schemes is extremely difficult: “How do you really know which programme is robust or not to begin with? You also risk bias creeping into your decision-making and excluding people because they come from a certain country.” This assessment framework will require adequate resources and careful consideration for proper implementation.

[29] Nobid Consortium, EWC
[30] BSP
[31] Bloomberg

> “ Passports took four hundred years to develop and, as identities are determined at a state level, this isn’t going to be instant. Each country has their own way of doing things, so interoperability will need to be established on a bilateral basis. There are parallels with passports. If governments trust the way passports were issued in one jurisdiction, there is easier access. If not, then individuals have to get a visa.”

ALISON MCDOWELL,
Co-founder and Director,
Beruku Identity

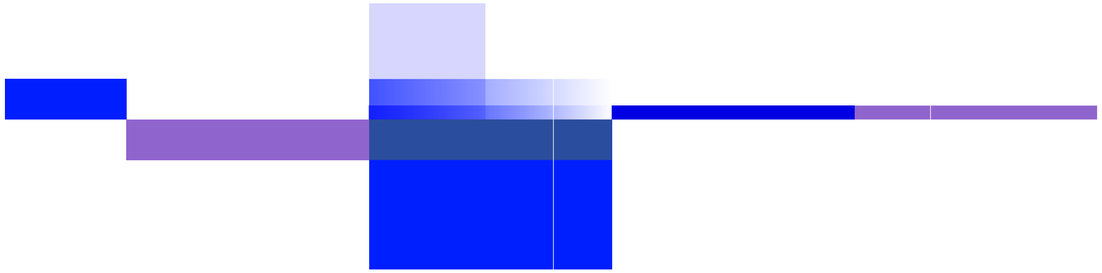
Despite a global move towards digital transformation and aligning with the digital economy, adopting digital identities has been slow-moving in many jurisdictions. In the United States, where individual state governments have their own identity infrastructure, digital identities are still in their infancy. This is likely to advance as the Improving Digital Identity Act of 2021, which aims to create a task force to coordinate efforts for interoperable digital identity, passes through to the Senate[32] In the context of high fraud levels and scams facilitated by tools like ChatGPT[33], there is an urgency to create systems that defend against identity theft and impersonation. These developments will likely encourage the adoption of digital identities as they become increasingly necessary.

[32] US Congress
[33] Europol

For financial institutions specifically, there are challenges around implementation, including operational concerns. One interviewee commented on the low likelihood of onboarding for financial services being the first use case for reusable digital identity, pointing out potential difficulties in sourcing technology resources given the highly costly task of rewriting and transforming a bank's onboarding process. Additionally, regulators will need to be more clear on how digital identity fits into anti-money laundering regulations. Another interviewee commented that as regulators aspire to be more data-driven, it is hoped that the expectations of the firms they supervise will also be data-driven. In effect, this means that digital KYC and digital identities will be embraced and explicitly advocated for, particularly with their potential to curtail fraud and other financial crimes.

" Digital identity will almost certainly reduce the kinds of fraud we face today. What will future fraud look like and how well can digital identity solutions continue to outsmart criminal solutions? I think that's yet to be seen as with all kinds of evolving fraud."

ALISON MCDOWELL,
Co-founder and Director,
Beruku Identity



A final challenge is customer acceptance. Depending on cultural nuances, some countries will be more willing to use digital identities than others. Reluctance based on security and privacy concerns will be weighed against consumer demand for faster and safe processes. One interviewee cited countries in Europe like the Netherlands and Estonia, which have implemented effective digital identity programmes, "Those aren't comparable to what is happening in the Commonwealth countries, for example. Identities aren't necessarily based on a state-issued ID and people aren't as comfortable with the concept of carrying their papers. So, there are some markets that are doing really well, but it's like comparing apples and pears." Ultimately, different jurisdictions will experience different concerns and levels of scepticism, requiring education on using digital identities, to build trust, transparency and awareness.

Financial institutions must pay attention to these emerging trends even when the implementation of digital identities seems far away in their jurisdiction. By some estimates, the global market for reusable digital identities is poised to grow to $266.5 billion by 2027[34] — highlighting it as an increasingly important trend. Customers from countries that do have digital ID schemes have higher expectations, as they are accustomed to more seamless, frictionless processes. Because these expectations translate to higher drop-off rates, firms must embrace technology and plan ahead to adapt and adjust, to realise their business interests.

[34] Liminal

CONCLUSION

Digital transformation continues to shape financial services and anti-financial crime operations. In the context of high global fraud rates, remote processes and growing customer expectations, firms will continue to need to adapt and modernise their compliance procedures. While digital identities already exist in many jurisdictions with different degrees of maturity, they will become increasingly important worldwide as governments progressively adjust to the digital economy.

Digital identity verification boasts many benefits for financial institutions in cross-selling, reducing manual processes, and improving accuracy and efficiency. Identity triangulation using digital identity verification has the power to create a frictionless experience for the customer whilst increasing accuracy and reducing operational costs. As consumers expect instant and frictionless services, leveraging digital KYC processes will become a key factor for survival. The anti-financial crime space must maximise the benefit of digitisation and avoid creating onboarding processes in isolation from other customer journey phases. Digital identities and digital KYC can aid the onboarding process, but also assist with ongoing monitoring and screening.

As the technology revolution continues, there are high hopes for those organisations that have already helped shape digital identity with e-signatures, identity verification and KYC schemes. With growing demands for innovation and smooth user experiences, the future of digital identity calls for portability and reusability.

With the promise of greater financial inclusion, better fraud detection, and a faster and more efficient customer experience, financial institutions must prepare for digital KYC and digital identity technologies now, in order to gain a competitive edge and enhance their anti-financial crime efforts.

About **REFINITIV**

Refinitiv offers organizations a competitive advantage by helping them effectively and efficiently manage risks associated with their customers and third parties. Our solutions include risk screening services through World-Check, detailed integrity and advanced background checks on any entity or individual through due diligence reports, identity verification, account verification and customer onboarding services. Find out more about our solutions **here**.

About **FINTRAIL**

FINTRAIL is a global consultancy passionate about combating financial crime. We've worked with over 100 global leading banks, fintechs, other financial institutions, regtechs, startups, venture capital firms and governments to implement industry-leading approaches to combatting money laundering and other financial crimes.

With significant hands-on experience, we can help you prepare, assure and fortify your onboarding and ongoing customer journeys to meet evolving regulatory requirements, use technology effectively, and stay competitive. Get in touch **here**.

Visit **refinitiv.com** | @Refinitiv Refinitiv

FINTRAIL

REFINITIV®

An LSEG Business

RE2861800/7-23