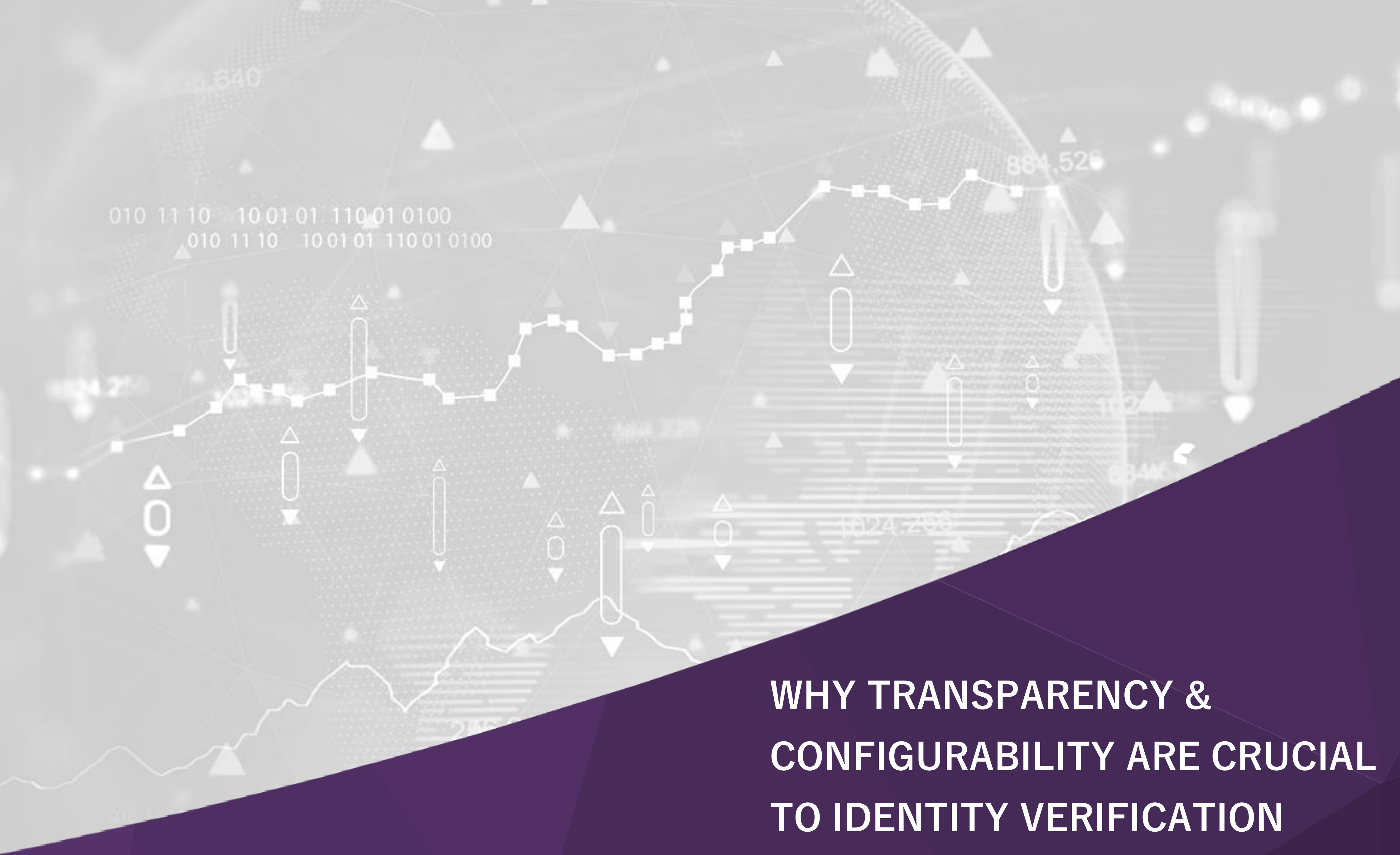


WHY TRANSPARENCY & CONFIGURABILITY ARE CRUCIAL TO IDENTITY VERIFICATION

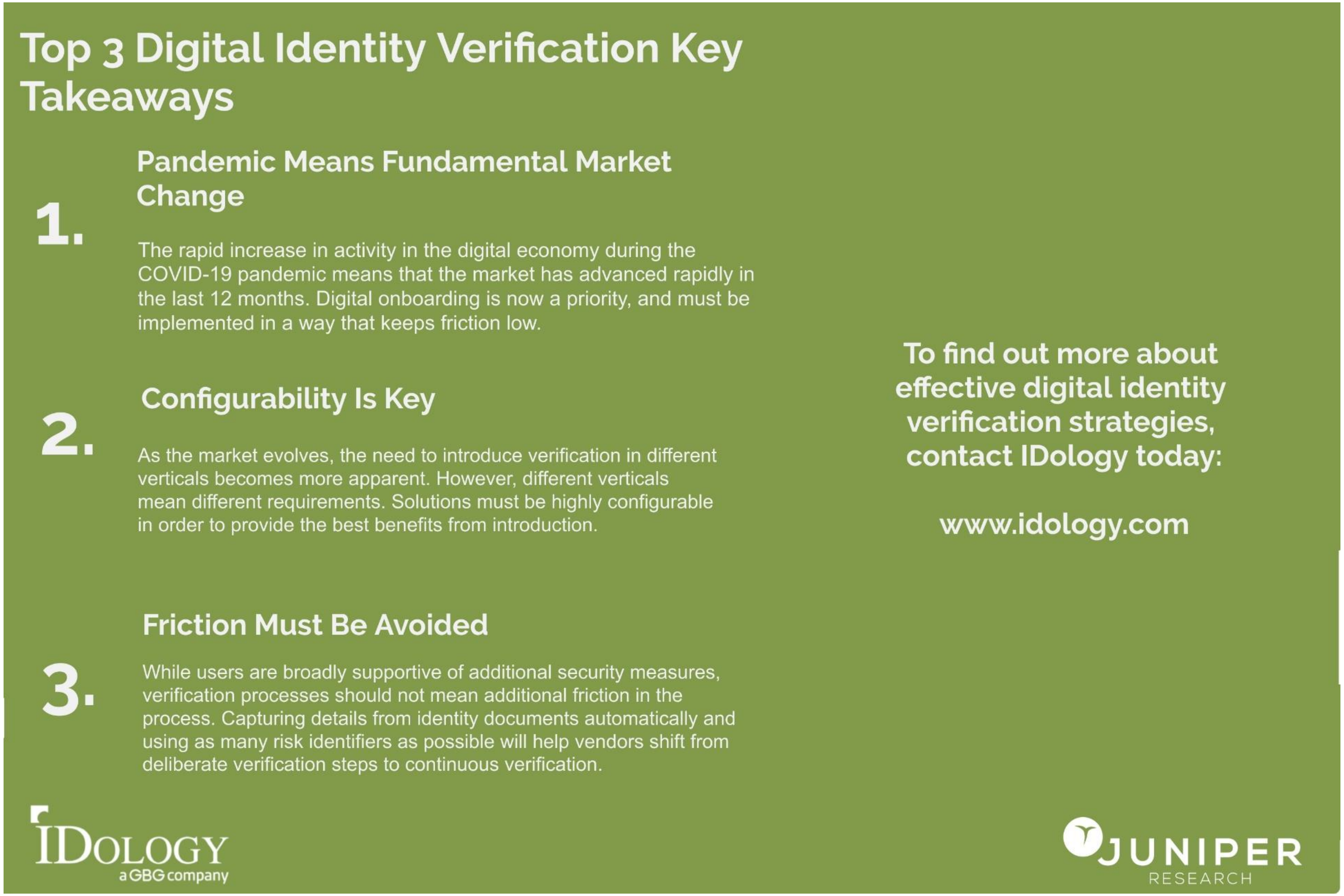
Whitepaper

Contents

1. Key Trends in Digital Identity Verification

2. Key Considerations for Digital Identity Verification Success

3. Digital Identity Verification – Vendor Comparison



Top 3 Digital Identity Verification Key Takeaways

1. **Pandemic Means Fundamental Market Change**

   The rapid increase in activity in the digital economy during the COVID-19 pandemic means that the market has advanced rapidly in the last 12 months. Digital onboarding is now a priority, and must be implemented in a way that keeps friction low.

2. **Configurability Is Key**

   As the market evolves, the need to introduce verification in different verticals becomes more apparent. However, different verticals mean different requirements. Solutions must be highly configurable in order to provide the best benefits from introduction.

3. **Friction Must Be Avoided**

   While users are broadly supportive of additional security measures, verification processes should not mean additional friction in the process. Capturing details from identity documents automatically and using as many risk identifiers as possible will help vendors shift from deliberate verification steps to continuous verification.

To find out more about effective digital identity verification strategies, contact IDology today:

www.idology.com

1. Key Trends in Digital Identity Verification

1.1 Introduction to Digital Identity Verification

In the past few years, the digital identity has gone from a concept, to a technological disruption that is having a significant impact across a number of markets. Knowing who the customer is at all times has emerged as critical to creating data-driven business models that can reduce fraud and improve customer experiences. However, the rise of digital identity has led to a number of other developments. Given the increasingly critical nature of digital identity, an important area is digital identity verification. Digital identity verification is where a person's identity attributes can be validated and used to access services. These attributes can be physical, in terms of identity documents, or digital. Digital identity only works, and achieves its full potential, when these digital and physical identity attributes are analysed and verified effectively. Securing digital identity with verification techniques is the best way to resolve increased fraud in the online area, without compromising the user experience. In order to best realise this, it is vital to fuse together both digital and physical identity attributes, to ensure the best user outcome.

This whitepaper will examine how the digital identity verification market is evolving, and how verification has emerged as a critical requirement for stakeholders throughout the value chain, as well as key considerations for identity verification service adoption.

1.1.1 The Growth of Digital Identity & Verification

The digital identity market has experienced rapid growth, with the pandemic being a major contributing factor over the last 12 months. However, what the pandemic has done is accelerate the already existing transition towards the digital use of, and access to, systems. With this growth comes numerous considerations, which are intrinsically linked. Firstly, how to ensure that all these digital identity apps are part of a secure environment, and that digital identity use can be trusted. Secondly, how best to leverage increases in digital identity use to provide a better user experience.

Ultimately, the rise of digital identity apps, being driven by use of government-issued identities, is a way in which digital activity can be verified. The use of identity in the digital sphere is a potential way to improve security, but must be accompanied by robust verification strategies to extract the maximum potential from the digital identity ecosystem.

1.2 Key Digital Identity Verification Trends

This section will examine the key trends that are prominent within the digital identity verification space, and how these trends are shifting the landscape.

1.2.1 The Digital Shift & Digital Identity Verification

At this stage, it is difficult to underestimate the impact that the COVID-19 pandemic has had on society. The digital economy has seen a once-in-a-lifetime growth surge, with increases in usage of digital onboarding and enrolment in banking and eCommerce, being very noticeable. However, this has not been a process without its challenges, meaning that there are opportunities for further innovation to be made. The pandemic saw an unprecedented shift to remote access of services, with consumers in many places unable to make payments in person in store. In the US, there have been a number of stay-at-home orders in states such as California, although these have varied to a large degree on a state-by-state basis. Despite the differences, there has been an overall shift towards access to digital services.

In order to meet the requirements for greater digital access, customer-facing stakeholders of all sorts had to introduce stopgap measures to facilitate completely digital onboarding processes. This has not only impacted banks, but also many other businesses in different verticals, including insurance companies, lenders, fintechs, sports betting companies, retailers, eCommerce providers and others. In many cases, this has seen the deployment of authentication of personal details versus digital databases, as well the deployment in some cases of 'selfie onboarding,' where users take a picture or video with their government issued ID, which is then validated manually by a staff member, as an escalation method.

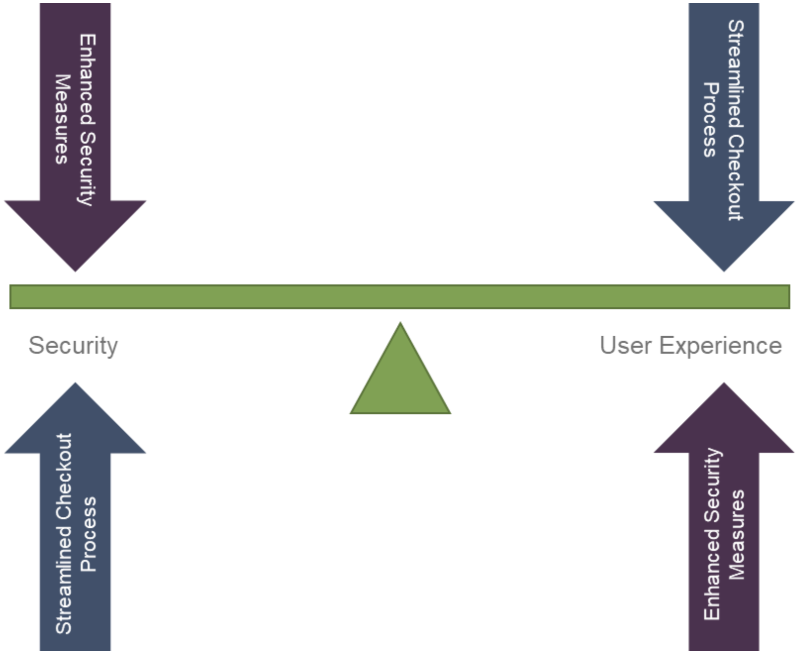
While this has enabled processes to carry on in the short term, it is not suitable for long-term use. Indeed, as these processes are still manual, they do not benefit from the automation that is possible as part of digital identity. As such, we anticipate that key stakeholders will shift to longer-term strategies in 2021 and 2022, that will better allow them to embrace the full potential of digital identity. These strategies will revolve around the concept of automated onboarding, where identity systems can automatically utilise the correct assessment for each scenario, including dynamic KBA, address verification, mobile attributes, email and others, as well as checking for fraudulent documents by using analytics.

Essentially then, the pandemic has proven to be an accelerator for digital change, and in identity has been a digital identity change event and accelerator. In this period, the rapidly changing landscape has proven the worth of digital identity in terms of what it can deliver. The next 12-24 months will see stakeholders deploying, upgrading and adding more capabilities to systems to unlock its true potential.

1.2.2 Verification vs User Experience

In online fraud, there is a fundamental challenge that has been difficult to resolve for many years, the conflict between security and user experience. Traditionally, the interaction between the two is a trade-off. If security is increased in the account application and onboarding and this causes undue friction, this can cause higher account opening abandonment rates and lost revenue for the business. However, streamlined account opening processes typically mean reduced security checks, which can result in more revenue lost to fraud. As can be seen in Figure 1.1, the checkout or onboarding processes are a fine balancing act, that can be tricky to get right.

Figure 1.1: Security vs User Experience Trade-off


Enhanced Security Measures
Streamlined Checkout Process
Security
User Experience
Streamlined Checkout Process
Enhanced Security Measures

Source: Juniper Research

However, digital identity verification can be a significant step away from this traditional challenge. Digital identity verification encompasses a wide range of technologies and approaches that can be used to break this traditional impasse. By using orchestrated smart multi layered verification techniques which are dynamic and feature integrated escalation processes, stakeholders can improve security credentials, while also providing a more compelling user experience.

In order to achieve this goal, stakeholders need to shift to models centred around the use of digital identity verification tools, enabled by the wide availability of solutions on a SaaS basis.

1.2.3 The Role of AI in Verification

Of all the technological innovations that have taken place in recent years, AI's emergence and evolution is one of the developments with the highest potential, but also one of the most challenging, seen to date.

AI works by applying analytics at scale – AI models ingest curated datasets to 'train' their systems, then they are applied to unsorted data to make decisions. AI has become popular in several areas, including fraud detection and prevention.

AI is highly valuable in digital identity verification because it can handle the enormous scale of data analysis required. In the wake of the pandemic, the global digital economy is larger than ever before. This, combined with the wealth of indicators available on user behaviour, such as emails, geolocation and mobile identifiers, mean that the task of analysing this data and generating operational insight is daunting. As such, AI has an important role in processing this data, alongside rules engines and human intelligence.

However, these capabilities come with limitations. AI is designed to emulate the human mind in the way it analyses data. This delivers very good performance, but also risks a lack of transparency. AI is often described as a 'black box'. This description refers to the difficulty AI can have in explainability. As AI models are so complex, they generally cannot produce a list of the factors that influenced a decision. This is theoretically similar to the human mind – this too is a 'black box'. The difference is that the human mind can communicate reasons, whereas AI has struggled to do this.

This limitation is a significant challenge in digital identity verification. Verification during digital processes is critical and can be the difference between users being able to transact or not. This means that verification processes such as KYC (Know Your Customer) are highly regulated in certain sectors, such as by the PATRIOT Act in the US. Verifying bodies need to be able to justify to regulators why certain decisions are made, which becomes complicated to achieve under an AI model. AI can also struggle when presented with unusual patterns or swings in data, which the pandemic will have exposed.

While many vendors have set about the task of bringing explainability to AI processes, this is yet to coalesce in one successful approach. As such, AI, plus the transparency of a rules engine, provides the optimal combination for identity verification processes.

1.3 Digital Identity Verification – Future Outlook

Ultimately, the digital identity verification market is presently focused on the accelerating effect that the pandemic has had and how to bring in more robust procedures. However, it is important to examine the outlook beyond this short-term timeframe.

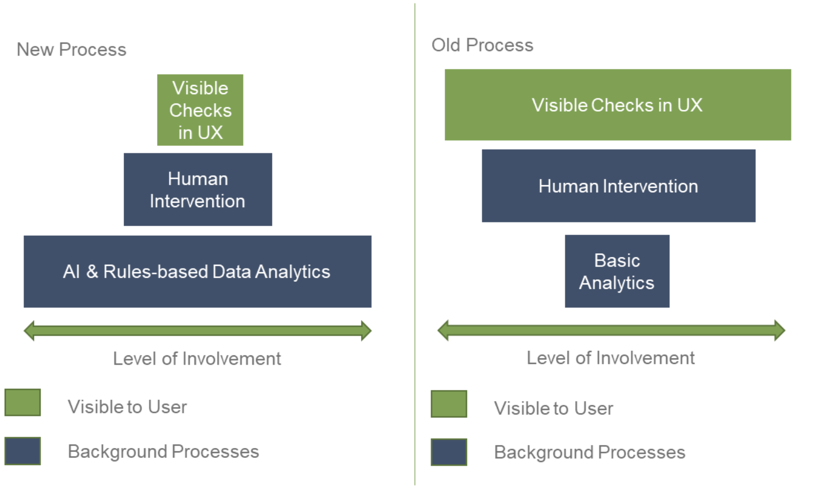
We anticipate that by 2022, digital identity verification will have focused on the concept of AI-assisted verification, in order to provide the most seamless verification processes possible. This will include both AI applied at the time of transaction, as well as AI being used post transaction to identify wider trends.

Ultimately, the upsurge in digital usage will not diminish over time; digital is here to stay, following the pandemic. This is because the pandemic accelerated existing trends towards digitisation, rather than completely changing the landscape.

This permanent shift means that by 2022, stakeholders throughout the ecosystem will be looking to design the most robust, low friction verification processes possible. Choosing the right digital identity verification partner here is critical to unlocking the potential, which will bring a better user experience. This in turn will bring increased revenue with higher approval rates, less expenses and fraud and decreased manual reviews.

This means that verification will increasingly become automatic and seamless, rather than requiring interruptions to the user journey, such as identity document scans or other additional checks.

Figure 1.2: New vs Old Digital Identity Verification Process



Source: Juniper Research

As can be seen in Figure 1.2, we anticipate that the process will require much less user intervention in processes, and will increasingly rely on multi-layered orchestrated metrics such as device verification, IP and geo location, email as well as phyiscal attributes such as address deliverability verification Vendors that offer these capabilities as part of their platforms now will benefit as this transition occurs.

< >

2. Key Considerations for Digital Identity Verification Success

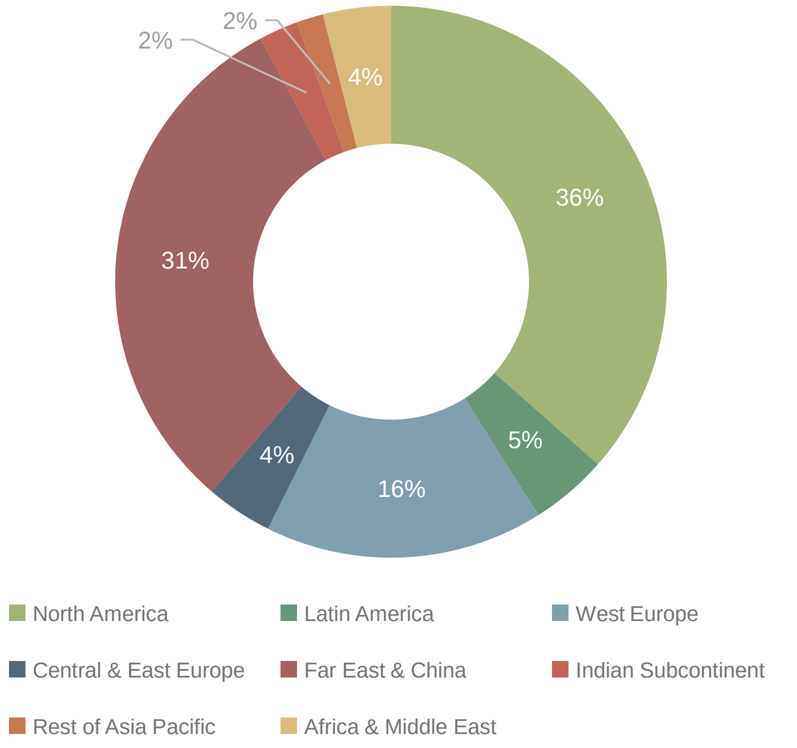
2.1 Key Considerations for Digital Identity Verification Success

The first section outlined how the digital identity verification market is evolving and changing, given the impact of the pandemic, how verification is balancing friction versus security, and the increasing role of AI. This section will highlight key considerations for how stakeholders should approach their digital identity verification processes to achieve the best outcomes for them and their users.

Digital identity verification touches every aspect of how businesses operate, meaning careful consideration must be given to the right approach.

The concept of digital identity verification is particularly complicated in the financial services ecosystem. With the vast amount of regulation in place, including the BSA (Banking Secrecy Act) and the PATRIOT Act, security is a very important requirement. This is intensified by the current scale of the online payment fraud challenge globally. Juniper Research forecasts that in 2024, there will be an excess of $44 billion lost to fraudulent digital commerce transactions, including fraudulent online purchases and bank transfers, rising from $27 billion in 2020. A breakdown of this is in Figure 2.1, which shows that North America accounts for 36% of total anticipated fraud values.

Figure 2.1: Total Transaction Value of eCommerce Fraud (% of Global), Split by 8 Key Regions, 2024



This means that the stakes are higher than ever – vendors must get their strategies right, or they will face significant damage to their operations. This can take two main forms: direct losses from fraud and reputational/brand damage. The second of these is the biggest threat, as customers who experience fraud will associate that with a brand, causing loss of revenue and a significant risk of further word-of-mouth damage.

We believe that there are seven main considerations to achieve digital identity verification success:

- Frictionless onboarding – ensuring that enhanced security measures do not increase friction in the new account sign up/application and checkout processes.
- Customisability – choosing a system that can be heavily customised and configured for industry, business model and individual fraud trends and requirements.
- Transparency – enabling all systems used to seamlessly provide explanations to regulators and end users. This is also important in terms of getting the greatest value from data by understanding why decisions are reached, which can be fed into further analytics.
- Using AI in the right role – identifying the correct use of AI, which leverages its advanced analytics capabilities without leading to damaging 'black box' issues.
- Ability to boost growth – ensuring that the system can not only make the environment secure, but can also foster growth by increasing approval rates.
- Ease of management and implementation – point, click change-ability of settings so IT resources do not need to get involved, also enables real-time response to change events (fraud techniques) and it offers a high level of governance – black box models can change without notice.
- Consortium networks – These allow data diversity and fraud experiences from other businesses to benefit all users in a network.

Only when all seven of these considerations are taken together can stakeholders create an effective digital identity verification strategy that protects their clients and business, while allowing them to grow at the fastest rate possible.

2.1.1 Frictionless Onboarding

A massive requirement in the digital sector is the requirement to onboard customers in a frictionless way. The transition to digital services requires vendors to think about digital onboarding in a way that they have not had to before. The pandemic forced purely remote onboarding in some cases, which required an extension of existing digital onboarding processes to account for 100% of the onboarding journey. In particular, banks and other financial services players have had to adapt rapidly. As such, there are many key requirements for creating a frictionless onboarding process:

- Flexibility & Risk Management: Flexibility and the intelligent use of risk management are key to reducing friction. The best solutions are those that start with a simple level of validation during an onboarding process, then can dynamically escalate depending on use cases and other factors escalating to further onboarding steps, such as dynamic knowledge-based authentication or a photo ID scan. This risk-based approach ensures a very simple, frictionless process for the majority of users, with only small elements of friction introduced for more high-risk processes. Flexibility also in settings customisation in real time point click also means that systems can be reconfigured quickly as circumstances change.
- Seamless Integration: The best solutions for digital onboarding are seamlessly integrated into the overall customer journey. By this, we mean that processes should be invisible to customers wherever

possible. If simple onboarding parameters are used, then this information can be pulled from general data, rather than a specific process. If further details or validation are required, this should be white labelled to minimise the disruption to the user journey. If third parties are given prominence, this can lead to customer confusion.

- Clear & Transparent Messaging: In the onboarding process, it is important to be very clear in the messaging around what the process is and what the data is being used for. In a recent Juniper Research survey on payments, respondents were broadly supportive of security measures, so identifying measures as such is important. Users are more likely to trust a brand which is conspicuous in its emphasis on security, and while completely frictionless is the goal, users will accept some friction as an indication that the process is secure.

- Embracing Data Diversity: The transition to digital services means that there is more data than ever being generated by users. In order to design the most frictionless process possible, vendors should harness as wide variety of data sources to create behavioural checks, which will add security and reduce the need to carry out overtly security-based interruptions to the customer journey.

By considering these requirements carefully, vendors can create an onboarding process that requires little interruption to the overall user journey. This efficiency will be critical to ensuring that customers' opinions of onboarding processes remain positive.

2.1.2 Customisability

One key requirement in the digital identity verification area is the ability to customise how systems work. This is particularly important as not all businesses and requirements are the same. This is true in several ways:

- Different Verticals: Businesses need identity verification tools in numerous verticals, with identity playing an important role in financial services and eCommerce, as well as eGovernment and other areas. As such, tools need to be adjusted to each vertical; a one-size-fits-all approach is not appropriate, given the different regulations, business models and verification requirements involved. For example, a gambling company will see account takeover attacks used to take control of account credit, whereas in lending and finance this could be used to fraudulently apply for credit, so in each case users will want to customise their escalation steps and criteria to ensure that they provide an effective barrier to fraud.

- Different Regulations: These tools need to work for a number of verticals and critically, these verticals are governed by different regulators with different rulebooks. As such, the reporting requirements and the different checks required create an environment where customisability is massively important, in order to deliver the necessary functionalities. For example, banks will need to meet strict criteria around correctly carrying out KYC processes, whereas in eCommerce, address verification is an important part of preventing fraud.

- Different Countries: In the modern financial services and banking landscapes, large players tend to operate in many different countries. For example, JP Morgan operates in over 60 countries. While those different countries will have some similarities in regulatory terms, with rules being based on similar frameworks such as Basel III or FATF (Financial Action Task Force) guidelines, there will be differences. This means that in each country, the solutions used by the vendor for digital identity verification will need to be customised. It is also not just about regulation – in certain markets some indicators will be less reliable than others, with some countries less likely to use email, or more likely to have government-issued digital identities. As such, the ability to customise solutions to match the market conditions is highly important to multinational operations. In the eCommerce area, the rise of cross-border eCommerce means that these considerations are more important than ever.

- Different Objectives: Even if the regulations are the same, not all businesses will have the same objectives for their verification processes. Ultimately, the onboarding process is critically important to how the customer perceives a brand, as the friction or lack thereof can be a big factor in customer satisfaction. Therefore, the onboarding process is an aspect of the customer journey that businesses must have control over and be able to customise. If they lack control, then it will be difficult for them to create a seamless customer journey, which can result in users not signing up to financial services and a loss of revenue.

Ultimately, in terms of verification, while security is always necessary, there is a risk management balance to be had. Customisation means that vendors can set the correct level of risk for them, rather than turning away potentially important customers. Giving the vendor control over their own onboarding processes is necessary in the current environment, where the transition to digital services means that competition is more intense than ever. Without this control and customisability, vendors will lack the agility to deal with the complexity of the digital economy.

2.1.3 Transparency & Explainability

Banking, lending & finance, healthcare, insurance, sports betting, gambling and tobacco, among many other industries already operate in heavily regulated environments, for good reasons, given the implications of fraud and identity theft, as well as the need for processes to be fair and reasonable. Regulations on the banking sector relating to KYC alone include The Banking Secrecy Act, the PATRIOT Act (both in the US), the Canadian PCMLTFA (Proceeds of Crime [Money Laundering] and Terrorist Financing Act), The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (UK) and the 5th Anti Money Laundering Directive (EU).

This wealth of regulation means that dealing with and staying compliant with these regulations in all the different areas that vendors operate in is the number one priority for all digital identity verification services. Even for eCommerce, there are still regulatory requirements around identity protection in many areas, meaning that this is still the main priority.

Accordingly, digital identity verification systems need to ensure regulatory compliance as the core of what they offer. This leads to two key requirements:

- Transparency: All systems in use must be fully transparent, in that the stages of the process and the user journey must be able to be identified and shared with regulators. This could be important in investigations, and the inability to produce details would be a serious regulatory breach. Transparency ultimately builds user trust, which is highly important.

- Explainability: Being transparent around events is not quite enough – vendors need to be able to explain why decisions were taken at each stage. This entails being able to explain why an onboarding request was declined, or why a fraudulent transaction was authorised erroneously. This is crucially important, given the requirement of many regulations that demand that consumers be treated fairly by businesses. This causes a problem for many AI systems, which rely on 'black box' algorithms that are not easily explicable to regulators.

The two requirements are basics needed in a digital identity verification system. Not only do systems need these basic capabilities, but they also need to be easy to use and produce at a moment's notice for regulators. This could include a risk of accidentally allowing a sanctioned individual to access banking services, which would be a serious regulatory breach. For many eCommerce merchants, not correctly blocking access to accounts for fraudsters could result in significant loss of funds for individuals, which could then become viral on social media or reported on, leading to a severe reputational risk. These risks drive the need for overall management tools and dashboards for systems that can provide insight from a global customer view level, right down to the individual transaction level. This is particularly important in the light of AI bias, which has been a problematic area where decisions made by AI are translating unconscious bias in training data sets into real world operations, which again is accompanied by a severe reputational & regulatory risk.

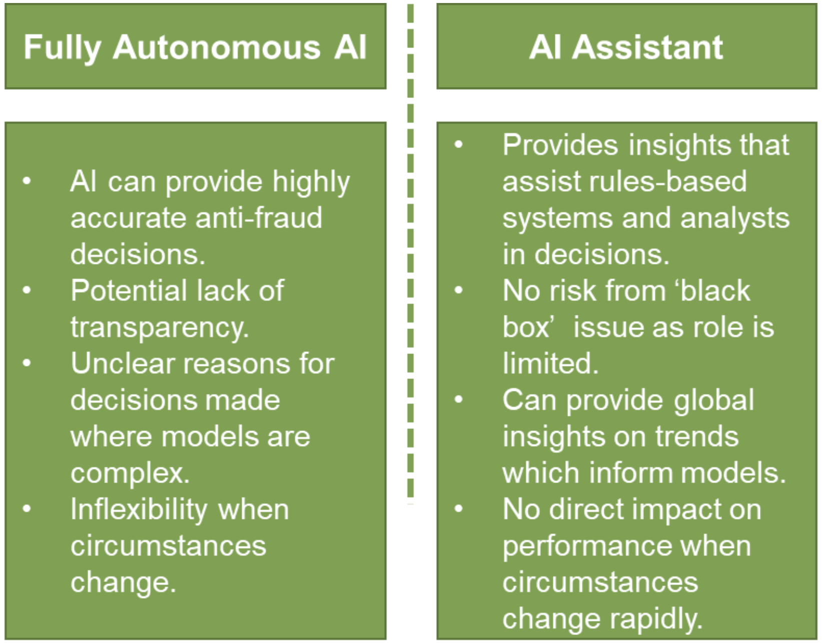
However, transparency and explainability are about more than regulation. Transparency in operations enable data visibility to the vendor. They can use this data visibility to assess trending and further risk analysis – essentially understand why did a customer fail? Vendors using the tools can then use this data to further customise decisioning models and for providing business insights.

2.1.4 Using AI in the Right Role

As mentioned earlier in this whitepaper, AI has a problem with the 'black box' issue. This is where AI systems are unable to explain why they made a decision, meaning that AI models can lack transparency, failing one of the basic considerations for digital identity verification implementation. However, AI can play a very important role in the digital identity verification market. Therefore, ensuring that AI is in the appropriate role in the chosen solution is an important requirement for system adoption.

Figure 2.2 shows the different models AI is taking in the digital identity verification market.

Figure 2.2: AI Models in Digital Identify Verification



Fully Autonomous AI

- AI can provide highly accurate anti-fraud decisions.
- Potential lack of transparency.
- Unclear reasons for decisions made where models are complex.
- Inflexibility when circumstances change.

AI Assistant

- Provides insights that assist rules-based systems and analysts in decisions.
- No risk from 'black box' issue as role is limited.
- Can provide global insights on trends which inform models.
- No direct impact on performance when circumstances change rapidly.

Source: Juniper Research

Both models in use have their advantages and disadvantages, meaning that solutions need to be considered carefully:

- Fully Autonomous AI: This model has proven its ability to reduce false positives by analysing data, comparing favourably to older systems in many cases. However, it comes with the potential challenge around a lack of explainability, which can be hazardous when dealing with regulators. It is also quite inflexible. Training AI using historical data will translate the biases of the data into the model, which can be a major risk. If the training data is biased against a certain ethnicity for example, then the AI model could discriminate against certain sections of society, which would be both devastating in reputation terms and likely to lead to strong fines from regulators. This use of AI also assumes that future activity will follow the same patterns, or at least that the pace of change will be consistent. This will have been a specific weakness with COVID-19, where a sudden change will have required significant adjustment to analytics models, as transaction behaviours fundamentally alter.
- AI Assistant: This model is where the AI tools are used to provide input and insight into other processes, rather than carrying out fully autonomous decisioning. AI can be used to flag inconsistencies with requests to review certain applications, or to provide a global view of trends, without needing to carry out the whole process in an opaque way.

We recommend that at present, AI is best utilised in an assistive role, enhancing human expertise and existing systems, rather than fully displacing them. However, we also believe that as AI advances, this will be less of an issue as explainability is built into systems at the design stage and AI will be able to take a more proactive role. As such, verification vendors should be following AI developments closely.

2.1.5 Ability to Boost Growth

The final consideration for choosing a digital identity verification system is the ability to boost digital sales growth. While identity verification is important for security reasons, this goes beyond merely ensuring a secure environment. When vendors use the correct solution that is customised to their needs and market conditions, they can increase their approval rates, accepting valid business at a higher rate whilst continuing to reject fraud. The challenge with verification systems is always accuracy and the degree to which false positives/negatives are generated. If a system is highly customised and judging potential customers on valid criteria, then this will be a fair platform to operate from. However, if the system is not customised enough, the rules are not complex enough and the validation criteria are poorly judged, then a high number of manual reviews will be required. This is a problem for two main reasons:

- Resources Consumed: When a high number of cases need manual review, this is an onerous requirement on antifraud teams at financial institutions and eCommerce merchants. This takes up a significant amount of resources that could be better spent on more accurately assessing the fraud cases that are in play.
- Interruption to Customer Journeys: By triggering a high number of cases for manual review, systems would interrupt customer onboarding journeys much more regularly than is necessary, leading to high levels of abandonment. This would also increase costs, as lower initial locate rates means that more requests will need to be escalated to more complex verification methods, such as an identity document scan. The higher the approval rate from initial checks, the lower the costs will be and the higher customer satisfaction will be, making the efficiency of the decision making process critical to success.

Ensuring access to appropriate escalation methods will be vital in securing revenue that may otherwise be lost at the first hurdle. Two methods that can be useful are KBA and identity document scans. Dynamic KBA can be used as a verification method when a check is escalated, using transaction history or other details the user would know to verify their identity. An identity document scan is another step up method that can be critical in securing this potential lost revenue.

Therefore, it is important that digital identity verification solutions must be designed from the ground up to have the ability to improve approval rates and boost growth accordingly by having broad features, inclusive of a broad range of escalation methods, or their introduction will be counterproductive to overall business goals.

2.1.6 Conclusion

To conclude, we believe there are broadly four characteristics that verification systems must satisfy, summed up by the acronym FAIT

- Frictionless – systems should be as frictionless as possible to end users.
- Adaptable – systems can be configured to reflect different verticals, businesses, end consumer variations, disruptive change events (e.g. covid) regulations and scenarios.
- Intelligent – systems feature built-in analytics based on both artificial and human intelligence that can offer insights on trends.
- Transparent – systems offer transparent reporting and regulatory compliance.

Vendors should consider these elements when deciding on a system, or they will risk taking the wrong approach and failing to reap the benefits of digital identity verification implementation. Adaptability is particularly important – not all verticals are the same, and not all businesses are the same. By choosing a vendor with a broad set of capabilities that offers different verification methods in different scenarios, businesses can access the highest possible levels of approval rates.

< >

3. Digital Identity Verification – Vendor Comparison

3.1 Vendor Comparison

This section contains an assessment of multiple vendors by how they fulfil key digital identity verification capabilities, followed by analysis of each vendor.

Figure 3.1: Juniper Research Digital Identity Verification Vendor Comparison

	experian	IDOLOGY a GBG company	jumio	LexisNexis RISK SOLUTIONS	onfido	Socure	Trulioo
Configurability	✗	✓	✓*	✗	✗	✗	✓*
Ongoing Fraud Team Monitoring	✓	✓	✗	✓	✓	✓	✗
Consortium Approach	✓	✓	✗	✗	✗	✗	✗
Rules Engine Capabilities	✓	✓	✗	✓	✗	✗	✓
Multi-layered Nature	✓	✓	✗	✓	✗	✗	✗
Comprehensive All in One Solution	✗	✓	✗	✓	✗	✗	✗
Mobile Capabilities	✓	✓	✓	✓	✓	✓	✓
Machine Learning Capabilities	✓	✓	✓	✓	✓	✓	✗

*Source: Juniper Research. * Please note Jumio and Trulioo were found to be configurable in their specific areas, not in a wider context.*

3.1.1 Vendor Commentary

i. Experian

Experian is a well-known provider of credit scoring, anti-fraud and identity services. In the digital identity area, it offers identity verification services, fraud prevention and age verification services, as well as other solutions.

These solutions are integrated with CrossCore, which provides a hub for fraud and identity capabilities, powered by machine learning. CrossCore orchestrates different fraud and identity tasks using a series of APIs, and has a great deal of flexibility in terms of implementation.

ii. IDology

IDology provides an extensive set of digital identity verification solutions, built around its core ExpectID platform. This platform offers and orchestrates a range of integrated capabilities, including age verification, document ID mobile scanning and mobile attribute verification and out of wallet authentication. IDology's solutions are designed to be highly configurable, meaning that they can be customised for each client's requirements and changed in real-time with point and click. Transparency is at the core of IDology's solutions, meaning that each system is designed to be fully explainable, while being supported by a post transaction dedicated fraud team and assistive AI analytics system.

The system is supported by IDology's Consortium Fraud Network, which allows customers to benefit from fraud learnings across its broad network of customers, meaning that the system is continuously improving. The system includes access to fully integrated fraud layers such as email analysis, IP and geo-location indicators, address deliverability verification, which is not always available in the space, and, uniquely, with its GBG parent company has integrated cross-border identity verification into one plug and play system.

iii. Jumio

Jumio provides an end-to-end identity verification platform, which is called KYX. The system uses AI at its core and includes features such as liveness detection for selfie onboarding.

Jumio has a focus on the eCommerce checkout process, with solutions such as BAM Checkout offering an integrated eCommerce checkout and fraud check solution, supported by Jumio's PCI DSS certification.

iv. LexisNexis Risk Solutions

LexisNexis Risk Solutions offers analytics and risk intelligence in the identity space, with LexID, its analytics for identity management solution, providing the backbone for its onboarding systems. Its identity systems are deeply integrated with its fraud network.

Its main identity verification tool is LexisNexis IDU, which is designed to provide verification at every point in the customer journey, supported by its large databases. LexisNexis Risk Solutions are responsible for configuration of rules and AI models, meaning that it can lack configurability compared to some other solutions.

v. Onfido

onfido

Onfido is an AI-driven identity verification vendor, which offers document authentication, biometric verification and ongoing authentication through processes.

Onfido has concentrated on facial recognition and analysis versus official government identities as its key capabilities. It offers a robust onboarding process based on these capabilities, with the ability to trigger rechecks at high-risk points in the customer journey, such as authorising high-value or unusual transactions. However, it is very focused on the document onboarding stage, and it lacks the other solutions, such as KBA, that are important in verifying users when they fail initial checks.

vi. Socure

Socure

Socure provides a range of verification services, including Sigma Identity Fraud, Sigma Synthetic Fraud, KYC, DOCV, Global Watchlist and Socure ID+. These solutions are available using a single API connection and they leverage analytics to improve approval rates.

Socure's focus is on its analytics capabilities, which are extensive. Its Socure ID+ solution includes predictive analytics, powered by machine learning.

vii. Trulioo

Trulioo

Trulioo offers GlobalGateway, an identity verification marketplace. This system supports AML & KYC tasks across numerous countries, supporting mobile-based verification during onboarding.

Trulioo's services are designed to provide a fully transparent list of data matches and reasoning behind every decision made. Trulioo's solution is designed to be highly configurable for different scenarios, combining different verification methods as required. Trulioo also offers business verification tools, which are not widely available from competitors in the space. However, they lack escalation options when a customer fails initial checks, and their solution is not as configurable as others in the space.

3.2 IDology Profile

IDOLOGY
a GBG company

i. Corporate

Founded in 2003, IDology is a key provider of digital identity verification and authentication. IDology focuses on providing innovative identity solutions combined with fraud prevention tools for organisations operating in a digital environment. The IDology platform's real-time consortium network monitors and stops fraudulent activity, while also driving revenue, decreasing costs, and meeting compliance regulations for companies across multiple industries.

IDology is built from the ground up to be fully transparent, which is reflected in its products, which prioritise configurability, ease of reporting and simple regulatory compliance.

In February 2019, IDology announced that it was being acquired by GBG, the UK-based global identity data intelligence specialist. The total consideration for the transaction was £233 million ($300 million), and followed a partnership between GBG & IDology. In October 2020, Christina Luttrell was announced as IDology's new CEO, replacing previous CEO John Dancu. Other key executives include Dennis Maicon (Vice President of Sales, Business Development, Partner Programs), Eva Turner (Vice President of Finance, Administration) and Eric Leiserson (Vice President of Research & Marketing).

GBG announced that in the half year up to 30th September 2020, it had revenue of £103.5 million ($141.3 million), of which the identity segment accounted for £64.5 million ($88 million), representing 62% of GBG's total revenue in the period. GBG's platforms in the identity space include ID3global, KYP, IDology and GreenID.

ii. Geographic Spread

IDology is based in Atlanta, Georgia, with customers and operations around the world.

iii. Key Clients & Strategic Partnerships

- In February 2019, NextGate, a leader in healthcare enterprise identification, announced a strategic partnership with IDology to leverage its capabilities within the Enterprise Master Patient Index.
- In December 2019, WireWheel, a data privacy management provider partnered with IDology to offer a solution for verifying and authenticating the identities of customers who submit SRRs (Subject Rights Requests) under the CCPA (California Consumer Privacy Act) and other privacy laws.
- IDology has a number of international and leading US clients in areas including social media, ridesharing, retail & eCommerce, financial services, alternative finance and tax.

iv. High-level View of Offerings

IDology offers 4 key areas of products, each with individual product lines. These are:

- Onboarding: Removing friction from account creation.

- Verification & Setup: Quickly locating and confirming identities.
- Authentication: Ensuring identities and protecting account access.
- Fraud Detection: Detecting and preventing fraud at every step of the customer journey.

The ExpectID platform is at the heart of all the solutions, providing a highly configurable system that can offer different capabilities as required by clients.

a) Onboarding

- ExpectID Scan Onboard: This is where an ID document is scanned, information is extracted and used to pre-populate enrolment details.
- ExpectID Barcode Scan: This is where data is extracted and populated by scanning the barcode on the back of an ID card.

b) Verification & Setup

- ExpectID: This is the main identity verification product, which comprises an engine which analyses details submitted, risk assessing to identify discrepancies. This includes fraud detection layers, and the transaction can be approved, failed or escalated for additional checks through IDology's other solutions.
- ExpectID Age: This is a version of ExpectID specifically designed for age-restricted industries, such as lotteries, online gaming, social media etc, which confirms potential users are of the correct age and have a valid identity.
- ExpectID IQ: This is a dynamic knowledge-based authentication solution that asks consumers a series of relevant, multiple choice questions based on transaction and other data.
- ExpectID Scan Verify: This solution offers facial comparison using identity documents, which is analysed using advanced forensics to detect fraudster activity or tampering.
- ExpectID CBA: This solution allows for knowledge-based authentication, based on data such as purchase history.
- ExpectID PA: This is IDology's solution for PATRIOT Act compliance, allowing verification of a user's identity versus government watch lists. Watch lists include OFAC (Office of Foreign Assets Control), PEP (Politically Exposed Persons), FBI 10 Most Wanted Lists and many others.

c) Authentication

- ExpectID Secure OTV: This allows for one-time verification of users.

d) Fraud Detection

- IDology Consortium Fraud Network: This solution shares real-time fraud intelligence between companies and across industries, giving vendors the power to leverage the fraud mitigation efforts of every IDology customer. A combination of machine learning and human intelligence work together to detect repeat transaction attempts across the network, or flag specific attributes associated with known fraud.

- Smart Layers: This is where numerous layers beyond basic identity matching, including location, activity, device and email, are used together to identify and verify customers.

All of these solutions together provide a comprehensive set of features to clients, who can ensure a secure operating environment in a low-friction way. AI is utilised in the ExpectID platform, providing insights that fraud analysts can action, rather than in a fully autonomous role. Different verification options are called upon as needed, creating a solution which can ensure that the maximum number of genuine customers are accepted.