DIGITAL IDENTITY VERIFICATION SECTOR SPOTLIGHT- BANKING

Whitepaper

IDOLOGY a GBG company

1.1 Banking

It is well understood that the banking industry has a complicated set of regulatory requirements when it comes to verifying their customers' identities, in terms of KYC (Know Your Customer), KYB (Know Your Business) and AML (Anti Money Laundering), which have significant fines for non-compliances, as well as reputational risks. The other major pressure on banks is competition from other financial institutions and emerging fintechs, whose new approaches are leading to rapidly evolving user expectations around streamlining the onboarding process. Users also want to trust their banks, need to feel a genuine sense of security, and need to be regularly engaged within their customer journey.

Outside of this, the ever-present threat is fraud, with new account fraud being a major driver of fraud, which can cause massive financial losses, needs high levels of resourcing to manage and can cause a large risk to the brand. These intertwined pressures mean that digital identity verification is highly important in this sector, and must be considered a priority.

This spotlight will examine the banking industry's individual challenges around digital identity verification and outline our anticipated future outlook.

1.1.1 Industry Identity Verification Situation

The banking industry faces the most difficult identity verification situation of any industry, given the important role that identity verification plays within the area. Banks and financial institutions are bound by KYC regulations, which means that they have to verify their customers' identity or they will not be meeting their regulatory requirements.

Traditionally, banking was in a simple situation with identity verification. Identity documents were presented in branch when opening an account, and when making certain transactions, then being verified by the teller. However, the rise of digital banking has transformed this simple model into one that is highly complex.

Digital operations mean that identity also needs to be verified digitally. If a user loses their mobile device, for example, banks need to be able to ensure that the device cannot be used to immediately authorize transactions without additional checks.

Digital-only banking has changed the equation in the banking area in a number of ways. By their very definition, digital-only banks do not have an in-branch element, meaning that they require a purely digital onboarding process. This has generally involved the concept of 'selfie' onboarding as a customer-facing method, where a user takes an image of themselves, and this is compared to a scan of an identity document. However, this is by no means the only verification type available.

At this point, banking is at the stage where traditional banks and other financial institutions are introducing digital onboarding capabilities to compete with digital-only banks and to operate remotely during the COVID-19 pandemic. This has brought the market to a point where digital identity verification needs to be well integrated, robust and effective.

In the context of needing to provide a robust and secure experience, this represents a balancing act versus friction. Getting this balance right is difficult and requires leveraging the correct verification tools and strategies. By creating an onboarding process that is robust yet user friendly, banks can create a competitive differentiator. However, there is risk in not doing this correctly. Ineffective identity verification processes can lead to losses in terms of new customer acquisition and friction during the onboarding experience. This is critical, as this does not create a good first impression for the potential user relative to engagement and trust, which is highly important in this new digital world.

1.1.2 Industry Use Cases and Considerations

There are several different use cases and considerations for banking in digital identity verification. These are explored below.

i. Fully Remote Onboarding for Digital-only Banks

For digital-only banks, they need to have a completely standalone digital onboarding process, where identity can be verified remotely in a way that minimizes fraud and friction (since these "challenger" banks appeal to younger, more tech-savvy

consumers, they need to have an enhanced, superior, smooth identity verification and onboarding experience, it is a competitive differentiator. This means doing all the elements that are required normally, such as KYC, AML, checking against sanctions lists etc., in a digital-only environment.

For digital-only banks, this is fairly straightforward, as they tend to be built on robust technical infrastructures based on APIs, which enable them to operate in a technologically agile way. The difficulty is ensuring that the measures that these banks put into place are robust enough to secure banking, as banking is a high-risk target for attacks such as account takeover fraud.

ii. Remote Onboarding for Traditional Banks

Banks and financial institutions need to develop digital onboarding as an ongoing capability, as more of their business moves to the digital channel. The pandemic has accelerated this transition, but ultimately, banks have been closing branches for some time, meaning digital onboarding is a very important capability to support this wider transition.

The difficulty for traditional banks is in ensuring that solutions are compatible with their wider technical infrastructures, which can be complex and difficult to update.

For smaller regional banks, community banks and credit unions need to achieve the same goals to be competitive, but on smaller IT budgets, so ease of integration is critical in ensuring effective roll-outs.

iii. Data Diversity & Consortium Networks

Central to the requirement for effective digital identity verification is data diversity – banks and financial institutions must be able to access enough data to know that user onboarding information and their behavior is unusual. Incorporating other identity verification data sources is important, as the more indicators are used, the more robust the system is compared to a traditional system reliant on credit checks, which can be breached.

The other consideration is data transparency – data must be able to be sourced and explained, as a key requirement for ongoing regulatory compliance and fundamentally being able to explain decisioning to customers.

This is where the idea of consortium networks of data sources becomes highly important, as this enables new account openings at different institutions to benefit from fraud data and learnings elsewhere in the ecosystem, securing the whole market in a more effective way.

iv. Ongoing Verification

Onboarding is an important element, but just as important is ongoing verification – that is, authentication. Opening a fraudulent account is a risk, but account takeover of an existing account is also a significant risk. As such, the requirement is for banks to design strategies that ensure that verification is carried out on a continuous basis. This could be when an unusual transaction is made, or when a new payee is set up, or in any number of given scenarios.

v. Open Banking & Embedded Finance

As banking becomes increasingly open through the proliferation of APIs, the bank account is shifting from a single, transactional account to a gateway to access any number of services. Open Banking, for example, is a new threat vector that will require identity verification steps around permissions to ensure that account data sharing and payment initiation is authorized by the correct party. As embedded finance grows, where payments and banking are increasingly embedded in other activities outside of core banking experiences, this identity verification importance will only grow.

1.1.3 Pain Points for Identity Verification

As with any industry, there are specific pain points in banking around digital identity verification. These will be outlined below.

i. Integrating with Existing Infrastructure

To date, much of banking's technical infrastructure is highly complex and, in some cases, outdated. Many banks, particularly in Asia, are still running older core banking software systems that can be extremely complex and costly to maintain and integrate new software with. This means that if this outdated software is in place, implementation can be a serious challenge.

Even with an updated cloud-based technological infrastructure, integrating with existing systems can still be a pain point. Banks are complicated, and systems need to be integrated quickly, with the minimum of coding required by IT teams.

Due to these challenges, models which focus on easy to integrate APIs and dashboards that can make changes, rather than relying on code changes, will reap the biggest rewards in the banking vertical.

ii. Using ML in the Right Way

The use of ML, as opposed to the general term of AI, is highly important within banking, and automation has been a pain point for the banking industry. As one of the most heavily regulated industries today, banking has a firm requirement to be explainable and transparent to regulators.

This is a problem, when many ML models in use today are difficult to understand when it comes to reasons for making decisions. Therefore, the inability to explain decision-making has been a limiting factor for the use of automation within banking.

This means that using ML within the banking sector requires a careful approach, which balances these needs and still leverages rules-based systems, combined with human intelligence. Aside from ML bias which is both a regulatory and brand risk, there are dangers in using vendors who utilise "ML Only" technology, specifically as it relates to governance of changes to the ML decision engine. When the model changes, these changes are applied to the engine itself, impacting multiple customers across multiple industries, which can result in false positives and more fraud.

iii. Faster Payments Driving Up Fraud

The rise of faster payments, such as RTP in the US or SEPA Instant Credit in the EU, is leading to major fraud risk, given the limited time to intervene in the transaction process due to their inherent speed. As such, banks need to implement better identity verification during onboarding, as well as better ongoing verification to offset this risk.

iv. The Rise of Synthetic Identity Fraud

Of all of the fraud types currently prominent, synthetic identity is one that is a major concern for banks and other institutions. Synthetic identity, fuelled by a very high level of data breaches, can bombard verification systems with plausible-looking identities, meaning that verification strategies need to advance in order to secure against this risk.

Over time, the use of ML will be increasingly critical in combatting synthetic identity fraud and will attract more attention from regulators as an area where fraud is booming. Combining identification methods with powerful ML-based analytics is the best way to offset this risk.

v. Growing Regulatory Needs & Compliance

FIs are both experiencing and expecting further tougher compliance requirements and oversight from the likes of the CFPB (Consumer Financial Protection Bureau). This is being particularly felt by credit bureaus, which FIs depend on. The high levels of fraud that have been experienced around the PPP (Paycheck Protection Program) are likely to be a catalyst for state and federal regulators to seek more accountability on the part of FIs and lenders. Decisioning bias around machine learning is another area that will see increased scrutiny. As such, strong identity verification programs that feature multiple layers, strong data diversity and above all transparency can mitigate rising compliance costs and inefficient processes, without worsening customer friction.

1.1.4 Industry-specific Needs and Settings

Banking has highly specific requirements based on its complexity and the trends that are influencing it. These will be examined here.

i. Need to Support Digital Transformation

The greatest need within banking is to digitally transform operations. Digital transformation is important in banking and has been strategized by banks for many years to support wider goals. Digital transformation in banking is critical to ensure

profitability and lowering operating costs whilst maintaining service levels, as branches close in unprofitable locations.

As digital identity verification is a major change, its introduction and evolution needs to be at the center of digital transformation goals. Its capabilities, in terms of enabling a greater range of onboarding and continuous verification activities to be carried out, are critical to successful digital transformation.

ii. Need to Prevent Account Takeover Fraud

As the bank account is central to a user's financial life and is increasingly a gateway to other services with the rise of Open Banking, preventing account takeover fraud is absolutely critical.

In practice, this means having a combination of verification methods and a wide-ranging level of data diversity. If this is lacking, then banks can miss the fraud signals they need to prevent fraud techniques, such as account takeover fraud. It also highlights how important behavioral checks and ongoing verification are in the banking space.

iii. Need to Use Multiple Layers of Verification Together

To ensure effective verification, the best way to operate is to utilise multiple layers of identity verification together, in an effectively orchestrated platform. This will enable an improved anti-fraud performance, whilst enabling transparency around which layer of fraud verification has been triggered, which is important for transparency.

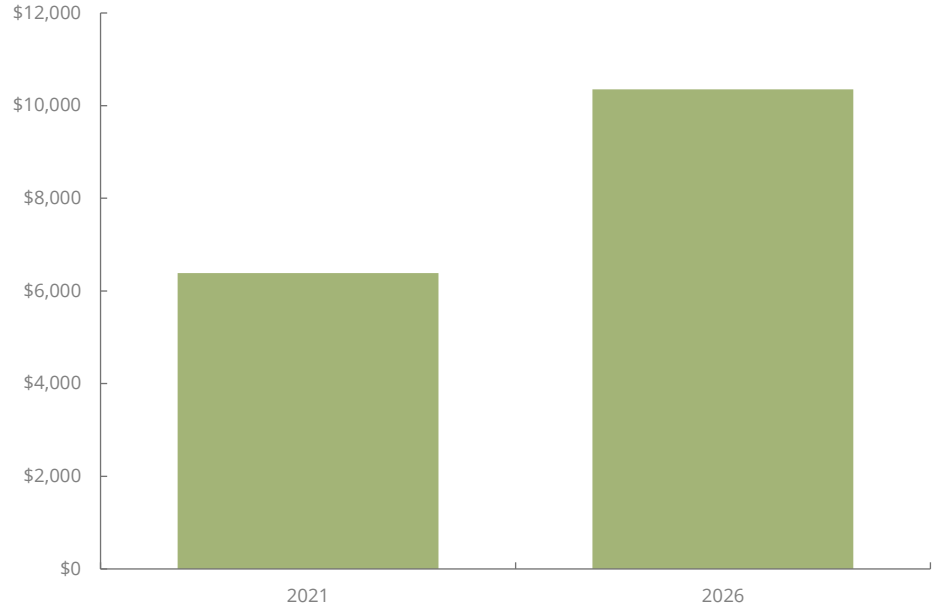
Of critical importance here is customisability – by being able to tune the different verification layers and how they interact, banks can gradually improve fraud detection whilst allowing more good business in by reducing fraud.

1.1.5 Future Outlook and Requirements

We predict that banking will be the leading industry for digital identity verification introduction and innovation over the next 12-24 months. Simply put, banking has the highest priority for deployments, as its efforts for digital transformation mean it needs verification urgently.

As banking is such a high-profile target for the use of synthetic identities and account takeover fraud, banks must use broad platforms with wide-ranging capabilities, in order to best mitigate fraud risk. If they fail to build a robust system, based on more than just point solutions for ID document scanning, then they will struggle to deal with evolving fraudster tactics. It is for this reason that we will see the continued fusing together of both physical and digital attributes for verification, such as taking name, address, date of birth, etc., and with IP detection, email & mobile analytics, enabling better decisions to be made. Only by taking a multi-layered, customizable approach will banks achieve the best anti-fraud and customer experience outcomes.

Figure.1: Global Spend on Digital Banking Identity Verification Checks per annum ($m), 2021 vs 2026



Source: Juniper Research