THE PAYPERS

Insights into Payments and Beyond

Digital Onboarding and KYC Report 2020

Balancing Convenience and Compliance

Endorsement partners:

ONE WORLD IDENTITY

consult hyperion
securing tomorrow's transactions

Key media partners:

IDENTITY WEEK
GLOBAL • TRUSTED • VISIONARY
SDW2020 PLANET BIOMETRICS DIGITALID

ONE WORLD IDENTITY

Digital Onboarding and KYC Report 2020

Balancing Convenience and Compliance

Contact us

For inquiries on editorial opportunities please contact:
Email: **editor@thepaypers.com**

To subscribe to our newsletters, click **here**

For general advertising information, contact:
Mihaela Mihaila
Email: **mihaela@thepaypers.com**

RELEASE VERSION 1.0
FEBRUARY 2020

TEL: +31 20 893 4315
FAX: +31 20 658 0671
MAIL: EDITOR@THEPAYPERS.COM

Editor’s letter

‘Bank confidence is a fragile reed, and a troubled bank is damaged by any rumours, true or not,’ **Irvine Sprague, former chairman of the Federal Deposit Insurance Corporation**

First impressions can make or break a business, and a positive experience can create long-lasting business relationships. But what happens when you missed your chance to rise above your customer expectations or damaged your brand reputation by being involved in large (money laundering) scandals?

For the last decade, **The Paypers** has been closely watching the payments and banking space, and has been reporting about the innovation taking place within the financial services, large mergers and acquisitions in payments (**Santander and FirstBank**, **Worldline and Ingenico**), delving into money laundering scandals (e.g **Panama Papers**, **Danske Bank**, and others), presenting **law enforcement taking action to fight crime in financial services**, and many more. As a result, we have been witnessing both the welcoming initiatives that the financial industry has been (and is) developing, plus the challenges it is facing and the negative media around them.

And what struck us was the urgency for the whole industry to cooperate to serve the customer well and to fight crime. Overall, banks and other financial institutions are viewed as the gatekeepers of the financial system and hold a high level of responsibility to prevent financial crime. As such, modern identification methods have been applied (video streaming, facial recognition, document scans), know-your-customer (KYC) and anti-money-laundering (AML) policies have been established, and ongoing technological developments have opened new opportunities for fintech and regtech providers.

However, for these tools to be efficient, they need to be presented, shared, and acknowledged. Therefore, the **Digital Onboarding and KYC Report 2020** was born. With this report, we want to help leaders navigate even better the digital onboarding process and decipher what takes banks and financial institutions to fight financial crime. Thus, our main three objectives are:

Increase awareness – on two levels:

B2C – retail banks are losing their customers due to outdated onboarding practices. In the UK, for instance, consumers are not happy when applying for financial products, and similar unpleasant experiences can be found throughout the whole banking sector in Europe. **Signicat found** that 40% of consumers had abandoned bank applications before they were complete. More than 1 in 3 of these abandonments occurred due to the time it took to fill in the required details. Their conclusion? FIs have two options: either onboard new customers in less than 14 minutes and 20 seconds, or risk losing money.

Don’t forget: every interaction that your customer has with you is an opportunity for you to make an impression.

B2B – money laundering is a big problem. **According to Europol**, despite comprehensive money laundering legislation in EU Member States, the results of asset tracing in terms of confiscations remain at an extremely low level. Of the billions of euros generated by the illicit drug trade in Europe, around only 1% is confiscated and more needs to be done to address this situation. The result is an increasing number of criminal groups with significantly higher profits, which can be used to fund other illicit operations and to infiltrate legitimate business structures.

If left unchecked, money laundering can erode a nation’s economy by changing the demand for cash, making interest and exchange rates more volatile, and by causing high inflation in countries where criminal elements are doing business, according to Manfred Wandelt, Senior Manage at **Deloitte RegTech Lab**. The draining of huge amounts of money a year from normal economic growth poses a real danger for the financial health of every country involved, which in turn adversely affects the global market.

Editor's letter

Share knowledge

Most often, companies and service providers focus on only one aspect of a customer's digital lifecycle, whether that is onboarding, validation, or identification, and fail to capitalise on a customer's full digital engagement potential.

Moreover, extracting relevant information from paper-based or incompletely digitised sources can be inaccurate and time consuming. In such an environment, compliance leaders increasingly focus on the use of Artificial Intelligence (AI) and advanced analytic techniques to aggregate enterprise-wide data to fight financial crime.

Additionally, hiring and retaining top talent with the skillsets required to thrive in the new market environment has also become an imperative for the financial compliance sector.

In a bid to help financial institutions understand these topics, The Paypers has invited top consultants, lawyers, and banks to share their knowledge, insights, and hands-on expertise. Furthermore, skilful technology providers present best practices and practical solutions to enable businesses to improve the customer onboarding experience and find the right balance between the user-friendliness and the compliance measures needed.

Provide direction

By tapping into technology such as artificial intelligence, machine learning, and lately also blockchain, businesses can solve money laundering issues, while improving the security of the onboarding process and reducing compliance costs (as people checking documents and re-entering data can be both expensive as well as error prone). However, sometimes it is hard to find the right solution provider or solutions that really work.

The Paypers wants to actively guide you in order to find some solutions to your challenges, and why not the right business partner who can provide sustainable compliance programs in banking and financial services, to help you stay 'regulator ready'.

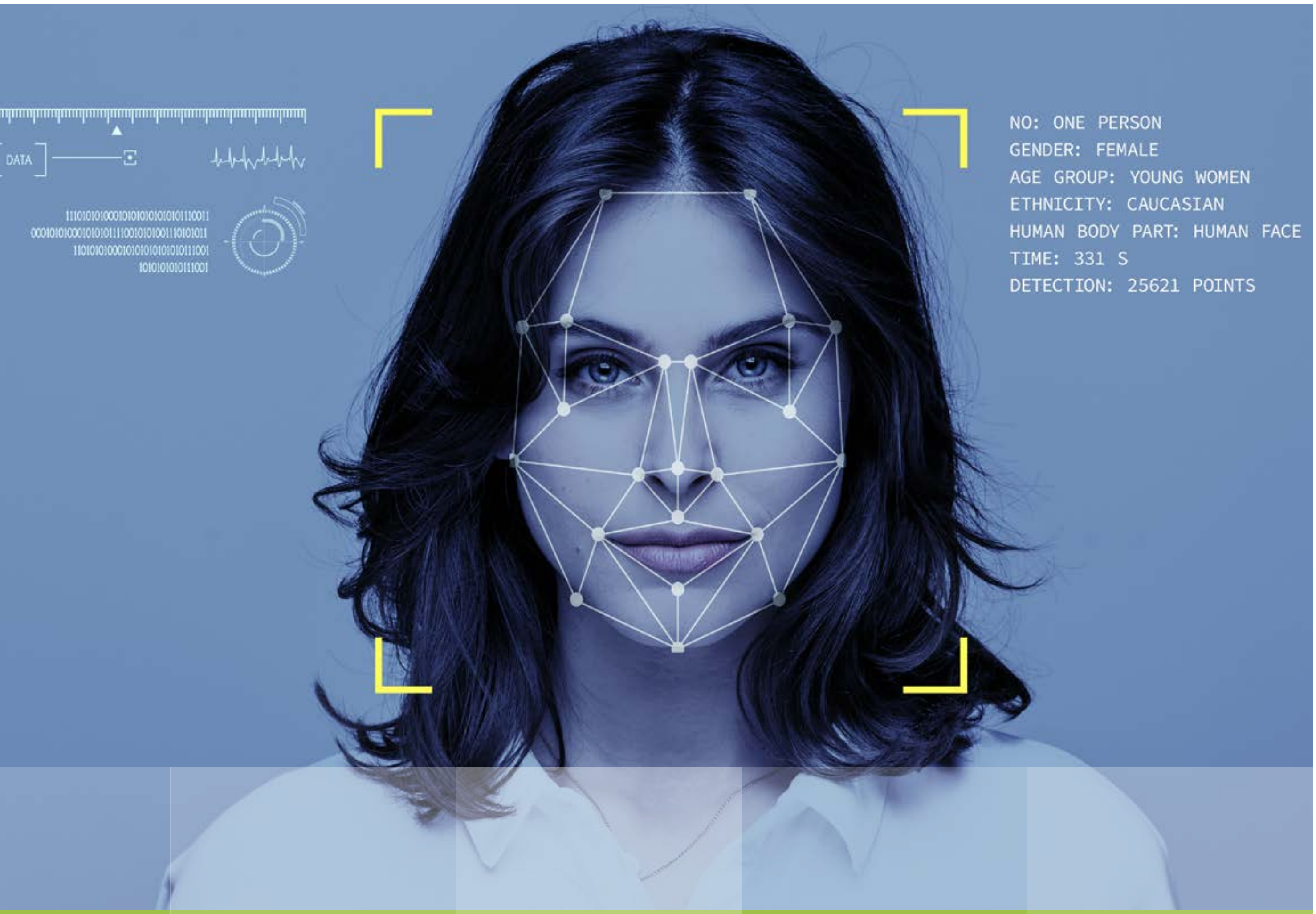
With these objectives in mind, we invite you, the reader, to also share your opinion, to help us spread the message and make the first edition of the **Digital Onboarding and KYC Report 2020** a virtual space that encourages dialogue and healthy cooperation among all stakeholders.

We would like to express our appreciation to **One World Identity** and **Consult Hyperion** – our endorsement partners who have constantly supported us – and also to our thought leaders, participating organisations, and top industry players that contributed to this edition, enriching it with valuable insights and, thus, joining us in our constant endeavour to depict an insightful picture of the industry.

Enjoy your reading!

Mirela Ciobanu | *Senior Editor* | The Paypers

Table of Contents



Best Practices in Digital Onboarding, Identity Verification, and e-KYC

Your First Impression Counts, So Get It Right

'Onboarding means creating a digital identity for a new customer and charging it with all things required to deliver the requested service', **INNOPAY**

Customers have decided: user experience is the most important thing when choosing your bank

In the financial services sector, the level of service offered to customers coupled with the drive to innovate new products, based on the latest technology, plus strong branding, are crucial to attract and retain customers. New players on the financial market like neo-banks and fintechs have influenced this business reorganisation, by reshaping the landscape and accelerating digitalisation of many services and processes.

Customer experience (CX) has emerged as a major differentiator for large financial services providers. Plus, it pays off to treat your customers excellently, as for every 10th percentage-point uptick in customer satisfaction, a company can increase revenues from 2% to 3%, **according to McKinsey**. Consumers expect a seamless experience from their bank, along with high level of service, and personalised communication, starting with the first touchpoint, which could be the onboarding process or opening a current account.

Digital onboarding – a key differentiator for financial services

Digital onboarding starts the moment a customer wants to use your products and services and it requires a careful mix of technology and data, with digital identity (management) being the essential ingredient of successful processes. But banks and financial institutions don't always get it right. The experience of opening accounts with traditional institutions leads to many common friction points like being re-routed to different channels, the need to provide physical identification, answering the same questions multiple times, and long delays to access the account.

A few years ago, **Fenergo**, a client lifecycle management technology developer, conducted a study with Forrester Consulting, to measure the time, costs, and challenges involved in onboarding institutional clients. Some key findings revealed that *financial institutions generally don't have a good view about the average time it takes or how much it costs to onboard new clients*. For instance, broad estimates suggest *it takes two to 34 weeks for financial institutions with completely manual client onboarding processes*.

Though it proved hard to calculate how much it costs to onboard a new client due to the fragmented nature of the onboarding process (spanning sales, onboarding, compliance, credit, legal and back-office operations), broad estimates suggest that it costs up to USD 25,000 per client, with the average cost calculated at USD 6,000 per new client.

To find some answers to these issues, in this chapter, we have gathered knowledge, insights, and hands-on expertise from top consultants, lawyers, and digital identity solution providers on 'Best practices in digital onboarding, identity verification, and e-KYC'.

John Erik Setsaas, **Signicat**'s VP of Identity and Innovation, has managed to spot the point where companies fail to do onboarding properly, as *'most often, companies and service providers focus on only one aspect of a customer's digital lifecycle, whether that is onboarding or electronic signing, and fail to capitalise on a customer's full digital engagement potential'*.

Consult Hyperion's **Steve Pannifer** ponders over the legal implications of customer onboarding and agrees that *'onboarding is just the start'* as *'once you have navigated your way through the complexity of building onboarding processes that both satisfy the relevant regulatory requirements and work for your customers, you cannot relax'*. A well-known point of friction and a key component of the onboarding to any financial service is the **'Know Your Customer'** process, a step that checks to confirm they know who is requesting the service and that the request is legitimate.

KYC was born at the end of the 20th century. The old-style KYC procedure was guided by the 'paper only' principle, when information was very limited, and the Courts and prosecutors were hardly involved at the time. Currently, camera onboarding has become the new normal, if

Your First Impression Counts, So Get It Right

of course certain basic conditions have been set up in the meantime, such as the requirement of the customers' consent, the condition that the passport must be readable, the person on the picture must be recognisable etc. Security and storing requirements are standard features for camera onboarding today.

However, even though the KYC processes have improved over the last decade, there are still issues associated with insufficient online KYC programs. Sometimes, the automated digital onboarding is not fully recognised, as **there is general scepticism to trust the machine**. Regulators in many jurisdictions still require a human intervention.

Cameron D'Ambrosi, Principal at **One World Identity**, takes a look at the status quo of customer onboarding and raises some awareness around data protection as *'with an ongoing wave of data breaches and an unprecedented amount of personal data on the dark web, knowledge-based verification is often easier to complete for fraudsters than it is for consumers. A full set of personal information sufficient to pass KBA can be obtained for about the price of a fancy New York City cocktail'*.

Frictionless, secure, innovative… all add up to the idea of the ideal digital onboarding process. However, considering today's digital world, the word 'identity' is meant to allow people to exercise their rights or to prove who they are. Sometimes identity systems can be sources of exclusion. If we investigate the future of the customer onboarding process, our colleague, **Simona Negru**, stresses the need to create systems that include also *'the transgender people who might present themselves differently than the name and gender on their IDs', which 'might lead to abuse and discrimination'*.

What can businesses do to not miss out on the opportunity?

Financial institutions **aiming to improve the customer account opening experience are advised to think across all steps in the process**, starting with discovery and data capture and continuing to give customers clear value from the new account. These strategies could reduce the abandonment rates and increase the number of people that become customers.

When it comes to the customer onboarding processes, to understand what constitutes distinctive customer experience in financial services, **McKinsey analysts** found four pillars of great customer-experience performance:

- ***Focus on the few factors that really count for your customers***

Transparency of price and fees, ease of communication with the bank, and the ability to track the status of the onboarding process account for overall satisfaction.

- ***Make it easy (less time consuming)***

Simplifying the onboarding process and cutting down the time it takes to apply for an account have deep effects on customer satisfaction. For example, **in France, customer satisfaction drops by up to 30 percentage points when the time to open an account exceeds 45 minutes**. **In the UK**, 40% of consumers had abandoned bank applications before they were complete, due to dissatisfaction with onboarding processes. More than 1 in 3 of these abandonments were due to the amount of time it took to complete the details required.
As more processes are digitised, journey times will be cut back. Nevertheless, low cycle times alone don't equate to superior user experience, and McKinsey research indicates that customers respond most positively to the ease of a transaction or process.

- ***Master the digital-first journey, but don't stop there***

While customer journeys could be completely online, others start online and finish in a branch, or start in a branch and finish online, or can take place fully in a branch. In their research, McKinsey analysed these different types of journeys, and found that overall, digital-first journeys led to higher customer-satisfaction scores and generated 10 to 20% more satisfaction than traditional journeys.

Your First Impression Counts, So Get It Right

Moreover, many financial services do not provide fully digital services even when they exist, such as digital identification and verification. Therefore, financial-services providers can still significantly improve customer experience by digitising complete journeys.

• Brands and perceptions are important

Inspiring your customers with the power and appeal of your brand or generating word of mouth via advertising can deliver 30 to 40% more satisfaction than companies that don't adopt marketing strategies.

Even if the above four hallmarks for outstanding customer experiences tend to be universal, CX designers should also consider a range of customer preferences based on country, product, and age group. If we take age for instance, the ability to identify the right products is more important to 18-to-24-year-olds than to those 55 and older. This suggests that processes and value offerings need to be modular with their emphasis varying with what matters most to each customer segment.

Hoping that I stirred your curiosity around these topics and before I reveal too much from this chapter, I suggest we start reading.

Mirela Ciobanu | *Senior Editor* | The Paypers

Consult Hyperion

Digital Onboarding – the Beginning and End of Digital Services

About Steve Pannifer: Steve is COO at Consult Hyperion and a digital identity and security expert. Steve has a detailed understanding of the global digital identity market having advised numerous organisations around the world on all aspects of digital identity – commercial, technical, and regulatory. He is actively involved in key identity initiatives in both government and financial services sectors, and is a regular speaker at digital identity conferences and events.

Steve Pannifer ▪ *COO* ▪ Consult Hyperion

Last year we celebrated the 30 years of the web. Over those 30 years, we have been on an unstoppable journey towards the digitisation of everything. But we are not there yet. In financial services, one of the most mundane things is preventing the full digitisation of services – onboarding. The processes employed often place friction where you can least afford it, at the point you are starting to build a new digital relationship with a customer. At one level onboarding needs to be hard – it needs to be hard enough that fraudsters and money launderers cannot exploit the services. But all too often, that involves making it hard for everyone else as well.

KYC is hard

A key component of the onboarding to any financial service is the 'Know Your Customer' process. This is where the financial service undertakes checks to confirm they know who is requesting the service and that the request is legitimate. It is a well-known point of friction. In their **'Battle to Onboard' market research, Signicat** found that 'nearly 40% of consumers abandon digital onboarding processes'. Why? Because financial services are all too often employing identity-checking processes that were not designed for the digital world. Asking people invasive questions or requiring them to fiddle around with paper documents is no way to introduce someone to a forward-looking digital service.

KYB is harder

When it comes to onboarding an organisation, the problem gets harder. Much harder. To complete a 'Know Your Business' process, the financial service needs to establish the identity of organisation, the nature of its business as well as identifying the persons with significant interest or control. This can involve asking the business for documentary evidence to show who they are and what they do. It can also involve checking third-party data sources to corroborate that evidence. The problem is that there are many types of organisation (companies, charities, partnership, societies, trusts, and so on) with different structures and ownership arrangements, so getting to the bottom of the purpose of the organisation and determining who has significant interest or control can be time consuming and difficult.

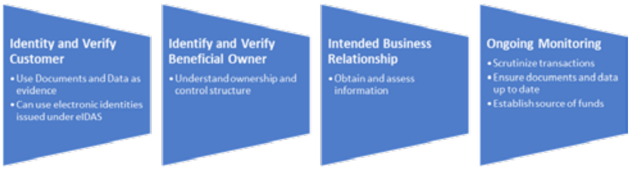

Identity and Verify Customer
• Use Documents and Data as evidence
• Can use electronic identities issued under eIDAS
Identify and Verify Beneficial Owner
• Understand ownership and control structure
Intended Business Relationship
• Obtain and assess information
Ongoing Monitoring
• Scrutinize transactions
• Ensure documents and data up to date
• Establish source of funds

Figure: Elements of Customer Due Diligence based on Article 13 of the 4th European AML Directive (modified by the 5th European AML Directive)

Is this something technology can solve?

At one level yes. KYC and KYB processes can be broken down into discrete steps and technology can help at each stage. Mobile technology can be used to accurately scan documents, biometric technology can be used to identify or authenticate people, advanced analytics can be used to normalise data and pinpoint the right records. Different technologies need to be employed at different points in the process, however. →

And putting it all together in a way that works for every customer may not be straightforward. Some customers will embrace new technology and be happy, for example, to use mobile technology to upload evidence and perform biometric identification checks. Others will not.

Ultimately it is not about technology however – it's about data. The data you collect from your customers needs to be verified against reliable sources. In countries like the UK, with its love of credit, the credit bureaux have been the mainstay data source, aggregating information on a large proportion of individuals and businesses.

Even then data quality issues, and the use of different identifiers across data sources, will mean that frequently the verification of customer data cannot be fully automated. Furthermore, the beneficial owners of the business you are verifying could live in a different part of the world where such comprehensive data sources may not exist.

The 5th European Anti-Money Laundering directive has put in place measures to help with this. As of 10 January 2020, European governments are required to provide public registers of the ultimate beneficial owners of businesses. Only time will tell how effective these registers are at helping financial services meet their onboarding requirements.

Onboarding is just the start

Once you have navigated your way through the complexity of building onboarding processes that both satisfy the relevant regulatory requirements and work for your customers, you cannot relax. AML regulations require you to continue to 'know' your customer. That means keeping records up to date and knowing when something has changed that could affect the customer. For business customers, this is a lot of work. Think of all the changes that can occur during the life of a business. Changes in ownership, control, and purpose are all things that could require you to revisit the due diligence performed on the customer when you first onboarded them. You should require your customers to tell you of such changes but you cannot rely on it. This again is a place where data plays an important role. Monitoring the media, for example, may flag up changes affecting one of your customers.

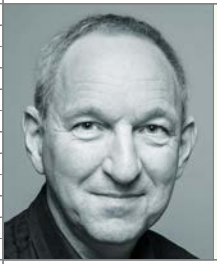
Digital onboarding is a key differentiator for financial services today. It requires a careful mix of technology and data. It is where your new customers begin. Don't let it be where they end.

About Consult Hyperion: Consult Hyperion is an independent consultancy. We hold a key position at the forefront of innovation and the future of transactions technology, identity, and payments. We are globally recognised as thought leaders and experts in the areas of mobile, identity, contactless and NFC payments, EMV, and ticketing.

www.chyp.com

Signicat

Signicat's John Erik Setsaas shares insights about successful digital onboarding processes for customers via electronic signatures and gives us a sneak peek into the future of digital identity



About John Erik Setsaas: John Erik Setsaas is VP of Identity and Innovation at Signicat. He is responsible for ensuring that Signicat's digital identity services are at the forefront of innovation, and solve the needs of customers, partners, and end users. John Erik Setsaas has over 20 years' experience in identity and over 30 in software product development. He is also a board member of the EEMA, Europe's leading digital identity think tank.

John Erik Setsaas ▪ *VP of Identity and Innovation* ▪ Signicat

The payments industry sees achieving consumer trust as a crucial feature of a successful business. Why are electronic signatures important topics for this idea?

Doing business online requires an inherent need for trust where we are witnessing fraud to be increasingly sophisticated, especially in the payments industry. Criminality is common where payments are easier to intercept in a digital society. In Europe alone, the annual value of fraudulent transactions was EUR 1.8 billion.

An electronic signature is a legal way to get approval on electronic documents or transactions such as payments. It can replace a handwritten signature in virtually any process and is legally valid. And remember that electronic signatures are also tamper-evident, meaning that any change to an electronically signed document will be flagged.

> *“Doing business online requires an inherent need for trust where we are witnessing fraud to be increasingly sophisticated, especially in the payments industry.*

With the well-established infrastructure in Norway, it is simple for anyone to sign a document electronically, which is used a lot from borrowing money, renting an apartment, to confirming the name of your newborn child.

How can electronic signatures enable financial institutions to balance compliance (there are many regulations, with updates) and customer experience?

As we are used to scribble a signature with a pen on a paper, a lot of people think that an electronic signature is scribbling the same signature on a digital device. But it is important to note that this does not give any identification of the user signing, so a better mechanism is needed. For an electronic signature to be useful for financial institutions, it must identify the signer. This is also the requirement from the eIDAS regulation for AES (Advanced Electronic Signatures) and QES (Qualified Electronic Signatures). In addition, the signed document must be tamper-evident, meaning that any changes to the document after the signature was added shall be detected.

The difference between AES and QES lies in the processes to both validate the identity of the signer, and the requirements of the signing solution. In general, QES is more complex and more costly, and may not always be needed.

There are two real benefits of using AES or QES which is that it firstly is efficient and secondly, secure. In our digital age, paper-based processes of signing, sending reminders, scanning, and e-mailing should be obsolete in all business operations. Not only should consumers' electronic signatures be verified and secure, but the management should be automated, thereby speeding up financial institution's operations resulting in significant cost reductions and improved customer experiences. ➔

SIGNICAT
Trusted Digital Identity™

What is the complete digital identity lifecycle? What services should a service provider offer in order to achieve it?

Most often, companies and service providers focus on only one aspect of a customer's digital lifecycle, whether that is onboarding or electronic signing, and fail to capitalise on a customer's full digital engagement potential. Signicat's Digital Identity Platform enables the full digital identity lifecycle, incorporating the most extensive suite of identity verification and authentication systems in the world, all accessible through a single point of integration.

Signicat is a qualified trust service provider (QTSP) enabling the full digital identity lifecycle from:

1. **Onboarding** - verifying a user when they first onboard to a business or service;
2. **Validation** - verifying a user against additional due diligence checks such as against any sanction lists, address registries or credit scores;
3. **Authentication** - once users are onboarded, returning users will need secure methods to continue logging in and accessing those services;
4. **Electronic signing** - ensuring users can sign legally binding agreements online, in a secure and trustworthy way.

The foundation of the platform is the technical 'hub'. Businesses can get all the tools they need for their customers' digital identity through us, no matter where they are located or conduct business. The hub provides access to the following services:

- Electronic Identities – we connect to over 25 electronic identity (eID) schemes globally;
- Attribute providers – connect to public and private registries to provide additional information about a user (B2C) or organisation (B2B)
- Identity verification providers – do additional verification checks such as scanning of over 6000 identity documents from passports to driver's licenses; to enabling web-based video interviews; to NFC-reading of passports.

How can financial institutions (especially banks) boost the customer onboarding process with the help of digital identity verification solutions?

Signicat's **Battle to on Board III** study conducted in 2018, surveyed over 3500 individuals in over six countries in Europe demonstrating that 40% of consumers abandon onboarding. That's 2 out of 5 customers that financial institutions – especially banks – are failing to recruit. Financial institutions spend significant funds to first attract these customers, which is then completely wasted due to cumbersome onboarding processes. Among consumers, 25% describe financial services applications as somewhere between difficult and painful to complete where they find onboarding takes too much time, there is too much personal information users have to provide or there is an overall poor user experience. The challenge here is that only 10% of financial service providers see their own onboarding process as difficult or very difficult.

Compared with a paper-based onboarding processes, digital onboarding reduces the average time it takes to onboard a customer. Aegon, one of the world's leading financial service organisations providing life insurances, pensions, and asset management was able to reduce customer onboarding from 4 days to 30 seconds using Signicat's Digital Identity Platform. In addition, they had savings of EU 100,000 and 2400 kg of paper in their first year, as a result of the effective digital onboarding process.

About Signicat: Signicat is a pioneering, pan-European company with an unrivalled track record in the world's most advanced digital identity markets. Its Digital Identity Platform enables the full digital identity lifecycle, incorporating the most extensive suite of identity verification and authentication systems in the world, all accessible through a single integration point.

www.signicat.com

ID Crowd

Cross-Border Digital Identity and Onboarding

About Adam Cooper: Adam Cooper is a technical consultant to the World Bank ID4D programme, and an advisor to international initiatives such as the UN Commission for International Trade Law, the MOSIP Modular Open Source Identity platform, and the Scottish Online Identity Assurance Programme.

Adam Cooper ▪ *Technical consultant to the World Bank ID4D programme* ▪ ID Crowd

Countries all over the world are working on or implementing digital identity systems. Almost always these identity systems are specific to the nation sponsoring its creation based on national laws, cultural preferences, and local requirements. But identity in general is something that we use everywhere not just in our home country – thus, in the same way that people are mobile, so should be their ability to assert identity in a digital context.

Identity is also an enabler, a building block of digital economies, and a means of service transformation, as it makes services easier to access particularly for those who most need to transact whether that be financial, access to education or to healthcare.

Understanding digital identity in different contexts

When we consider cross-border use of digital identity, what we really mean is recognition of digital identity in other contexts i.e. an identity from one country being used to access services in another country, not because it is the same type of identity as in the second country but because it can be understood and can be trusted. The European Union created a law defining such a system, the eIDAS Regulation, which enables compliant EU member state digital identities to be used in any EU country for access to public services, and in time, private sector services. This is achieved though the creation of a trust framework that supports the concept of mutual recognition of digital identities.

One of the key aspects of eIDAS is that it does not insist on the harmonisation of identity systems. Instead it provides a reference point, a set of outcome-based standards, to which each country can measure its digital identity system so that other countries can understand the level of trust conveyed when individuals authenticate with an identity obtained from their country of residence. In this model each country is free to implement the digital identity systems most appropriate for their internal needs, but can still enable their citizens and residents to use their identities to access services in other countries.

The concepts behind eIDAS, particularly that of mutual recognition, are being actively explored in other jurisdictions and geographic areas. For international trade law purposes the UN is working on a means of enabling a trust scheme allowing public and private sector digital identities to be recognised at potentially global scale. There is also increasing interest in countries with highly mobile populations as seen in many African states. Recognition of schemes and identities holds many advantages in these situations such as making it easier to trade, cross-borders, and prove eligibility to access services as citizens' go about their daily lives.

Equivalence, interoperability, and liability: a constant quest

So how do we create the right conditions for mutual recognition and enable people to use their digital identities in another country or jurisdiction? The three largest problems to solve are equivalence (of identity), interoperability (between the underlying systems and services), and liability (who is responsible when something bad happens such as eID being used to enable fraud). ➔

The answer is to seek outcome-based equivalence to a reference standard that all participants can accept, thereby creating a common language that describes the trust level for each digital identity regardless of which participant scheme created it. When we talk about equivalence we often speak in terms of levels of assurance and how we 'map' from one scheme to another. For example, the eIDAS Regulation defines a common set of levels of assurance (LoA) that all participating identity schemes measure their capability and issued identities against. Many potential reference points for LoA exist, such as those provided by **NIST**, **ISO**, and **eIDAS**, but schemes may also decide to create their own derivatives as long as all participants agree on a single reference point.

How do we ensure that digital identities once created comply with these reference standards? Under eIDAS this is achieved through a mechanism of cooperation between countries which draws heavily on EU law. More practically, certification is a proven and well understood mechanism for gaining confidence in the compliance of a system to certain standards.

To achieve technical interoperability there needs to be means of transferring assertions containing the result of authentication and any required attribute data between the provider of identity and the consuming service (relying party). This can be achieved, as in eIDAS, with a common technical specification for these assertions and rules for the authentication process that each party understands.

Alongside these assertions there must be a conveyance of trust at the technical level usually provided through cryptographic means including digital signatures or public key encryption. Technically this interoperability could be implemented in many ways and supports self-sovereign as well as more traditional node infrastructures.

We also need to know who takes responsibility when things go wrong. Defining liability in digital identity systems is vital, it engenders trust between those providing and those consuming digital identities, and it should show clearly who is responsible when incidents occur. The key is to ensure that the provider of identity is liable for damage caused due to intentional or negligent failure to comply with its obligations as defined by the cross-border identity scheme such as failing to verify the identity of individuals holding a digital identity, or failing to implement measures to guard against data breaches.

Finally, there is governance, a means of agreeing the rules and standards for equivalence, interoperability and liability, and a mechanism that encourages those running compliant identity schemes to work together in an impartial forum.

About ID Crowd: ID Crowd specialises in mitigating business and technology risks relating to identity, helping clients understand how to better trust their customers and the businesses they transact with. We understand the critical and interrelated concepts of digital identity and trust together with the various threat vectors including cyber-attack, identity and eligibility fraud.

www.idcrowd.co.uk

Cracking Down on Fake IDs

The Paypers sat down with Daniel Suess, Commercial Director at Keesing Technologies, to learn about innovative ways to establish a customer's true identity

About Daniel Suess: Daniel, MBA International Business at EUBS and Commercial Director at Keesing Technologies, helped the company to successfully transform from a database publisher into a software service provider in the identity verification space. Daniel guided his team in the successful onboarding of many international governmental and commercial clients for Keesing's cloud based and on-premise identity verification solutions.

Daniel Suess ▪ *Commercial Director* ▪ Keesing Technologies

Counterfeit and forged ID documents are found yearly by law enforcement officers. How big is this problem and how does it affect the payments industry?

As consumers and businesses transition their banking activities to the online and mobile channels, it becomes more difficult to verify customers through these faceless channels, thus leading to a rise in fraud cases. In fact, **financial service providers reported fraud rates up to eight times higher in their digital channels** compared to the branch. In recent years, **fraudulent digital financial transactions** amounted to EUR 1.8 billion annually in Europe. In the UK, digital payments and remote banking (internet, telephone, and mobile banking) fraud **totalled GBP 152.9 million in 2018**.

> *With the release of our Keesing Web API, we successfully transformed to a full-service identity verification provider serving the digital world.*

For financial service providers, fraud has increased dramatically in recent years, specifically in cybercrime, identity theft (data breaches), and synthetic identity fraud. The rise of synthetic identity fraud is costing the financial industry considerably: the billions of consumer data records* that were exposed in data breaches the past years are in the hands of criminals and present them with unique data to transfer money using stolen, spoofed or fake identities. Consequently, simply assessing personally identifiable data (e.g. login details, e-mail, address) is no longer sufficient to prevent fraud. It's critical to verify the unique data associated with a customer's (digital) identity.

To combat the rise in fraud, financial service providers implement digital Know-Your-Customer (KYC) programs**. Digital customer identification is paramount for remote customer onboarding and also for identity proofing and financial transaction monitoring. To ensure a smooth digital process, banks and other financial service providers start using biometric technologies for the remote identification of their customers, supporting, for example, selfie-based identification. As organisations adopt digital transformation and biometric technology, **thorough ID document verification remains imperative**. Unfortunately, biometric checks sometimes fail to meet legal requirements or security standards. In these situations, **thorough ID document verification offers the most reliable solution for establishing a customer's true identity**. At Keesing we believe that an accurate and reliable ID verification process consists of a combination of biometric checks and thorough ID document verification. AuthentiScan's unique ID verification technology enables our users to accurately cross-check the ID documents of their customers against Documentchecker; the world's most comprehensive ID reference database. With AuthentiScan Keesing provides an unparalleled balance between remote, biometric identity proofing with trusted ID document verification. →

*More than 14.7 billion consumer data records were exposed in data breaches from 2013 (KPMG Global Banking Fraud Survey)

**85% of financial service providers have implemented digital Know-Your-Customer (KYC) programs (EY Global Banking Outlook)

Narrowing down the topic to personal ID, how can document authentication and verification processes prevent counterfeiting of documents and reduce instances of identity fraud?

Much like a car thief will choose to steal a car without an alarm, a fraudster will be deterred from using a financial institution that has an effective ID verification process in place. While these processes certainly protect against ID fraud, no system can offer a 100% guarantee.

With AuthentiScan, however, we offer our customers ID verification technology of the highest quality. This technology builds on almost a century of expertise that is reflected in the ID reference database powering our solution. With the unique combination of cutting-edge biometric technology and our trusted ID verification we offer customer identification that is accurate and reliable.

How do companies like Keesing Technologies enable businesses to achieve regulatory compliance while streamlining their customers' onboarding journey?

The AuthentiScan web API offers a seamless identity-proofing system that enables businesses to onboard new customers remotely and achieve regulatory compliance while streamlining their customers' onboarding journey. In the web API, Keesing combines its trusted ID document verification with biometric facial recognition and liveness detection functionalities, guaranteeing an extremely secure customer identification process.

AuthentiScan guides the customer through the process of taking a photo of their ID document and a selfie for facial comparison with the photo on the ID document. To ensure biological identifiers are from the proper user and not from someone else, liveness detection takes place through eye (blinking) and lip movement (smiling) analysis. The addition of liveness detection to the process bolsters security by making it extremely difficult to impersonate the individual whose photo appears on an ID document. The ID document is then rigorously verified against Keesing's ID reference database Documentchecker, which contains information on more than 6,000 ID documents from over 200 countries. This process provides ID document verification that can be trusted. AuthentiScan also includes OCR (Optical Character Recognition) autofill functionality to speed up the enrolment process for both the business and customer, instantly boosting efficiency and providing a convenient onboarding experience. AuthentiScan meets all Anti-Money Laundering (AML) compliance mandates and creates a compliance report for each onboarded customer.

Education and collaboration are used by fraud teams as important tools to fight counterfeit documents. How can technology companies assist them in this matter?

Keesing Technologies has been around for almost a century, allowing us to build an extensive network and in-depth knowledge of ID verification and authentication. This knowledge is used in the development of our new technologies and products, as well as by the document experts at our Helpdesk. Our document experts use our large global network to stay up to date on the latest developments and releases of ID documents. We share our knowledge and expertise with regard to ID documents and fraud (prevention) via training courses, lectures, and workshops worldwide provided by document experts from the Keesing ID Academy. Through the ID Academy and our ID verification solutions we build on our mission to help organisations prevent and combat ID fraud on a global scale.

About Keesing Technologies: Keesing Technologies leads the way in digital ID verification since 1923. The objective of Keesing is to help organisations prevent fraud by providing easy-to-use, cloud-based and on-premise identity proofing solutions combining biometric checks with its trusted ID document verification technology. Keesing's solutions are known for their security, accuracy and usability.

www.keesingtechnologies.com

The Paypers

Trans and Gender: An Issue of Non-Conforming Identities in Today's Digital World

About Simona Negru: A graduate of English Language and Literature studies, with an MA in American Studies, Simona is always on the lookout for the best and new stories to capture. A passionate content editor, Simona is keen on discovering and sharing all the relevant news and topics on both distributed ledgers and cryptocurrencies, as well as online security and digital identity, all while finding the hottest trends in the industry for The Paypers' readers.

Simona Negru ▪ *Content Editor* ▪ The Paypers

Why being different is an issue?

Article 6 of the **Universal Declaration of Human Rights** states that: 'Everyone has the right to recognition everywhere as a person before the law'. Considering today's digital world, the word 'identity' is meant to be a key driver for financial and social inclusion, as well as a means of allowing people to exercise their rights or to prove who they are. However, sometimes identity systems can be sources of exclusion. If we take into account the transgender people who might present themselves differently than the name and gender on their IDs, we can see that this situation might lead to abuse and discrimination.

In fact, **32% of individuals** whose name and gender represented on their IDs don't match with how they present themselves reported negative experiences including harassment, denied services, and/or physical attacks. Changing government identification and applying for banking services (e.g. opening accounts, issuing payment cards) are also some of the biggest struggles transgender people face nowadays.

The US

Around **1.4 million adults** in the US consider themselves transgender, meaning they identify as a gender that differs from the one on their birth certificate. Moreover, a survey from the National Center for Transgender Equality conducted in 2015 found that only **11% of transgender** Americans reported that all of their IDs had the preferred name and gender, while 68% suggested that none of their IDs showed this information.

In addition, if a trans person wants to open a bank account, start a new job, enrol in school or travel, they need accurate and consistent IDs. The issue is that because of the federal government's strict requirements – court orders, proof of surgery etc. – only the persons **who have already transitioned** have been able to update all of their ID records.

Europe

The Council of Europe requires that all its member states provide for legal recognition. However, **20 countries demand trans people to undergo sterilisation** before their gender identity is recognised, and only 5 European countries spare transgenders from experiencing sterilisation, medical interventions, divorce, or a psychological diagnosis or assessment. These requirements and the lack of clear legislation result in the fact that most trans people abide by documents that do not match their gender identity.

Asia

In India, the Aadhaar ID is 'de facto mandatory for bank accounts, SIM cards, tax filings, and school enrolment', with more than 1.2 billion IDs being issued, as per government data. However, large numbers of marginalised and trans people are denied or excluded from services. More precisely, an estimated 102 million people – 30% of the country's homeless population and over a quarter of its trans people – do not have Aadhaar but are more likely exposed to errors in their ID information, which could lead to denials of welfare services. When requested to comment on the matter, the Unique Identification Authority of India (UIDAI) denied any response. →

Embarking on a quest to change the world

For the transgender communities, payment cards can be a source of sensitivity, as their chosen names don't always appear on the front of them. These issues have not been overlooked by companies and banks that don't want to misrepresent these people's identities on the issued documents. As such, Mastercard is one of the companies that addressed these challenges by introducing its True Name card initiative in June 2019, which enables chosen names to appear on credit, debit or prepaid cards, with no requirement to change the legal birth name before applying for a card.

When proposing its ideas, Mastercard's goal was also to prompt more banks and issuers to start rolling out this feature in a bid to bring non-discriminatory banking and credit services to the trans community. And it seems that it succeeded: two financial institutions, more precisely BMO Harris and Superbia credit Union, announced their intention to launch this capability across their card offerings. Superbia plans to roll out the True Name feature across its Mastercard products somewhere in spring 2020, while US-based bank BMO Harris already launched this feature on personal debit cards in December 2019, considering that **'Breaking down barriers to inclusion requires bold action'**. Therefore, before printing their debit card, BMO customers are given the option to choose between their legal and preferred name to be added on the BMO Harris Bank Debit Mastercard.

Aiming to facilitate the customers' banking experience, HSBC also offers its transgender community a choice of **10 new gender-neutral titles such as Mx, Ind, M, Mre, and Misc**. This service reflects the 'financial needs of the trans community', and it was applied across customers' accounts including their bank cards. Similarly, UK-based Metro Bank added the title **'Mx' alongside Mr, Mrs, Miss, and Ms**, after a Scottish teenager was not able to open an account because her only option was to tick either the male or female box.

Let's see how bright the future is

While some may consider that these new products reflect a commitment to diversity, inclusion, and acceptance, when people want to use differing forms of conflicting personal identification, we should also speak about the elephant in the room: several unaddressed questions drag along a whole other range of problems. For example, **LexisNexis Risk Solutions said that what Mastercard's initiative** does is to acknowledge that banks still have work to do in verifying customers whose names or identifying attributes may have changed over time. However, the issue with this is that changing the tech that supports banks' capabilities to check identities across a range of use cases will likely take time because of complex, legal and regulatory requirements.

If, on the other hand, a trans person decides to legally change their name, there are significant costs involved, not even mentioning the bureaucracy – **from court orders to change legal names, to state and federal agencies** that must verify that no one is trying to defraud the state. The National Center for Transgender Equality found in their survey that almost one-third of trans people can't afford to change their name because of the cost, which can range from less than **USD 100 to USD 2,000**. Also, fees required by the process of obtaining a **legal name change may include the cost of legal help, court fees, and newspaper publication**. As a result, **35% transgender people have not changed their legal name, and 32%** have not updated the gender on their IDs. Another issue found in the survey is that 25% experienced health insurance issues, including denial for healthcare-coverage for gender transition or simply routine care.

What is sure is that organisations such as NCTE (National Center for Transgender Equality) or TGEU (Transgender Europe) work to remove all sorts of barriers (e.g. surgery, court order requirements) to make sure that trans people have access to accurate IDs. **NCTE, for instance, provides technical support** for states, in a bid to update their name change, diver's license, and birth certificate policies. **TGEU runs campaigns** providing research, legal analysis, and advocacy materials, to raises awareness regarding transparent legal gender recognition procedures. The question that comes to mind is: what's next to come? Will these attempts be successful and indeed change the most reluctant minds? Will we see alternative names on driver's licenses or will trans people soon be enabled to choose any desired name when opening a bank account or applying for a loan anywhere in the world? We should see what the future holds.

One World Identity (OWI)

A Look into the Future: Customer Onboarding

About Cameron D'Ambrosi: Cameron D'Ambrosi is a Principal at One World Identity and host of the State of Identity podcast. Cameron is responsible for supporting OWI's advisory services platform by offering clients key insights into the companies and technologies shaping digital identity today.

Cameron D'Ambrosi ▪ *Principal at One World Identity and host of the State of Identity podcast* ▪ OWI

Over the past few years, identity and awareness around the concept of identity have changed dramatically. **Identity verification** and Know-Your-Customer (KYC) were once financial industry-specific jargon, with strict regulatory requirements under the USA PATRIOT Act driving a high-level of responsibility to prevent financial crime for both banks and money transmitters. Companies met minimum identity verification standards not to enhance the customer experience, but rather to meet minimum due diligence requirements and safeguard themselves from legal consequences. These 'legacy' anti-money laundering (AML) and KYC procedures have long been associated with high levels of friction and poor customer experience.

It is a storyline that has been told time and time again, but the explosion of the digital economy has forever altered the business calculus when it comes to digital identity. We've seen an explosion of the digital economy. More companies are relying exclusively on online customer touchpoints, which means they're collecting customer data, and we're all familiar with the challenges of maintaining and protecting customer data. The new digital economy comes with demands: customers expect trust to complete these online transactions. For all companies, not just fintech, assurance about who is on the other side of a transaction is now more important than ever.

The bottom line is that identity is no longer a niche, limited to banks and financial services. Awareness of digital id and the concept of controlling personal data is gaining mainstream momentum, thanks in no small part to the Cambridge Analytica/Facebook scandal and a seemingly never-ending list of data breaches.

Even US Presidential candidate, Andrew Yang argued that **data should be considered a property right**. And while there is still a lack of use cases for identity solutions, the circumstances are creating demand for identity solutions that emphasise the customer role in owning their data.

This article will take a look at the status quo of customer onboarding and the problems with the current status quo before moving onto the future of customer onboarding.

Where onboarding stands now

Knowledge-based authentication (KBA) quickly emerged as one of the default identity verification (IDV) methods in the digital economy. A KBA process identifies users by asking them to answer specific security questions to verify their identity. For example, providing your social security number, selecting your previous address from a list of choices, or confirming your approximate monthly mortgage payment. While KBA-based IDV flows are still in use, superior alternatives exist. With an ongoing wave of data breaches and an unprecedented amount of personal data on the dark web, knowledge-based verification is often easier to complete for fraudsters than it is for consumers. A full set of personal information sufficient to pass KBA can be obtained for about the price of a fancy New York City cocktail.

As a result, we're seeing many companies transition to document-based verification that generally includes scanning a physical ID document to prove identity. This is becoming a more common option for tech companies. →

Document-scanning is a step-up from KBA because it requires physical possession of an identity document, which while possible to fake requires more sophistication than purchasing or phishing personal data. Current-generation platforms are implementing AI and machine learning to increase the ability to quickly identify fake documents and approve valid ones, but manual review by human eyes is often required in some instances. For example, when a finger is mistakenly captured holding a document, or glare makes automated processing more difficult.

While document-based flows have helped to improve the user experience and reduce instances of fraud, the fact that users must separately prove their identities to each online platform they wish to join remains inefficient for consumers and costly for businesses. There is a growing buzz in the identity community about the functionality and potential of self-sovereign identity (SSI) platforms to solve these challenges by allowing for users to prove their identity once digitally, and then share that identity across platforms. Basically, you're able to carry around a digital wallet with different types of attestations that prove you are who you say you are. It also represents a system where the users control their attributes, how they are collected, and when they're shared, instead of each individual enterprise managing their own databases, each with millions of potentially duplicate identity records.

The next generation of identity

In this next generation of self-sovereign identity platforms, the initial verification of a user identity is still provided by a third-party document-based IDV provider.

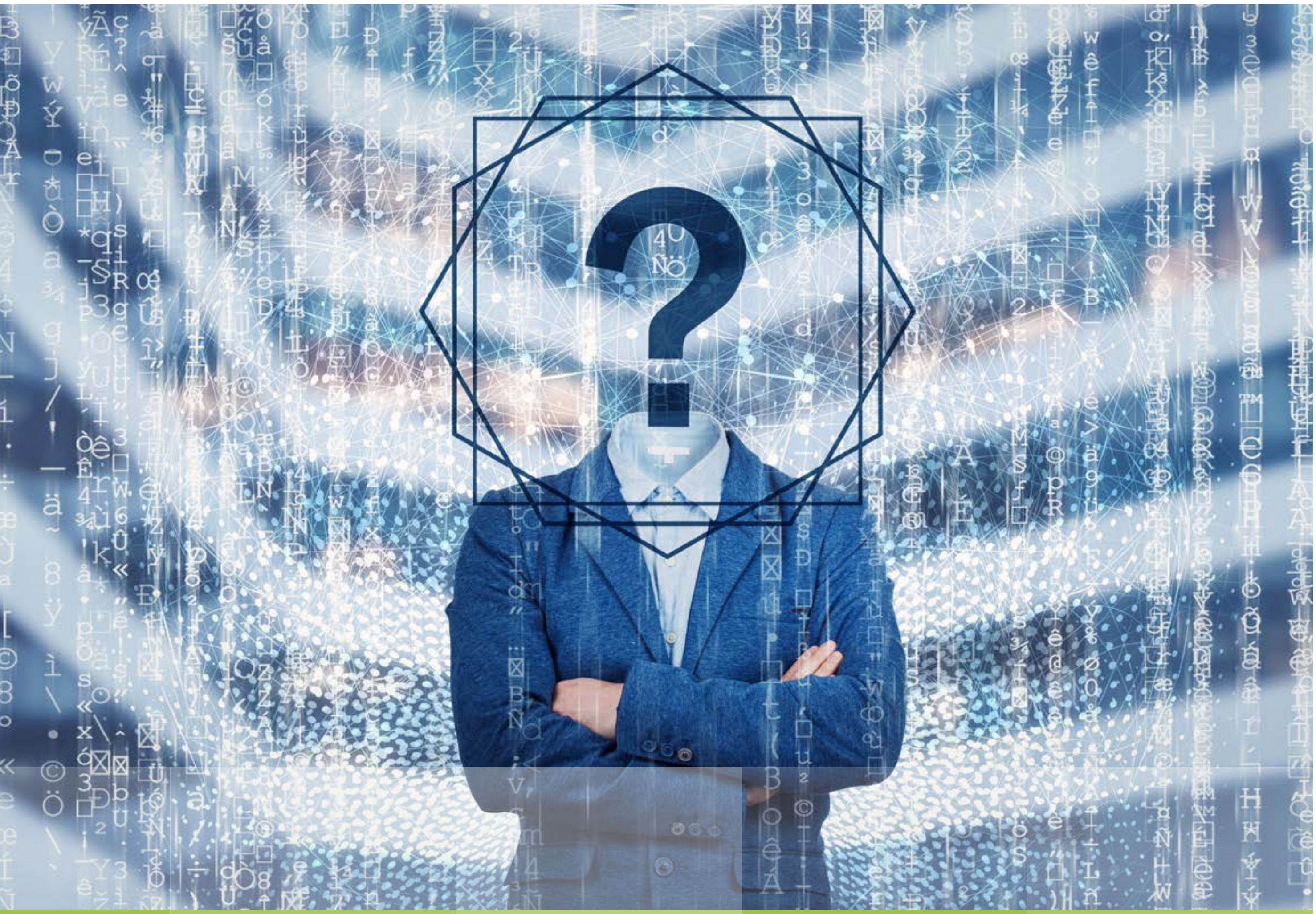
However, once a user is verified, they now have a digital identity credentials that can be used as many times as desired. This means consumers can onboard themselves simply and quickly without having to re-scan their documents while businesses are not forced to bear the cost of individually proofing each new user. This gives the consumer more ability to achieve a high-level of identity verification, and it also gives consumers more control of their data attributes and who they're shared with.

Continued consumer embrace of federated digital identity platforms may continue driving towards an even more seamless future state, where a government API would exist to bridge the gap between consumers and government issuers of identity, cutting out the middle-men currently performing verifications. Under these systems, consumers would be able to connect directly to the source that issued their identity card or passport, for verification directly against the source database. Estonia's eID is a good example of this. The country has one of the most highly-developed national ID-card systems that enables consumers to directly leverage their government-issued digital identity when applying for a bank account, applying for government services, or booking travel.

As demands for proven digital identities continue to grow across all sectors of the economy, the evolution of digital identity will certainly continue unabated. With data breaches and privacy laws continuing to dominate headlines across the globe, expect these issues to remain a focal point of both private and public-sector attention in 2020 and beyond.

About OWI: OWI is a market intelligence and strategy firm focused on identity, trust, and the data economy. Through advisory services, events, and research, OWI helps a wide range of public and privately held companies, investors, and governments stay ahead of market trends, so they can build sustainable, forward-looking products, and strategies.

www.oneworldidentity.com



Identity Verification Methods

A Digitalised World Requires Digital Identities

'This is especially true for regulated sectors such as payment and banking but also education, health, mobility, telecommunications, and certainly e-government', **Maximilian Riege, Chief Representative & General Counsel, Verimi**

The concept of **digital identity is at the core of nearly every interaction of individuals, companies, and even devices**, and it involves multiple distinct processes, such as determining what attributes can be used to identify a person, how to prove them over time, when to share them, and what a person can do with them. To understand **the five core identity use cases**, **OWI has developed a basic framework which includes the creation, verification, authentication, authorisation, and federation** of the digital identity.

In this chapter we will focus on identity verification or identity proofing, with some KYC flavour, security spice, and technology ingredients. Even if all these ingredients are available, the recipe is hard to bake, as customers' high expectations of top-notch user experience (UX) and their demand for omnichannel use of their digital identity make the designing of the digital onboarding process (together with the identity verification part) a complex activity involving many processes, providers, and systems.

The trust dilemma

Today's customers accept no less than real-time digital services, around the clock. If a bank creates, in the eyes of the customers, unnecessary hurdles in the process of becoming a customer, they will most probably switch to a digital competitor. At the same time, anti-money laundering legislation has led to substantial fines already in the financial industry, stressing the importance of high-quality KYC processes.

This situation has led to what **InnoValor/ReadID**'s co-founders **Maarten Wegdam** and **Wil Janssen** call *'a trust dilemma banks face in onboarding new customers'*. Financial institutions must design a KYC process that is smooth and secure, as well as enable *'reverification, app activation, password reset, and other use cases in which the identity of an existing customer has to be re-verified'*. The good news is that *'NFC (technology) is increasingly helping banks to overcome this dilemma. The same NFC chip in mobile phones that enables payment, also enables mobile identity verification. NFC can be used to create smooth customer experience with a high level of trust at a lower cost'*.

Another possible answer to decipher the dilemma mentioned above, could be **the use of electronic identity solutions (eIDs)**. eID is the digital proof of identity of citizens or organisations, used to access benefits or services provided by government authorities, banks or other companies. Apart from online authentication and login, many electronic identity services also give users the option to sign electronic documents with a digital signature.

Identity verification methods such as **iDIN**, **BankID**, and **Itsme** have become very popular as they simplify the process of *'becoming a customer'*, provide access to reliable data, and make it easy to log in as a returning user. *'When it comes to complying with legislation and regulations, Electronic ID Document Verification can help where an eID is not enough, for example when more attributes are needed than an eID shares, or when an additional check of an identity document is required by law'*, according to **Margot Markhorst**, Product Consultant iDIN, **Currence** and **Amos Kater**, Head of Team Online **Currence**.

Moreover, the *'so-called 'lookup services' support flexible combinations of verification methods. With a lookup service, individuals can be matched with other records, such as the Chamber of Commerce records. Additional services can also be provided, for example to perform a check on the name and account number of a person or merchant as reported by his or her bank'*.

A Digitalised World Requires Digital Identities

Since we mentioned data, digital identity, verifying customers' identity, it is also worth mentioning that behavioural biometrics can be successfully applied to leverage customer experience, as it is invisible to the end user because the data is collected passively, meaning there is typically less friction in the user experience in comparison to other biometrics techniques.

Besides user data, this technology can also reveal how the device is held using gyroscopic measurements inherent within mobile devices. According to **Mike Nathan** from **LexisNexis**, *'this type of data is probabilistic rather than deterministic. This means that it is generally used as a risk-factor on whether the transaction appears fraudulent rather than as a deterministic yes/no response that you might get with physical biometrics solution that use fingerprint or iris scanning'*.

Security first

The onboarding process requires identifying customers and verifying their identity with a high level of security and low level of risk, as required by KYC and AML legislation. An important role here is played by IT systems and technical solutions, and, depending on several factors such as channel strategy, the existing technology landscape, and the flexibility in the continuous improvement of the onboarding process, five elements need attention. **According to Deloitte**, these are:

1. **Collecting clients' static data** and **identification document**, plus **checking the accuracy of the information** provided through different methods (e.g. Optical Character Recognition – OCR, a method that extracts textual data from documents, or document validation).
2. **Supporting anti-impersonation solutions** – to ensure financial institutions that the customers applying for the product are 'who they say they are'. This step can be performed via Knowledge-based Authentication (a method mainly used in the UK) and Facial Recognition.
3. **Verifying the customers' identity and compliance** (Anti Money Laundering/Counter Terrorism Financing – AML/CTF) – by running background checks on inputted static data (e.g. name, gender, date of birth, country of residence, nationalities).
4. **Using electronic signatures** to ensure that a contract is duly signed between the customer and the financial institution.
5. **Orchestration** is a key element of the process, as it enables a smooth and transparent experience for the customer who does not see all the systems used during the process.

Financial institutions can implement onboarding solutions following two alternatives, Deloitte's paper added. They can either **orchestrate the digital onboarding process with a dedicated end-to end solution that comes with already integrated technology components, or orchestrate the digital onboarding process using a mix of internal and external technology components** (since financial institutions can leverage existing components such as front end development tools, document management) and orchestrate all services in house.

When it comes to designing the digital onboarding process, not only are technological efforts complex and time-consuming, but also regulations to be applied, as these must be carefully analysed before launching the new digitalised process. These regulations include: Anti Money Laundering/Counter Terrorism Financing (AML/CTF), data protection and guidelines provided by local regulators (e.g. BaFin in Germany, CSSF in Luxembourg).

As digital onboarding is a new type of product, most of the times regulations are not explicit/clear about all the steps of the process. And, depending on the consumer target group, local regulations apply and as a result the process needs to be considered. For instance, the number of documents to provide is different between a digital onboarding in Belgium and France.

Overall, onboarding processes should adopt a customer-centric approach, with financial institutions considering integration feasibility and local requirement, since some of these requirements can be unclear and require special attention.

Mirela Ciobanu | *Senior Editor* | The Paypers

LexisNexis Risk Solutions

Adding Behavioural Biometrics to Digital Identity

About Mike Nathan: Mike Nathan has 15 years of experience in the risk and fraud space, with key interests in online banking fraud, application fraud, internal fraud, and card fraud. Mike started as a credit analyst at Lehman Brothers, before moving to Lloyds Banking Group as a Fraud Manager, where he led large teams of analysts and data scientists. He was a consultant at SAS, the analytics company, and a Vice President at Barclaycard, looking at Credit Card Fraud. As the Senior Director of Solutions Consulting EMEA for Fraud and Identity at LexisNexis Risk Solutions, Mike advises many of the world's largest banks and holds an MSc in Information Management & Finance from Westminster Business School in the UK.

Mike Nathan ▪ *Senior Director, Fraud and Identity, Solutions Consulting, EMEA* ▪ LexisNexis Risk Solutions

Financial institutions continue to face the perpetually shifting task of how to reliably differentiate between good customers and fraudsters. While providing a slick and streamlined online user experience is paramount, the consequences of getting it wrong are costly. It is not just damage to banks' reputation and bottom line at stake, but the lives and wellbeing of end users too. We know that, for the victims of fraud and identity theft, this can be an emotional and stressful experience.

Building solutions to this problem also brings a unique set of challenges: fraudsters are professionals, adapting and developing their techniques to dupe even the most robust systems. This is why a layered defence is key to defending your organisation against fraudulent attacks.

Digital identity intelligence and behavioural biometrics are two key components in this layered defence solution. Digital identity can mean many things to many different people. It can mean the digitising of identity documents such as passports or driver's licences; it can also mean identifying the digital persona of an internet user.

In the case of digital personas, the real-world identity might not be important when deciding whether a digital transaction is genuine or fraudulent. Banks and other financial institutions are constantly looking at both of these versions of digital identity: digital identity documents, to make sure they are fulfilling regulated Know-Your-Customer (KYC) requirements, and digital persona checks, to make sure the transactions are genuine.

Device, IP, and personal data (such as email or telephone number) can be used for both creating and matching digital personas. However, this can be further supported by looking at how the consumer actually interacts with their device – whether keyboard or mobile phone – to further enhance risk decisions.

Enter behavioral biometrics – *the measurement of human behavioural patterns to better identify fraudulent patterns of behaviour and verify/authenticate good users over time.*

Behavioural biometrics collects information related to how a user interacts with their mouse, keyboard or touchscreen. It is also based on how the device is held using gyroscopic measurements inherent within mobile devices. This type of data is probabilistic rather than deterministic. This means that it is generally used as a risk-factor on whether the transaction appears fraudulent rather than as a deterministic yes/no response that you might get with physical biometrics solution that use fingerprint or iris scanning.

One of the key benefits of behavioural biometrics is that it is invisible to the end user as the data is collected passively, meaning there is typically less friction in the user experience in comparison to other biometrics techniques. ➔

Baselining the good customer base

Having contextual rules in your system is essential to model what is normal for that specific user or device, and this approach should be applied holistically for all data points within a fraud decision to answer questions such as: is this a normal ISP for this individual; is this a new city/country for them; how are they psychically interacting with their device? Having this context then allows you to compare what is happening right now to that normalised baseline. This data helps you make better-informed fraud risk decisions.

In an account takeover fraud, the bank will typically have a baselined provision of the user's regular behaviour. This means they're able to detect anomalies that are inconsistent with this behaviour. For example, is the time spend on a particular action unusual for this user? Do they normally use the keyboard or the mouse?

How behavioural biometrics can help with social engineering

Fraud has shifted in banking in the last three to five years. Social engineering and scams have become an increasingly larger problem to solve. An example of a scam: A customer is called by phone and convinced to make a payment to a fraudster. Sometimes the fraudster is purporting to be the bank's own fraud team or a telco supplier. How a bank can identify whether this payment is under coercion? Whilst traditional fraud methods have yielded some success, behavioural biometrics brings many new detection opportunities to the table, including:

- Can we see evidence of duress in the way the customer is interacting with the website?
- Are they taking a lot longer to make a payment because somebody is talking them through what they need to do?
- Has there been any other behavioural changes during the session suggesting another user is involved?

There are lot more factors that need to be considered for this type of fraud including destination account risk, typical payment amounts, and others. Adding behavioural elements provides more information and, more importantly, context: What is happening now and how is it relative to what happened before? Using this information allows banks to come up with more dynamic customer journeys, such as providing pop ups or additional screens to warn the customer that there is some suspect behaviour on the device like a remote access take over. Machine learning and AI is essentially quantifying and identifying human behaviour and behavioural biometrics is a great way to capture actual human behaviour to risk-assess human interactions.

By itself, behavioural biometrics is not a silver bullet to identify fraud. But when it is combined with the other digital features that can be collected from a device, matched against a global digital identity network, and machine learning is overlaid, the overall solution provides a powerful passive fraud and authentication tool which is adaptive, changing as the fraudsters themselves adapt.

The arms-race continues between fraudsters and banks, using tools that better understand the customers can be as valuable as identifying the bad actors.

About LexisNexis Risk Solutions: LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including financial services. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX, a global provider of information-based and analytics and decision tools for professional and business customers across industries.

www.risk.lexisnexis.com/emea

HID Global

The Paypers sat with Olivier Thirion de Briel, Global Solution Marketing Director at HID Global, to discuss why is crucial for banks and financial institutions to offer a holistic management approach towards digital identity when onboarding and servicing customers

About Olivier Thirion de Briel: Olivier Thirion de Briel is Global Solution Marketing Director for financial services at HID Global. In this role, Olivier leads the banking strategy and product marketing for the IAM solutions business unit.

Olivier Thirion de Briel ▪ *Global Solution Marketing Director* ▪ HID Global

How would you portray a complete digital identity journey? What solutions should a provider of trusted identities offer in order to achieve it?

There are 4 main steps in a complete digital identity journey:

1. The identity creation (one can challenge that the identity is created/distributed only after being validated and the identity distribution could be listed as an additional step);
2. The identity verification/proofing to ensure the identity attributes are correct;
3. The identity usage with:
   a. The authentication that is about demonstrating the person is the right owner of an asset;
   b. The authorisation that is about determining what the user can or cannot do based on his identity;
   c. The federation that is about conveying identity attributes and/or authentication across multiple parties.
4. The identity revocation when this digital identity should be removed from the digital world.

> *“Linking the identity verification and the authentication processes greatly improves the overall digital identity security.*

Narrowing it down to the current role that digital identity plays in the process of customer onboarding, what technologies should banks adopt in order to balance compliance, costs, and UX?

If we split the customer digital onboarding process in multiple steps, it would be:

1. Identity verification:
   a. Data capture with ID documents scanning and OCR (Optical Character Recognition techniques);
   b. Document authentication (tamper detection, validity verification etc.);
   c. Biometric capture (electronic facial matching between the face capture and the photo on the document ID, liveness detection);
   d. Customer report generation for KYC compliance checks.
2. Decision making based on KYC checks;
3. Digital contract signature;
4. Account opening.

As a specialist in trusted digital identities, HID Global provides all the identity verification steps.

By covering both the identity verification and the authentication/authorisation/federation, HID Global provides a smooth and consistent UX from end-to-end around the digital identity lifecycle (face recognition onboarding for authentication during the ID verification process and same user experience ‘style’ during the full process). HID helps banks being compliant with KYC regulations and all regulations requiring strong authentication, like the PSD2 in Europe. Additionally, it provides a more secured digital identity as the solution is starting to gather data for threat detection during the identity verification process (device fingerprinting, start building the digital user profile etc.), but it also secures the most critical step of the authentication: the authentication onboarding. Indeed, when successfully completing the identity verification process, the authentication credentials can safely be issued to the right user. →

The demand for identity verification solutions is driven by regulatory pressures and by inefficiencies in investigative techniques. What methods should the banking sector adopt to create secure/trusted transactions?

I think identity verification for digital onboarding is mainly driven by the extension of the digital world and the technology evolution (better quality of mobile cameras, better face recognition algorithms and so on).

As explained before, linking the identity verification and the authentication processes greatly improves the overall digital identity security. So, in order to better secure transactions, banks have to deploy solutions that are provided by digital identity specialists who are able to protect the full digital identity lifecycle.

Do you think mobile ID verification can be the answer to preventing identity fraud?

I don't believe there is one silver bullet to completely prevent identity fraud. However, by proposing mobile ID verification to their customers, banks not only reinforce the security of the digital ID but also provide a seamless user experience that has a direct impact on the efficiency of new customer onboarding by facilitating account creation and diminishing application drop out. It also smooths the KYC process that is constantly evolving and that brings high cost for banks.

Until now, banking has been predominantly about physical trust. How does HID Global enable them to continue this trend in a digital world over the next 5 years?

As discussed in this paper, more and more (banking) operations can be made online. But this expansion will be successful only if the end-customer feels safe and doesn't see his money and data being stolen. In order to ensure this right level of security, banks have to secure in priority the digital identity of the end-user. That is why HID Global is building a holistic trusted digital identity platform where banks will have a full view from end-to-end on the digital identities of their end-customers. This platform will be made of identification, authentication, and orchestration of the whole processes. This will ensure banks to consistently protect the digital identity of the end-customers but also this will allow banks to better know their customer and therefore to better customise their user experience depending on their profile, on their habits, and on their needs. And finally, having one single provider for a holistic trusted digital identity platform simplifies banks' life and reduces costs.

HID Global is proposing today a consistent identification and authentication solution to banks and is leading a development plan to bring more value and more security to the banks. Working with us is a guarantee to be ready for the future.

About HID Global: HID Global provides trusted identity authentication and lifecycle management for people, places, and things. Our modern approach to authentication incorporates an adaptive, risk-based methodology, providing frictionless and continuous experience. Organisations can protect digital identities and accurately assess cyber-risk, by delivering trusted transactions and empower smart decision-making, while going beyond just simple compliance.

www.hidglobal.com

iDIN

Updates on Already Established Digital Identity Schemes

About Margot Markhorst: Margot Markhorst is Product Consultant iDIN at Currence. Her focus is on the online identification service iDIN. She has prior experience in project management at a payment service provider.

Margot Markhorst ▪ *Product Consultant iDIN* ▪ Currence

About Amos Kater: Amos Kater is Head of the Currence Team. Amos has a broad background in payments, telecom, and identity management.

Amos Kater ▪ *Head of the Currence team* ▪ Currence

Industry experts say: *'To date, the focus of many digital identity solutions has been within the identification domain (i.e. customer onboarding, ID proofing, KYC etc.), however the general movement of the industry is now shifting towards a broader ecosystem enabling the sharing of trusted or verifiable data centred around the subject (person, organisation, or thing). All these factors have led to a fragmentation of the digital identity market. But all is not lost. Several collaborative cross-sector organisations are actively working to get everyone on the same page.'*

- How do you comment?
- What has been working great?
- What are some challenges?
- How has PSD2/Open Banking influenced the digital ID space in the Netherlands?
- Plans for 2020 and beyond

How do you comment?

The use of electronic identity solutions (eIDs) such as iDIN, BankID, and Itsme is increasing. The use of eIDs simplifies the process of 'becoming a customer', shares reliable data, and makes it easy to log in as a returning user. Combinations of different verification methods enable a smooth digital customer journey and comply with legislation and regulations. Electronic ID Document Verification can help where an eID is not enough, for example when more attributes are needed than an eID shares, or when an additional check of an identity document is required by law. So-called 'lookup services' support flexible combinations of verification methods. With a lookup service, individuals can be matched with other records, such as the Chamber of Commerce records. Additional services can also be provided, for example to perform a check on the name and account number of a person or merchant as reported by his or her bank.

The benefits of using iDIN

With an eID like iDIN, people can identify themselves online and share attributes (name, address, gender, date of birth, email or telephone number), login or verify age (18+). This is possible because these persons have already been extensively identified and verified by their bank. iDIN is a joint initiative of Dutch banks. With iDIN, Dutch banks contribute to a secure and safe digitisation of the Dutch economy, based on many years of experience with online banking and security and the iDEAL online payment service. iDIN increases usability without compromising security and privacy. Moreover, iDIN secures and protects personal data.

Over 200 organisations in various industries integrated iDIN in their customer journeys, for many different use cases. iDIN can be used directly by (almost) all consumers with the trusted and secure login method of their own bank. Consumers used iDIN already more than 8 million times for logging in and for identification.

➔

Some results:

- Signing up for an account with insurance companies takes 30 seconds instead of 4 days waiting for a letter with access codes by mail.
- Access your credit registration online in a few minutes instead of waiting days for delivery by mail after identification at the post office or bank.
- Saves 160.000 letters a year at an insurance company, amounting to 2.400 kilos of paper. Reliable online identification is more sustainable.
- Another insurance company saved EUR 100.000 in direct costs in the first year since using iDIN.
- Soccer clubs save on manual labour at box offices and in back-offices when identification and verification of spectators is digitised and automated. Online customer journeys are much easier and faster than at physical counters. This provides a much better service to the supporters.
- Healthcare providers can go through an online registration within 10 minutes where previously it could take up to 28 days.
- Taking out a mobile phone subscription now takes a few minutes, where it first took almost half an hour.
- Onboarding new investors within five minutes instead of a few days.
- A lottery that takes responsibility for checking the age (18+) of participants and allows them to confirm their age safely and easily online.

Market uptake

The market uptake is challenging. For example, the digitisation in some branches is far behind and decision processes take long especially within larger organisations. Furthermore, organisations and consumers are not yet fully aware of the value of e-identity.

The influence of PSD2/Open Banking on digital identity in the Netherlands

There are market initiatives to use iDIN related to PSD2 services. iDIN could be used for onboarding users to AIS and PIS, for example. iDIN could also be used for Strong Customer Authentication required by PSD2. iDIN requires two-factor authentication and with iDIN a user always gives explicit consent.

Opportunities & next steps

Citizens often expect iDIN to work for online public services, with social security numbers. This is not yet possible, however iDIN and the participating banks are committed to fulfil those expectations when it is made possible by law. iDIN ensures trust and reliability in online transactions between people, companies and authorities thanks to its universal applicability. The Dutch Tax Authorities already held a two-year pilot with iDIN, with high approval rates by participants.

iDIN is extended with functionality for signing documents. With iDIN Signature, a document to be signed is linked to an iDIN transaction that confirms that the user has signed the document digitally, with his or her bank's login method. In his familiar online banking environment, the customer gives explicit permission to share his data for signing a document.

iDIN is also extended with QR codes. Anyone with a smartphone will be able to scan an iDIN QR code for the purpose of logging in, identification or age verification. Just scan the iDIN QR code, securely approve it in your bank app and you are logged in or identified. The first pilots with iDIN QR codes are started. Thereafter the service will be rolled out this year. Try it out at **https://qrdemo.idin.nl/**.

About iDIN: iDIN is a service offered by banks that allows consumers to use their bank's secure and reliable login methods to identify, login or confirm age on the websites of other organisations. The scheme management of iDIN is vested with Currence, the product owner of iDEAL, iDIN, and Incassomachtigen (eMandates).

www.idin.nl/en/
www.currence.nl/en/

ReadID

NFC First Approach to Instant Mobile Onboarding

About Maarten Wegdam: Maarten Wegdam, PhD, is CEO and co-founder of InnoValor/ReadID. Maarten is an expert in the area of digital identity and online identity verification.

Maarten Wegdam ▪ *CEO and co-founder* ▪ InnoValor/ReadID

About Wil Janssen: Wil Janssen, PhD, is CMO and co-founder of InnoValor/ReadID. His focus is on impact of digital technologies on organisations.

Wil Janssen ▪ *CMO and co-founder* ▪ InnoValor/ReadID

The pressure on banks to make their KYC processes more secure is strong. At the same time, KYC should be as smooth as possible to create a good customer experience. NFC-based mobile onboarding makes it possible to bridge this dilemma. We describe how NFC can lead to an optimal mobile KYC process and what this means for Open Banking.

The trust dilemma

Customers are more demanding than ever. They accept no less than real-time digital services, around the clock. If a bank cannot deliver fast enough or creates, in the eye of the customer, unnecessary hurdles in the process of becoming a customer, a digital competitor is virtually around every corner. At the same time, regulatory pressure increases: anti-money laundering legislation has led to substantial fines already in the industry. The importance of high-quality KYC processes is higher than ever. Traditionally, KYC comes with visits to branch offices. Time consuming, costly and limited to office hours. Digital solutions for KYC have been in the market but have their disadvantages. Optical solutions using photos of identity documents are not secure, video sessions for matching customers to IDs are invasive and costly. Both have a poor conversion and take too long.

This is the trust dilemma banks face in onboarding new customers, as well as for reverification, app activation, password reset, and other use cases in which the identity of an existing customer has to be re-verified. And not only banks: pension funds need attestae de vitae for their customers and border control moves from the big hubs to mobile control. The need for effective mobile identity verification is growing fast.

Fortunately, NFC is increasingly helping banks to overcome this dilemma. The same NFC chip in mobile phones that enables payment, also enables mobile identity verification. NFC can be used to create of smooth customer experience with a high level of trust at a lower cost.

How does NFC work in identity document verification?

Modern passports are great – they are equipped with a chip following the ICAO 9303 standard. This chip contains similar information as is printed on the passport, but with a number of crucial differences. First and foremost: all information is digitally signed and encrypted and cannot be manipulated. Also, the face image is available at a high resolution, without any additional watermarks. Therefore, it is much more suitable for face matching than the printed face image. Finally, a copied chip can be easily detected. Moreover, most modern ID cards have the same chip, the EU even has a regulation mandating this for new ID cards.

➔

The big breakthrough in this technology came with the availability of smartphones with NFC. Basically, all modern smartphones are equipped with NFC, often used for mobile payments. A smartphone can be used to read and verify the chips in identity documents, without the need for expensive additional hardware. This is a great opportunity: by leveraging two things everybody has – a passport and smartphone – identity verification can move to a next level.

Our software product ReadID works on both Android as well as iPhone. The app is used to read the chip, and our software at the server is used to do all kinds of verifications and send the validated information to the bank. These calculations should be done in a safe environment, and not on the smartphone, as smartphones can easily be manipulated. We regard smartphones as unsafe, as a matter of principle. Only if the smartphone is under strong control of a company, ReadID is allowed to work client-only. The Dutch police, for example, has taken this approach.

An optimal KYC process

Reading the chip digitally allows to verify the validity of the identity document and read the customer information without the risk of any OCR or typing mistake – an important first step and sufficient for many processes. In a KYC process more is needed. We need to verify that the person owning the passport is currently holding the passport (holder verification). This implies that as a second step face matching is needed.

We work with partners such as the UK-based company iProov that do both facial matching – linked the holder to the image in the chip – as well as liveness detection. Quite a difficult process: the software should be strict enough to have almost no false positives (accepted persons, for example look-a-likes or masks), but liberal enough to deal with beards, aging, and different lighting conditions.

The combination of ReadID and iProov has shown to be successful in many mobile onboarding cases. Large banks such as ING, Rabobank, and DNB Norway use our solution. The UK home office has incorporated our technology in their app for the EU Settlement scheme, allowing EU nationals that, as a consequence of Brexit, need a residence status to apply for this online. More than 2.5 million EU nationals already successfully went through this process.

These use cases show that the trust dilemma can be overcome. NFC-based identity document verification creates a smooth customer experience, combined with the necessary level of trustworthiness at affordable cost. NFC first is the way forward in KYC processes.

About ReadID: ReadID is the leading NFC based mobile identity verification provider. ReadID originated from research at the Dutch fintech company InnoValor and is now a solution for mobile identity verification using NFC and smartphones that is adopted quickly in different sectors and application areas where fraud prevention is key, such as banking, border control, and digital signing.

www.readid.com

Verimi

Regulated Identity Platforms as the Key Enabler for the Digital Economy

About Maximilian Riege: Maximilian Riege is Chief Representative & General Counsel at Verimi. As a German and US lawyer and manager in the fintech, identification, and information technology sectors, he has worked for and advised leading digital identity and payment providers, banks, and regulatory authorities. He is admitted to practice law in Germany and New York.

Maximilian Riege ▪ *Chief Representative & General Counsel* ▪ Verimi

A digitalised world requires digital identities. This is especially true for regulated sectors such as payment and banking but also education, health, mobility, telecommunications, and certainly e-government. While there is an abundance of (fake) identities on the internet and on social platforms, regulated use-cases rely on **verified identities**. Thus, providing verified digital identities has become one of the biggest challenges in order to unlock the full potential of digital economy. At the same time, we need to provide for convenient digital identification procedures that are attractive to the user while safeguarding the user's privacy. The implementation of the General Data Protection Regulation (GDPR) in May 2018 and massive data scandals such as the **Facebook-Cambridge Analytica scandal**, **data breaches at Marriott hotels**, and the **German Federal Parliament (Bundestag)** have raised awareness and highlight the importance of secure data processing.

The issue with one-time single purpose identification

Digital identification procedures often face the same challenge as other services: the safer they are, the less convenient they are. While video identification is already a big progress that can make face-to-face identification in a bank or post office obsolete, it still takes up to ten minutes until the identification procedure is completed – a time span that is quite long for the fast-paced digital world, especially if this onerous procedure has to be repeated by the same user for every new onboarding process with another company. Furthermore, video identification is costly. Banks, payment, health-care, and telecommunication providers bear significant costs for the identification of their users, since each of these companies identifies the users individually.

Identity platforms as a solution

Identity platforms that provide for safe and compliant data storage and provide digital identities that comply with all relevant regulatory standards can be a solution. The user only needs to be identified once, stores his/her identification data set on the platform and re-uses it every time he/she needs to complete an identification procedure with another company. Ideally, this digital identity can serve all regulated and unregulated sectors by complying with the highest quality or assurance levels.

AML regulation and KYC in the financial sector

One sector with the strictest identification requirements is the financial sector. Banks and payment providers have to comply with strong AML-regulation. Within the European Union, the EU Anti-Money Directive (EU-AMLD) provides for the regulatory framework, which still requires national implementation acts.

EU-AML-Directive provides for multi-party transfer of identification data in AML context

The EU-AMLD already provides for the opportunity that obliged entities throughout the EU may 'rely on third parties to meet the customer due diligence requirements', Art. 25 EU-AMLD. This includes customer identifications conducted by other obliged entities, such as banks or payment providers from a different EU member state. Thus, if a customer wants to open another bank account with a B-Bank in one EU member state, he/she can ask B-Bank to reach out to another bank (A-Bank) in another EU member state, where the customer had previously opened a bank account, to request the identification details obtained during the previous identification at A-Bank. →

verimi

Certainly, a big improvement, which reduces onerous identification procedures but also provides for high quality identifications that comply with applicable AML-regulations.

EU eIDAS regulation harmonises eID for public sector

Also, in the public sector, the EU Commission has identified the need for standardised electronic identification. Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market, the eIDAS regulation, came into effect on 1 July 2016. The regulation aims to **'provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens, and public authorities'** within the EU. The eIDAS regulation has a direct impact on eID in the public sector, since it **'ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services'** in other EU member states where eID is available.

Call for EU-wide cross-sectoral harmonisation of KYC and CDD requirements

Following this legislative initiative, the EU-Commission explored how **'how electronic identification under eIDAS could be leveraged by the banking sector to comply with Know-Your-Customers (KYC) requirements under the fourth Anti-Money Laundering Directive (4th AMLD); and to guarantee strong authentication requirements of parties in the context of the revised Payment Services Directive (PSD2)'**. Understandably, the EU-Commission considers eIDAS as its starting point. Another option would be to make AML-compliant identities from EU regulated banks the standard. For example, in Sweden, **Bank ID is already the leading electronic identification system**.

Regardless which identity becomes the new standard, wouldn't it be great if EU citizens who want to start their Erasmus studies, work, or retire in another EU member state could use their digital identity for registering the new domicile online? And later on, they could also use this identity for signing up online for a mobile phone contract with a local telecommunication provider, opening a bank account with a local bank, and for signing up a new health insurance even before starting their move.

Identity platforms for secure and easy onboarding and user-centric data management

Regulated identity platforms that provide for secure storage of all different kinds of identification attributes and different identification levels can play an important role in harmonising identification requirements within the EU. Therefore, identity platforms that provide high quality digital identities can be the key enabler to unlock the potential of digital economy while at the same time safeguarding the user's privacy.

The European identity platform Verimi simplifies identity verification: the Berlin-based startup enables users to easily prove their identity within onboarding processes. Instead of confronting users in each industry with different legitimation processes, Verimi offers them the opportunity to store their identity data once in their Verimi account in order to reuse this data to identify themselves quickly for multiple use cases. The next onboarding procedure can be completed with one click, a smooth solution for the user which increases the conversion rate, saves costs and time for both users and companies.

About Verimi: Verimi is the European cross industry identity platform. Verimi combines all functions surrounding the digital identity: secure login, identity verification, digital signatures, and payment services. Verimi offers the highest data protection standards and the self-determination of users regarding the use of their personal data. The identity platform is supported by a large network of international corporations.

www.verimi.de/en

Identity Woman

Interview with Kaliya Young, leader in the field of Self-Sovereign Identity or Decentralised Identity, on the potential of Self-Sovereign Identity to reduce the growing regulatory burden

About Kaliya Young: Kaliya **'Identity Woman'** Young holds a Master of Science in Identity Management and Security from UT Austin. She co-founded the Internet Identity Workshop in 2005. She was elected as a founding management council member of National Strategy for Trusted Identities in Cyberspace (NSTIC) Identity Ecosystem Steering Committee. In 2012 she was named a Young Global Leader by the World Economic Forum (WEF). She consults with governments, companies, and startups about Personal Data and Self-Sovereign Identity.

Kaliya Young ▪ *Expert, Leader in the field of Self-Sovereign Identity or Decentralised Identity* ▪ Identity Woman

What are the regulatory burdens banks need to carry these days?

Banks have a whole slue of regulatory requirements all centred around figuring out who their customers are – Know Your Customer (KYC), Anti-Money Laundering (AML), Anti-Terrorism Financing (ATF). The Financial Action Task Force (FATF) mandates compliance globally and the cost to do all the checks needed are quite high.

> *“Self-Sovereign Identity technology is created by some existing technologies coming together in a new way to enable low-cost federation.*

Much of it involves looking at paper documents and trying to figure out if they are real/genuine or not. Even if one is based within a context, where something like eIDAS is applied, most of those schemes are oriented to government interoperability and there are over 200 different schemes in Europe – so they aren't actually interoperable and for the most part they were not designed for private sector use.

How can Self-Sovereign Identity technology tackle these challenges?

Self-Sovereign Identity technology is created by some existing technologies coming together in a new way to enable infinitely scalable low-cost federation. These technologies include smartphones, public key infrastructure (PKI), distributed ledgers (blockchains), personal cloud computing, and they are based on two open standards developed by the World Wide Web Consortium (W3C) – an international community where Member organisations, a full-time staff, and the public work together to develop Web standards.

These standards are called Decentralised Identifiers (DIDs) and Verifiable Credentials. Together they support individuals by being able to get credentials from an issuer, like a government, and present them to a verifier, like a bank, all without technical federation. This means that the bank does not have to 'connect' to the government to figure out if the credential is valid or not. The bank simply looks up the Decentralised Identifier of the issuing party to find in its associated DID document the public keys associated with the private keys used to sign the document, and uses this to confirm the digital document's validity. ➔

identity Woman

As the future of self-sovereign identity solutions depends on the appetite and adoption of users, from your experience, do individuals want (or even have the capacity) to manage their personal data themselves?

These technologies are new but are actually rooted in very well-understood paradigms of exchange. The digital versions of credentials act ‘the same’ as paper and plastic documents individuals carry in their wallet. When individuals present paper documents, they don’t ‘phone home’ to the issuers. The paradigms for the user-experience are still being innovated by companies working on the new technologies and the ones I have seen map well to the metaphors of a physical wallet.

There is a lot of work being done to refine the user-experience for decentralised identity basics like exchanging credentials. I do think that, with more advanced capacities to share and revoke data, new user-experience paradigms will be needed. Some people are also talking about how one can have personal artificial intelligence agents that work on an individual’s behalf so that the person themselves isn’t doing ‘all the management’.

Last fall I met with a startup, Spaceman ID, that has created a cloud based agent/wallet for individuals that they can control via SMS so this makes the technology accessible to people on feature phones.

A lack of regulatory certainty creates market uncertainty and a barrier for the adoption of self-sovereign identity, particularly for highly regulated industries such as financial services. Could this be an impediment when it comes to market adoption?

A lot of work is being done by some really great folks to educate governments about the potential of these technologies in Europe. The Identity Working Group of the German Blockchain Association published a position **paper** on how self-sovereign identity can enable identity. The European Union Blockchain Observatory and Forum has published **Blockchain and Digital Identity**. There are efforts put in to work with European governments to align the emerging Self-Sovereign identity with the existing eIDAS technologies. A **European Self-Sovereign Identity Framework** has been put forward and looks very promising.

In the North American context several Canadian provinces, **British Columbia**, **Ontario**, and **Alberta** are all actively working on developing the technology. The **Canadian national government** recently put out a call for proposals to support innovation in the space. This follows on the US Government Department of Homeland Security Silicon Valley Innovation Program solicitation for preventing forgery, **counterfeiting of certificates and licenses**. There is also the **Known Traveler Digital Identity** program that is a large and growing public private partnership.

How will identity look like in 5 years’ time?

I believe that in 5 years’ time adoption of wallets for decentralised digital identity will be widespread. Many startups and established companies like Workday are working on developing the tools for enterprises to issue and accept verifiable credentials. I know many different educational networks are exploring how these new standards can serve their members and it will become THE WAY for all educational credentials to be issued and shared digitally. I am really optimistic about the next five years.

Fighting Financial Crime with Regtech

Fighting Money Laundering – No More Oxygen to Organised Crime

'Money laundering is a very sophisticated crime and we must be equally sophisticated', **Janet Reno, while serving as Attorney General of the United States from 1993 to 2001**

Financial institutions have been investing large resources to build robust and comprehensive Know Your Customer (KYC) programmes that comply with regulators and Anti-Money Laundering (AML) laws. These procedures enable banks to better understand their customers, their financial dealings, and the risk associated with them.

What is currently happening

We often hear about drug dealers who convert dirty cash into clean dollar bills, or terrorist groups who launder money to finance their operations. As a result, **USD 1.45 trillion of the global turnover is lost to financial crime**, with bribery, corruption, and money laundering being top 'revenue makers'.

In October 2019, three European Supervisory Authorities (ESAs) published a second joint opinion on the money laundering (ML) and terrorist financing (TF) risks impacting the European Union's (EU) financial industry. The ESAs found that *transaction monitoring and reporting suspicious transactions, plus limited information flows between law enforcement, firms and CAs (competent authorities) are still a cause for concern, particularly for companies processing high volume transactions*.

Additional to these concerns, we will present some of the factors that have brought anti-money laundering (AML) to the forefront, especially in Europe.

The risks posed by virtual currencies – Virtual currencies (VCs) and cryptocurrencies have been the subject of significant media attention over the last decade. VCs are not typically regulated financial products under EU law and therefore customers are exposed to similar risks to those associated with other unregulated products and services. In the absence of a sound legal framework, the EBA recommends that national supervisory authorities should discourage customers and companies from holding VCs and carrying out activities related to them.

As businesses and authorities lack knowledge and understanding around the topic of virtual currencies, which prevents them from carrying out a proper impact assessment, VCs give rise to money-laundering and terrorist financing (ML/TF) risks. Furthermore, because of increased processing of transactions online, with only limited customer identification and verification checks being carried out, the use of these types of currencies should not be neglected by financial institutions.

UK withdrawal from Europe – **According to the Joint Opinion of the European Supervisory Authorities, UK's withdrawal from Europe might bear some ML/TF risks such as**:

- *Firms authorised in the UK and providing services to the rest of the EU might look to obtain authorisation and establish themselves in another Member State after the withdrawal of the UK from the EU. This could put a strain on CAs from that Member State, which will have to make enough resources available to assess the ML/TF risks associated with the business models, ownership, and control structures of a potentially large number of applicant firms;*
- *There is a risk that some of the UK firms that are looking to relocate would establish themselves in another Member State's territory in name only as 'shell' companies, which would make adequate AML/CFT supervision by the Member State's CA more difficult;*
- *Local authorities may not be adequately equipped and staffed to effectively oversee significant numbers of new businesses and AML/CFT supervision might suffer as a result;*

Fighting Money Laundering – No More Oxygen to Organised Crime

- *Firms will also have to update their AML/CFT policies and procedures to account for the UK becoming a third country for AMLD purposes. Such changes will be required particularly in relation to correspondent banking relationships, transfers of funds, third-party reliance arrangements, and customer risk assessments.*

Money laundering and terrorist financing risks arising from new technologies – Over the last decade, ongoing technological developments have opened new opportunities for fintech and regtech providers. However, the use of innovative solutions may also give rise to additional ML/TF risks. Some risk-increasing factors include:

- *The provision of unregulated financial products and services that do not fall within the scope of AML/CFT legislation;*
- *The quality of information gathered as part of the Customer Due Diligence (CDD) process, particularly the application of incomplete or ineffective CDD measures;*
- *A lack of understanding by fintech providers of their obligations under the AML/CFT legislation and the overall financial regulatory framework;*
- *Different compliance cultures between supervised entities and new fintech providers;*
- *An increased use of new technologies to onboard customers remotely, without putting in place proper safeguards, which could increase the firm's exposure to cybercrime, including identity theft;*
- *An over-reliance on outsourcing arrangements with fintech companies, without putting in place proper oversight mechanisms.*

Moreover, those CAs that have carried out a formal ML/TF risk assessment on regtech solutions used by supervised entities **highlighted the following risk-increasing factors associated with these solutions, if they are ill understood or badly applied**:

- *Firms' over-reliance on information technology solutions, which could lead to a loss of human professional expertise and judgement in monitoring processes;*
- *A lack of provisions in the current legal framework dealing with regtech solutions, which means that different standards are applied by different solutions;*
- *Firms' lack of understanding of new technologies that are used in their CDD processes, which may expose firms to ML/TF vulnerabilities;*
- *When firms are outsourcing all or part of their activities to regtech providers without proper oversight and governance arrangements in place, it may lead to:*
  - *difficulties with accessing customer data owing to regtech providers' potentially short lifespan and with establishing the ownership of that data;*
  - *questions about the reliability of records held owing to unsound and unsafe record-keeping practices put in place by the regtech provider;*
  - *a lack of transparency in the allocation of responsibilities between firms and regtech providers, particularly when the processes are outsourced to providers that are not obliged entities under the AMLD.*

Nevertheless, the European Supervisory Authorities **also highlighted how the use of these solutions can improve the effectiveness and efficiency of companies' AML/CFT controls**. For instance, *'in the case of Bitcoin, the blockchain provides a public ledger of each transaction which, in combination with good know-your-customer (KYC) procedures, may actually improve anti-money laundering checks'*, according to **Christian Chmiel**, CEO and founder of **Web Shield**.

In the last five years, there **has been an explosion of regtech startups**. **Just over USD 9.5 billion was invested in regtech companies between 2014 and 2018**, with 34.5% of this invested in companies providing KYC solutions. AML follows with 28% of the capital invested, GDPR takes third place with 13.1%. KYC and AML regulations have dominated the regtech landscape due to their cross-industry applications and heightened expectations from regulators.

Fighting Money Laundering – No More Oxygen to Organised Crime

Rising costs – Most AML activities require signifi¬cant manual effort, making them inefficient and difficult to scale. **In 2018, it cost US financial services around USD 25.3 billion** to manage money laundering risk.

Fighting money mules – At the end of 2019, European law enforcement authorities from 31 countries, **supported by Europol**, Eurojust, and the European Banking Federation (EBF), stepped up their efforts to crack down on money mule schemes. Money mules take part, often unknowingly, in money laundering activities by receiving and transferring illegally obtained money between bank accounts and/or countries. More than 650 banks, 17 bank associations, and other financial institutions helped to report 7520 fraudulent money mule transactions, preventing a total loss of EUR 12.9 million.

Recruiters of money mules are coming up with ingenious ways to lure in their candidates. Romance scams, with criminals increasingly recruiting money mules on online dating sites, grooming their victims over time to convince them to open bank accounts under the guise of sending or receiving funds, as get-rich-quick online advertisements on social media were reported on the rise, in 2019.

Criminals are using more sophisticated means to remain undetected – **According to Feedzai**, most of the fraud and financial crime prevention platforms are not properly equipped to detect this type of behaviour. Often, customer behaviour is siloed and only specific to a single channel, enabling criminals to avoid detection methods by exploiting gaps that exist between channels. Hence, it's important **to acknowledge how advanced financial crime and fraud has become, to best protect ourselves against them**. For example:

- **Lone-wolf terrorists** purchase weapons and vehicles in low-cost transactions that are difficult to detect, and fast response times are critical;
- **Cyber-enabled criminals** are globally coordinated, using sophisticated technology and insider information to target technology weak spots;
- Ecommerce, a market worth USD 2.4 trillion globally, has made it easier for criminals to pose as legitimate online merchants or payment providers.

Some regtech companies propose a more contextual approach to fight financial crime. This method is called **'contextual monitoring'** and it is based on big data techniques and advanced analytic capabilities **(machine learning and AI)** to detect high-risk anomalous behaviour. This approach identifies and connects all available data about a client and their counterparties at a given point in time. Basically, it replicates in an automated, yet fully transparent and understandable manner, the laborious research that is specific to an investigative process. The result is a process that offers greater accuracy and improved effectiveness, reducing false positives and finding potentially high-risk activity.

Need for robust anti-money laundering policies and practices

Manfred Wandelt, Senior Manage at Deloitte RegTech Lab *'who has worked many years for international banks and for more than 18 years as consultant in the environment of Anti-Financial Crime' has revealed that 'existing compliance practices are increasingly ineffective. Already back then I recognised the urgent need to adopt modern technologies as part of a compliance strategy. This is where regtech comes into play and offers every consultant an expanded field of action'*.

Compliance modernisation is no longer optional, but mandatory, due to increased number and value of the regulatory fines applied to large US and EU universal banks, high volume of regulatory changes and amendments, plus the outdated IT infrastructure and error prone processes, and threat evolution. Moreover, as financial institutions aim to build long-lasting brands, they aspire to be associated with financial success and excellent service, not drugs smuggling or wars funding.

All in all, one thing is clear — the days of box-ticking are over when it comes to compliance practises related to Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT).

Mirela Ciobanu | *Senior Editor* | The Paypers

Deloitte

Two of Deloitte's RegTech Lab top consultants, Manfred Wandelt and Anna Werner, share with The Paypers what is currently happening in the German RegTech space

About Manfred Wandelt: Manfred is Senior Manager at Deloitte and has more than 17 years of consulting experience working with national and international clients. He is member of the Anti-Financial Crime team, heading AML/CFT, and responsible for all RegTech related subjects.

Manfred Wandelt ▪ *Senior Manager* ▪ Deloitte

About Anna Werner: Anna works as Consultant at Deloitte and is one of the initiators of the Lab. Through utilisation of RegTech solutions, she tackles compliance pain-points by combining regulatory and technological expertise and is also responsible for vendor and client relationships.

Anna Werner ▪ *Consultant* ▪ Deloitte

When it comes to onboarding new customers (on a B2B level), what is on the top of the agenda for compliance leaders? Is it the weight of the regulation itself, the ability to respond, other?

Increasing regulatory complexity, challenging market environments, and disruption caused by the emergence of new technologies – all these aspects mean that even established market participants must confront major operational and strategic challenges, including when it comes to new customer onboarding.

> *“Analysts predict an increase in client demand for innovative RegTech solutions, with a market potential of USD 76.3 bln in Europe in 2022. This trend is consistent with the current situation in Germany.*

Extracting relevant information from paper-based or incompletely digitised sources can be inaccurate and time consuming. Not only are the manual tasks involved tedious, they also unnecessarily complicate the process of organising data into usable (and therefore valuable) resources. Lack of time and the presence of non-standardised or duplicated data sets, coupled with siloed and opaque compliance functions cause many institutions to struggle with inefficiencies in the onboarding process. In such an environment, compliance leaders increasingly focus on the use of Artificial Intelligence- (AI) and Text Mining-based solutions to aggregate enterprise-wide data. Advanced analytic techniques may then be applied to the aggregated data, for the purpose of enhancing decision-making. Additionally, hiring and retaining top talent with the skillsets required to thrive in the new market environment is one of the top issues compliance at the moment.

While the regulatory environment is undergoing such rapid change, those affected can feel pressure to find a ‘quick-fix’ solution for challenges affecting their onboarding processes. This approach does not always produce a satisfactory result, and previous cases have shown how failure to adequately address regulatory requirements can result in high fines. A better approach is to work proactively, increasing efficiencies by harnessing the latest technology to automate routine processes, enabling skilled staff to focus on value-add activities. Compliance leaders' ultimate goal is to adopt smarter approaches to ensure efficient compliance with overlapping regulations. →

Deloitte.

What is KYC?

The term 'Know Your Customer' (KYC) can apply to a variety of business activities, including marketing and sales. In the financial and regulatory sector, the term is mainly applied to customer due diligence and compliance activities. The KYC process is, in simple terms, checking the identity of your customer before doing business with them (i.e. 'onboarding' the customer). Specific KYC activities vary from company to company, but usually encompass ID verification, Ultimate Beneficial Owner (UBO) identification, Politically Exposed Person (PEP) and sanction screening, Anti-Money Laundering (AML) screening, along with various others.

Within regulated sectors, KYC is often referred to as part of AML; the processes are comparable and both take place when onboarding a new customer. Entities operating in regulated sectors are legally required to incorporate KYC in their onboarding processes, and many entities not legally required to do so choose to incorporate KYC in order to fight criminal activity. While not mandatory, it is important for all institutions, no matter what sector they operate in, to perform appropriate due diligence and compliance checks to mitigate their risk of becoming a victim of fraud. Essentially, optimisation of onboarding processes – including UBO identification, PEP identification, sanctions checks, and AML screening – have become an imperative in the world of compliance.

Could you please portray the RegTech landscape in Germany? What are the most relevant RegTech players on the German market?

Analysts predict an increase in client demand for innovative RegTech solutions, with a market potential of USD 76.3 bln and USD 10.7 bln in Europe in 2022. This trend is consistent with the current situation in Germany, where we see a great demand for RegTech solutions across sectors. This demand is not limited to financial service entities – as part of our **Deloitte RegTech Lab initiative** we also see requests from automotive, pharma, and public sector clients when it comes to tackling compliance pain points in new and innovative ways. Industrial clients are now obliged to conform to more far-reaching compliance requirements than in previous years and are therefore seeking new and innovative ways to handle overarching risks within their organisations. We are seeing German companies from a wide range of industries request agile solution implementation, as well as managed risk services.

The demand for RegTech solutions generated by market movement is further driven by regulatory pressures, and by inefficiencies in investigative techniques. Despite this, the German RegTech vendor landscape appears to be at a comparatively low maturity level. This is particularly noticeable when considering vendors from countries such as Luxembourg, the UK, or Singapore, where regulators actively contribute to the introduction of sandboxing mechanisms and experimentation with new RegTech services. Having said this, some RegTech vendor jewels offering state-of-the-art niche solutions are also headquartered in Germany. It is now up to German organisations to leverage emerging technologies in the most efficient manner possible. Further insights into the most relevant RegTech players, internationally as well as in the German market can be examined in the **RegTech Universe list** from our colleagues from Luxembourg.

What are some challenges that the RegTech adoption faces in Germany?

Over the last decade, the environment in which financial services operate has changed irreversibly. The after-effects of the global financial crisis have combined with the rise of new technologies to create a brave new world in banking and finance. Changes range from enhanced regulatory pressure, with the likes of the Fifth EU Anti-Money Laundering Directive (AML4/5/6, PSD2) and the General Data Protection Regulation (GDPR) coming into force, to market disruptions caused by emerging neobanks – and by the efforts of traditional banks to play catch up through transformation of their existing models – to the rise of cryptocurrencies powered by blockchain, and the arrival of AI and automation into everyday life.

The sheer volume and complexity of new and existing regulations have had the unintended consequence of encouraging financial service providers in Germany to focus on compliance rather than innovation. The potential of RegTech is far greater than the sum of its current available solutions. Indeed, it has the potential to enable a proportionate and close to real-time regulatory regime that identifies and addresses risk while also facilitating more efficient regulatory compliance. ➔

Many German business models and services are currently undergoing testing and are therefore subject to strategic realignments. In this area of conflict between regulatory, economic, and technological developments there is an increased pressure to improve efficiency, but a corresponding shortage of skills and data available to entities involved, affecting both companies and supervisory authorities.

The German supervisory authority (BaFin), which follows a rather strict and controlled regulatory approach to minimise risks that emerge through new business models, states *'[Financial institutions] must continuously monitor developments in RegTech, as proper functioning requires a comprehensive understanding of solutions that are relevant in practice'*. In addition to the many possible advantages of new technological solutions, a supervisory authority must also consider associated potential risks. RegTech applications can harbour a variety of risks due to technical and procedural designs, which would have to be analysed and evaluated on a case-by-case basis. Regardless of which innovative solutions achieve market prevalence, the use of RegTech applications must not lead to inappropriate risks. In any case, BaFin is closely monitoring developments – thus, RegTech adoption in Germany is progressing, but in a very restricted way.

Are German organisations familiar with the concept of a RegTech vendor? How do they know what to outsource and what selection criteria to apply?

At the RegTech Lab, we often find that companies don't have a clear understanding of the technologies that can be harnessed to effectively mitigate compliance risks and increase overall regulatory efficiency. Discussion of possible solutions often leads to a long trip along the road of digital opportunities and can end with unrealistic concepts. We also see that, while financial services institutions are interested in digital solutions, they can forget that these solutions require implementation in their own internal processes – hence, the involvement of the IT function from the sandboxing process's kick-off is missing.

Essentially, even though procedural knowledge is missing, RegTech is a buzzword for various German organisations and there is great willingness to find out more about the technologies that can be put in place to tackle specific compliance pain-points. Previous RegTech experience has revealed that many of our clients tend to implement vast, traditional software packages as their 'tailored RegTech solution'. Inevitably, the client's expectations are not met – either due to unmanageable quantities of false positives, inappropriate parametrisation, or inefficient application. Often, relatively few modules of the software are in fact necessary; the client must still pay (high fees) for the entire package. To refine these existing standard applications or to experiment with new technologies, companies are advised to select their vendors through a pain-point driven methodology, backed by regulatory as well as technical expertise from involved internal Compliance and IT functions.

Narrowing down the issues RegTech is trying to respond to, how important would you say that fighting financial crime is for the German economy?

Recent cases of alleged breaches of AML rules demonstrate the severe consequences of failure to comply with AML requirements. Failure can pose significant risks to entities, up to and including threat to their viability as a going concern.

EU Commissioner Jourová stated on 25 June 2019:
'We have a problem in Europe. Europol estimates that around 1% of Europe's wealth is involved in suspect financial activity. That's the equivalent of the annual EU budget.'

Decision makers in Germany are currently making great efforts to enable sufficiently effective mechanisms in avoidance of money laundering risks. At the end of October 2019, the Federal Ministry of Finance published the first national risk analysis on money laundering and terrorist financing; the real estate sector and financial transfer transactions with high cash intensity were identified as the areas with greatest risk.

Launderers are continuously looking for new routes for laundering their funds. Differences between national AML systems are exploited by those who tend to move their networks to countries and financial systems with weak or ineffective countermeasures. →

Deloitte.

If left unchecked, money laundering can erode a nation's economy by changing the demand for cash, making interest and exchange rates more volatile, and by causing high inflation in countries where criminal elements are doing business. The draining of huge amounts of money a year from normal economic growth poses a real danger for the financial health of every country involved, which in turn adversely affects the global market. Most fundamentally, money laundering is inextricably linked to the underlying criminal activity that generated it.

Safeguarding the financial system against criminals is of utmost importance to financial stability and system integrity, not only in Germany but also internationally. As a response to such developments the Financial Action Task Force (FATF), for instance, holds roundtables on FinTech and RegTech issues to ensure that AML/Counter Terrorism Financing (CTF) related measures remain up-to-date as new risks and vulnerabilities emerge, for example as a result of new payment products and services. Multiple stakeholders are present and the discussion includes the practical impact on AML/CTF standards on financial innovations and different approaches, with the goal always being to support innovative business models and technologies while mitigating related risks.

What's on the regulatory horizon for 2020, where should organisations, RegTech vendors, and the general public be focusing their efforts and how can RegTech help?

Over the coming years, we expect to see further reconciliation of legislative inconsistencies across regulatory frameworks, as well as across EU member states. Brexit-related uncertainty still hangs over the horizon, but firms in the financial sector also need to remain receptive to a wide range of developing areas – from sustainable finance, fintech, LIBOR reform, and operational resilience, to significant changes to regulatory capital and remuneration requirements.

As some of the key regulatory changes of recent years (such as MiFID II and MAR) are becoming 'business as usual', regulators are clarifying their expectations and turning the focus of their supervisory (and likely enforcement) activities to compliance. Amendments to key sections of financial services legislation are also on the cards for 2020, and are likely to have a far-reaching impact. Another area to watch over will be strengthening protection for whistle-blowers working in financial services. Significant developments have already occurred at the end of 2019, when the EU Whistleblowing Directive came into force.

Above all, AML and AFC continue to be key points of focus for regulators in the EU and globally in development of new policies, peer reviews, liaisons with other countries, and the collection, analysis and dissemination of information, as well as investigation requests to national regulators and prohibitions for individual firms. Last but not least we will see without exception banks, financial services providers, retailers, online marketplaces, and payment service providers gearing up their strategies and RegTech investments to ensure that SCA (Strong Customer Authentication PSD2) is in place.

About Deloitte: Deloitte provides audit, risk advisory, tax, financial advisory, and consulting services to public and private clients spanning multiple industries; legal advisory services in Germany are provided by Deloitte Legal. To find out more about latest RegTech trends and technologies send a mail to **RegTechLab@deloitte.de** and be inspired by hands-on sandboxing sessions in our hub for regulatory and technical know-how.

www2.deloitte.com/de/de/pages/risk/solutions/regtech-lab.html

Wołoszański & Partners Law Firm

Customer Data Protection and the Impact on Digital Money and Crypto: the 5th AML Directive

About Marta Solarska: Marta Solarska specialises in new technology law. In particular, she focuses on personal data protection law and she is appointed as Data Protection Officer at Hyundai Motor Poland. She manages numerous legal projects on a daily basis, with special regard to IT contracts and competition law issues.

Marta Solarska ▪ *Data Protection Officer* ▪ WLAW

About Kamil Kaleńczuk: Kamil Kaleńczuk is a lawyer from Wołoszański & Partners Law Firm specialising in providing services to entrepreneurs. Experienced in managing multi-threaded legal projects, he routinely works with clients in the field of new technology and regtech law, corporate governance, as well as labour law.

Kamil Kaleńczuk ▪ *Lawyer* ▪ WLAW

Changes in EU anti-money laundering legislation have been passed at break-neck speed. As demonstrated by the example of recent years, at a time when some Member States have not yet implemented 4th AML Directive, the 5th Anti-Money Laundering Directive (AMLD5) has already amended the previous one. Member States have brought into force the laws necessary to comply with this Directive on 10 January 2020. Therefore, an obvious question is whether such frequently occurring changes are in fact necessary?

New obliged entities and…

First of all, the scope of the so-called obliged entities has been extended in accordance with the financial market requirements and includes providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers. Actors engaged in the cryptocurrency business have finally been integrated into the European financial system as full-fledged members. The anonymity of virtual currencies allows their potential misuse for criminal purposes and enormously increases the risk of money laundering. Lawmakers have stopped pretending that alternative payment methods (beyond fiat money system) do not exist. As a curiosity, it is also worth mentioning the other new category of obliged entities, namely persons trading or acting as intermediaries in the trade of works of art, like art galleries and auction houses (transactions over EUR 10,000) have been added. Quite a specific business area, in which many people intend to remain anonymous, might be a challenge even though it opens numerous business opportunities for KYC service providers!

…virtual currency meaning…

Although that seems to be obvious to all those who deal with them professionally, it is worth noting that the definition is finally introduced by the AMLD5. So, what are virtual currencies?

1. digital representation of value that is not issued or guaranteed by a central bank or a public authority;
2. not necessarily attached to a legally established currency;
3. does not possess a legal status of currency or money;
4. accepted by natural or legal persons as a means of exchange and which can be transferred, stored, and traded electronically.

Yet another useful supplementary definition is 'custodian wallet provider' – an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store, and transfer virtual currencies. Bearing in mind the need of implementation of the Directive in each Member State, the introduced definitions may vary insignificantly from country to country. ➔

…and more onboarding requirements!

Furthermore, under the AMLD5 customer due diligence measures are adapted to technological developments. Identifying the customer and verifying the customer's identity requirements has significantly evolved and will be supported by possibility of use: ***electronic identification means, relevant trust services*** *as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities.* The real impact on the client onboarding process will also have the change in identifying the beneficial owner process, since with respect to the senior managing official: *obliged entities shall take the necessary reasonable measures to verify the identity of the natural person who holds the position* ***of senior managing official and shall keep records of the actions taken as well as any difficulties encountered during the verification process***.

As if that wasn't enough, there's still GDPR

Although it has been over a year and a half since GDPR came into force, its impact on the market continues to grow. First of all, the AMLD5 has finally clarified a retention issue – data collected for AML purposes may now be stored for 5 years exactly (as before an obligation to store for at least 5 years could have caused some interpretational doubts) plus possible extension under special circumstances introduced by domestic law. Therefore, the retention policies definitely should be reviewed!

Other updates, unfortunately, did not change the vague character of the rules of data processing in AML context, to mention, among others regarding information obligation towards entities whose data has been collected in AML procedure, the specific character of entrustment of data to providers of underwriting solutions or profiling.

Expectations vs. reality

Extension of the scope of obliged entities is primarily related to the need to implement comprehensive AML procedures for crypto exchange and wallet service providers. To realise how challenging it is, we should remember that the largest crypto exchanges have a daily turnover over a billion (!) dollars and thousands of active clients. Virtual currencies will cease to be a convenient tool for criminals and terrorists, and the industry itself will get rid of the 'patch' of suspicion that its economists and public institutions have attached to it. On the other hand, the introduction of official 'virtual money' and 'custodian wallet provider' definitions is not a breakthrough, however clarifies the matter and shall be noticed. Increased demand for advisory services in the scope of creating and implementing procedures for these entities will be noticeable at the turn of 2020. Moreover, the context of GDPR policies in view of both new and already existing demands under AML is not yet an exhausted subject for obliged entities. It is still visible, that as long as AML procedures are quite well understood by the market, their collision with GDPR side of the coin is still a challenge.

Nevertheless, in the upcoming months inclusion of the custodian wallet providers within the national deposit insurance schemes should be discussed together with a project for a systemic regulation of the virtual currency industry, in all areas of its appliance. Whether the market finally gets an effective and clear legislation in all Member States, only time will tell. Notwithstanding which AML Directive is force, the motto is still the same – 'Follow the money'.

About WLAW: Wołoszański & Partners Law Firm specialises in rendering legal advisory services for entrepreneurs. Our Law Firm offers comprehensive legal services. In particular Wołoszański & Part specialise in commercial law and companies law, civil law, and legal aid in respect of new technologies law.

www.wlaw.pl/en/

Web Shield

How to Manage Crypto Merchant Risks

About Christian Chmiel: Christian A. Chmiel, the CEO and founder of Web Shield, is responsible for the development and implementation of investigation techniques to identify fraudulent or brand damaging online merchants. He is also a lecturer at the Web Shield Academy and published several books in the fields of fraud, investigations, and accounting.

Christian Chmiel ▪ *CEO and founder* ▪ Web Shield

Bitcoin may have fallen from its December 2017 high of USD 20,000, but cryptocurrencies are still doing brisk business. In the first six months of 2019, more than USD 2.5 billion had been raised from about 150 new tokens, according to the tracking website CoinSchedule. Christian Chmiel, CEO of Web Shield, explains how acquirers and payment service providers (PSPs) manage the risks of the crypto space to grow and prosper.

A cryptocurrency is a decentralised digital currency that utilises cryptography for security and usually a blockchain as a ledger to record transactions. Cryptocurrencies challenge fundamental assumptions about money. They neither require banks to create money, nor serve as trusted intermediaries in financial transactions.

The principal actors involved in the sale or purchase of crypto-assets are no different to those in a standard four-party card transaction. The consumer purchases a product or service from a crypto exchange merchant. These parties are supported by an issuer and acquirer respectively, who must comply with applicable laws and card scheme regulations.

New money

Crypto-assets represent the traditional functions of money – a medium of exchange, unit of account, and store of value – digitally. They work across national borders via direct asset transfer. No clearing, settlement, intermediaries, and central infrastructure makes the market more efficient by stripping out cost.

'Virtual currency has the potential to improve payment efficiency and reduce transaction costs for payments and funds transfers', said a **2015 FATF report**. The European Parliament agrees. 'Transactions in virtual currencies can be cheaper, faster, more secure and more transparent', it said in **2016**.

Crypto-assets are a classic case where opportunities and risks are intertwined. The irrevocability of transactions could increase risk and fraud. Criminals also value the relative untraceability of such assets to monetise crimes, launder money, and finance terrorism. Crypto-assets may be used for illicit activity, yet in comparison to cash transactions the overall impact is still low: less than one percent of Bitcoin transactions has been spent on the dark web in 2019, according to a **Bloomberg article**.

In the case of Bitcoin, the blockchain provides a public ledger of each transaction which, in combination with good know-your-customer (KYC) procedures, may actually improve anti-money laundering checks.

Managing onboarding risks

Good background research is key to the successful onboarding of crypto-asset merchants. Acquirers and PSPs are advised to research the specific merchant or exchange. Have there been warnings around hacked accounts, stolen wallets or previous initial coin offerings (ICOs)? How did they fail? Were they considered scams?

Merchant activities before the crypto-asset launch can also be a strong risk indicator. Is this their first crypto venture? Are the people behind the business known for fraudulent schemes in other areas, like binary options? →

Examining a merchant's website and online footprint is critical as much of the publicity for purely digital businesses is generated via online forums and social media.

Aside from doing their own KYB on prospective merchants, acquirers and PSPs must validate that end-customer KYC procedures are adequate. Customer identification and verification can be done at the time of sign-up or first deposit, depending on applicable law (e.g. by implementing an ID/video verification process).

Identity verification is usually only required when fiat money is transferred into digital currencies. Thereafter, the use of cryptocurrencies is anonymous (or technically speaking, pseudonymous) for the parties involved, as the buyer and seller are not connected directly during the transaction.

Breaking down card scheme requirements

Mastercard added cryptocurrency merchants to its **BRAM programme** and since 12 October 2018 has required registration of both new and existing cryptocurrency merchants. As part of the registration process, acquirers must provide:

- **Evidence of legal authority** – including copies of the merchant's licence and registration to operate in each country where their cryptocurrency activity will occur or be offered to cardholders.
- **Legal opinion** – including reasoned legal opinion from a reputable law firm about the merchant's business and activities.
- **Effective controls** – including certifications that the merchant's systems are designed to remain within legal limits.
- **Notification of changes** – including the ability to notify Mastercard within 10 days of any changes to the information previously provided around applicable law, merchant activities, and systems.
- **Acceptance of responsibilities** – affirmation that the acquirer will not submit restricted transactions for authorisation.

It can be difficult for acquirers and PSPs to fulfil these and other requirements effectively. This is partly because there is no consistent global approach to crypto-assets or ICOs yet. Some jurisdictions impose an outright ban. Others bar their citizens from engaging in crypto activities locally but permit it outside their borders. Others place restrictions on financial institutions from facilitating crypto transactions. Acquirers and PSPs must monitor any regulatory changes regarding crypto-assets, but also monitor their merchants – this is no different to any other merchant.

The complex regulatory requirements can make onboarding and monitoring crypto merchants a daunting task. Fortunately, service providers can assist here. Web Shield's own **Regulatory Monitoring** solution, for example, is operated in connection with partner law firms from around the world to lessen the burden on acquirer's and PSPs.

About Web Shield: Web Shield equips the payments industry with tools that protect businesses from merchants involved in illegal or non-compliant activities. Their highly precise solutions provide acquirers, PSPs, and other financial organisations with the information they need to make valuable decisions about prospective clients, and alert them when existing clients behave dubiously. With Web Shield, you keep your business out of risky situations, saving time and money.

www.webshield.com

The KYC Utility

SWIFT

Marie-Charlotte Henseval, Head of KYC Compliance Services at SWIFT, talks about the cooperative's mission to provide solutions that simplify the KYC process for all participants involved

About Marie-Charlotte Henseval: After five years as Product Manager of the SWIFT KYC Registry, Marie-Charlotte is now globally responsible for KYC Compliance Services. From 2010 to 2013, Marie-Charlotte was Market Manager for Corporates on SWIFT, contributing to the development of the SWIFT for Corporates offering. She joined SWIFT in 2008 in the Operations department after graduating as a Civil Engineer, and holds a Masters in Management Sciences.

Marie-Charlotte Henseval ▪ *Head of KYC Compliance Services* ▪ SWIFT

What KYC challenges do banks and corporates face?

Historically, KYC has been a cumbersome process – slow and repetitive for both financial institutions and corporates. Despite technological advances, it's not gotten easier. KYC continues to be one of the biggest challenges in the compliance space, both for financial institutions and corporates. Over **90% of treasurers** report that responding to KYC requests is more challenging today than it was five years ago. In addition, **over 50%** of them reduced the number of banks they work with to avoid lengthy KYC processes, negatively impacting banking relationships.

> *“By simply sharing information in a standardised format, corporates and banks can save vast amounts of time and resource.*

Corporate groups work with multiple banking partners across the globe, many of which are in different regulatory jurisdictions. This means that corporate treasurers have to provide KYC data in multiple formats, often through bilateral exchanges, in order to meet the regulatory requirements of each partner, which is costly, time-consuming, and inefficient.

Meanwhile, banking partners have to reach out to their corporate customers for information or search for data across multiple sources only to find it is often incomplete or out of date. In many cases, they have to repeatedly follow up with existing customers as part of regular KYC reviews, which can strain relationships.

You mentioned in an interview for **Global Trade Review from September, 2019** that SWIFT's ambition is to create a 'one-stop-shop for banks to access information about all their clients'. Could you tell us more?

The key to effective KYC is information sharing. Data can be unstructured and non-standardised, meaning multiple different versions of the same information have to be repeatedly submitted to counterparties. By simply sharing information in a standardised format, corporates and banks can save vast amounts of time and resource.

This is why we created **SWIFT's KYC Registry**. It aggregates KYC information in a globally recognised, standardised format, providing banks with a centralised database with everything they need.

The registry, set up in late 2014, is currently used by more than 5,500 financial institutions, representing more than 80% of the traffic that flows over SWIFT's network. The standard defined for correspondent banking includes the latest Correspondent Banking Due Diligence Questionnaire (CBDDQ) from the Wolfsberg Group and covers up to 90% of the information that global banks typically require for due diligence, making it one of the most comprehensive KYC tools on the market. ➔

The SWIFT KYC registry opened to corporates at the end of 2019, following a successful testing period with 18 leading corporate groups, including BMW, Spotify, and Unilever, along with 16 global banks representing over 7,000 corporate-to-bank relationships on SWIFT. The registry provides corporates with the opportunity to upload their information in a standardised way so that all their banks can access the information required. Initially the solution was opened to corporates that are already using the SWIFT network. We aim to extend it beyond SWIFT-connected corporates over time to bring the benefits of the registry to all banks and corporates.

What are the benefits for entities (banks/corporates) joining the KYC Registry?

Corporate groups benefit from the ability to structure their KYC data in a standardised format, agreed by banks and corporates across the globe, and have their data checked by SWIFT for completeness. Through the registry, corporates and banks will have access to the Wolfsberg Group's CBDDQ. This enables them to implement an enhanced and reasonable standard for cross-border and/or other higher risk correspondent banking due diligence, reducing any additional data requirements.

They will also be able to comply with data privacy rules by remaining in control of their data, deciding which banks have access and having the ability to update their records in real-time.

For banks, the registry offers a single source to collect standardised and up-to-date KYC information about their correspondents, be it banks or corporates. It eliminates the burden of having to deal with multiple sources, contending with outdated data and repetitively reaching out to correspondents.

In 2019, a number of competitors have withdrawn from the KYC space, raising questions around the viability of the utility model. How confident are you in the utility model?

If you look at the landscape today, it's fair to say that SWIFT's is the only truly global central KYC utility that remains in the market. One of the reasons for this is that cracking and solving the KYC problem is not easy and takes time to address – even if you come up with a great solution, it still takes time for banks or corporate to change policy, to feel comfortable with the technology, and to look at embedding it into their business processes.

One of the differentiators for us is related to our setup as a cooperative. We are not a commercial venture looking at some point for a very specific return. We are there to bring the global financial community together to everyone's benefit.

What is in store for SWIFT's registry for the next 5 years?

Through our working group and engagement group, we are currently engaging with over 100 corporates and banks to open the SWIFT KYC Registry to corporates globally. The aim is to eradicate most of the lengthy bilateral exchanges that exist today.

Collaborating with banks and corporates has provided detailed insights into the current barriers to effective KYC due diligence and, through our global platform, we will continue this work to provide solutions that simplify the KYC process for all participants involved.

About SWIFT: SWIFT is a global member owned cooperative and the world's leading provider of secure financial messaging services. We provide our community with a platform for messaging and standards for communicating, and we offer products and services to facilitate access and integration, identification, analysis, and regulatory compliance. Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures, and corporate customers in more than 200 countries and territories.

www.swift.com

Afreximbank

Afreximbank's MANSA Repository Platform, Lowering Risk Perception of African Entities

About Maureen MBA: Maureen MBA is the immediate past Director of Compliance & Governance Department of Afreximbank, with over 25 years of experience working with the Bank. Maureen spearheaded the establishment of the Compliance Unit in 2007 and nurtured the Unit to a full-fledged department before she disengaged to head the MANSA Business.

Maureen MBA ▪ *Head, MANSA Business* ▪ Afreximbank

Afreximbank's MANSA Repository Platform (MANSA) is an initiative developed to address and lower the risk perception of African entities, reduce cost of compliance, and potentially reduce the cost of trade finance in Africa. These goals will help support increasing the access to funding as well as creating confidence among global financial institutions, investors, and partners in their relationships with African counterparties, serving as an incentive for them to deepen relationships in the African trade finance space. MANSA is a centralised digital platform that provides a single source of primary data required to perform customer due diligence checks on counterparties in Africa. African corporates, including SMEs and financial institutions, contribute with information on a voluntary basis.

MANSA Repository is based on three pillars; the first is the KYC pillar, which is central and addresses all customer due diligence matters. Invest in Africa is the second, providing trade information about African countries, while the third pillar focuses more on publishing developments on the compliance space and economic news and events around Africa. The KYC/CDD pillar has three users, which include Contributor, Verifier, and Subscriber. Afreximbank has been partnering with regulatory agencies in the various sectors of Africa's economies to play the role of verifier of information contributed on the MANSA platform. In this regard, African central banks verify information contributed by financial institutions under their supervision, while the Bank has identified credit bureaux, registrars, stock-exchanges, law firms, auditors etc. to act as verifier for corporate entities and others. Information are captured with contributors uploading their information on the platform after having duly executed the contributor agreement with Afreximbank. Accordingly, there are designed standard templates for the different contributors to be executed appropriately, carefully, following the defined instructions. These information after verification and validation by the appropriate regulatory agency are then published on the Platform and accessed by subscribers.

MANSA was launched on Afreximbank's 25th anniversary during the Bank's Annual Meetings held in Abuja, Nigeria, in July 2018. The name MANSA was derived from the name of the rich Malian king, Mansa Musa (1324-1325), who at that time made a pilgrimage to Mecca and had a stop-over in Cairo during the journey. It was reported that Mansa Musa was accompanied by 80-100 camel loads of gold and a personal entourage numbering in the thousands. He was very generous, exchanging gifts of gold to all dignitaries who lent him money that enabled him returned to his home-country, Mali in 1325. Mansa Musa's extravagance brought Mali, as a country, and Africa, as a continent, to the attention of the world. MANSA Repository platform is therefore, perceived as Africa's new gold, as it is hoped that MANSA will chat a new path in history for Africa.

There is no doubt that Africa possesses a lot of potential, but the challenge remains information asymmetry. The continent is endowed with both natural resources and human capital ready to tap into. For instance, today, the extractive industries remain untapped and suffer negligence as more focus is on oil; many African countries are increasingly discovering huge crude deposits in their respective environment. This continues to heighten the risk of negligence on other sectors of Africa's economies. ➔

Most of the investors who shy away from the region do so because they claim they do not have enough and adequate information about African entities. MANSA Repository Platform is the answer to that. The information captured on the Platform is based on international best practice and it is fit for purpose.

It is believed and hoped that MANSA, when fully operationalised, will become Africa's pride.

The contribution of information to the MANSA Platform is voluntary. However, in line with the Afreximbank vision '*To be the Trade Finance Bank for Africa*', the main incentive is that the Platform will enhance Africa's trade amongst the constituent countries and with the rest of the world through the digital intervention.

MANSA Repository Platform is 'LIVE'. The Bank is presently executing the Verifier Agreement with African central banks, and the Agency Agreement with already identified regulatory agencies who have passed the Bank's due diligence assessment. One of the qualified agencies have started populating the platform on the agreed African countries. The marketing plan is being pursued and it is believed that in 2020, subscribers would have attained a significant number of about 100,000- 150,000. Together with the Central Bank of Egypt (CBE) and the Egyptian Banking Institute (EBI), Afreximbank has conducted a series of training for trainee and train the trainer of African central banks and financial institutions. Afreximbank is increasingly discussing with corporate entities to encourage more contributors to upload their information on MANSA repository platform.

Besides being a centralised CDD repository for Africa and promoting good KYC profiles for African entities, additional objectives for the platform include:

1) Reduce compliance cost

An Africa-focused CDD Repository for customer due diligence checks will reduce the risks and burdensome processes on the financial institutions and lenders to conduct due diligence on customers/counterparties, thereby reducing cost of compliance;

2) Fight money laundering and counter financing terrorism

Access to Africa CDD Repository facilitate customer due diligence checks on counterparties as well as provide independent corroboration of entities CDD/ KYC data, which significantly filters potential AML/CFT transactions and screens out sanctioned entities from using global financial system;

3) Facilitate intra-African trade

Availability of information on African counterparties as well as investment information will enhance intra-Africa trade and stimulate uptake of new trade avenues;

4) First African Investment Information Hub

The repository contains corroborated CDD information about African entities as well as information on investing in Africa, investment climate and procedures in African countries, and investment products and services, making the repository an African Investment Information Hub for investors or potential investors in Africa.

About Afreximbank: Afreximbank is a multilateral financial institution with the mandate to promote, expand, and finance intra- and extra-African trade, particularly, exports of finished or semi-finished goods from Africa. The Bank developed its fifth Strategic Plan dubbed 'IMPACT2021 – Africa transformed' and has been in the process of creating new initiatives and tools to facilitate trade growth in Africa and the rest of the world.

www.afreximbank.com

Nordic KYC Utility

Fredrik Millde, interim CEO, Nordic KYC utility, soon operating under the new name Invidem, talks about the importance of preventing financial crime in the financial services

About Fredrik Millde: Fredrik Millde has since 2015 contributed to multiple initiatives prior to the creation 2019 of the Nordic KYC Utility AB. Millde has a solid background as Business, Information, and Technology consultant in project manager and advisor roles. He brings entrepreneurship experience as well as line management experience from large corporations in the Financial Services sector.

Fredrik Millde ▪ *Interim CEO* ▪ Nordic KYC Utility

What is Nordic KYC utility for those who do not know it yet?

It's a joint venture company formed in 2019, where leading Nordic banks have come together and joined forces to simplify and standardise the gathering and validation of KYC customer information. We expect this to improve the customer experience and increase the effectiveness of financial crime prevention in the Nordic countries.

> *“Gatekeeping through effective KYC processes is even more important than sophisticated transaction monitoring.*

What are the specific challenges that banks face when they want to offer a digital onboarding process to corporate customers?

First of all, if customers are not happy with the cumbersome situation of suppling data, the banks are unhappy too. The solution to this problem cannot be lower barriers for entry. In fact, banks should strengthen the capability of preventing financial crime. Today's challenges are the long lead times in processes that are far from automated. The trick of the trade when it comes to a utility, is to capture non-competitive KYC data once, keep it updated, and reuse it for multiple banks. The specialisation of capturing data from reliable sources and validating data with and from customers can be highly automated as the Nordic KYC Standard for data now is set.

How can developments like biometrics, AI or blockchain be successfully applied within the KYC space (and give some examples)?

We have studied many interesting developments, when in dialogue with business partners and vendors. We are building our solution for launch H1 2020 on robust proven technologies, providing great value to our client banks through the consolidation and validation of huge amounts of data. Biometrics will surely be deployed, not too far away as identification standards and practices evolve. Passports, other ID's and signatures for individual identification will evolve over time and we will manage them as they become accepted in the market. Artificial Intelligence has large potential to analyse complex patterns and spot suspicious behaviour. Much of this power will be for risk analysis in the hands of the banks. But I am eager to see how machine learning can facilitate the process of KYC data capture and validation over time. When it comes to blockchain, we haven't really yet figured how our philosophy with a trusted central hub for compliant KYC Information, can benefit from the promises of blockchain.

What is the regulator stance when it comes to technology being used to balance compliance and convenience?

Well, they should of course answer for themselves. Our message is clear. We simplify banking relations for corporate customers AND help preventing financial crime in the Nordics. We have received encouraging and positive interest from interactions with supervisors.

➔

INVIDEM

We use our technology platform and Nordic Data standard to strengthen compliance for our client banks and for the convenience of corporate customers who spend too much time feeding the banks with information again and again.

A cornerstone of global anti-money laundering controls is complying with KYC processes/requirements. What is the difference between effective client identification/source of their wealth and poor KYC standards?

We are of course a bit biased, but we have reason to believe that gatekeeping through effective KYC processes is even more important than sophisticated transaction monitoring. In a global world with digital business relationships, hygiene levels of transparency and resulting trust will from start require effective KYC processes and requirements.

How do you see the anti-money laundering space evolving in the next 5 to 10 years?

Sorry to say but there will be no moment to claim victory for the 'good forces', as innovation is booming, resources and incentives are strong on the 'bad side'. So, the cat-and-mouse-game will go on, sophistication rise, and the bets will be higher. In this environment I speculate on a vision where regional Nordic KYC Utility-like institutions interoperate across the globe and exchange KYC Information in a highly structured and automated operation 24X7.

About Nordic KYC Utility: The Nordic KYC Utility AB is a joint venture initiative between Danske Bank, DNB, Handelsbanken, Nordea, SEB, and Swedbank. The leading Nordic banks have come together and joined forces to simplify and standardise KYC customer information to improve the customer experience and increase the effectiveness of financial crime prevention in the Nordic countries. The company will launch a product as well as the new brand Invidem in H1 2020.

www.invidem.com

Company Profiles

Company	4Stop (Fourstop GmbH)
4STOP	4Stop specialises in providing leading global KYB, KYC, and compliance services, paired with their proprietary real-time anti-fraud and monitoring technology and data science – all available from one API integration. 4Stop establish a true all-in-one solution for automated and premium fraud defence worldwide, saving businesses time, money, and resources by managing their risk.
Website	www.4stop.com
Keywords for online profile	KYC, KYB, compliance, fraud prevention, risk management, verification, VaaS, digital identity
Business model	Software-as-a-Service (SaaS), managed services, support, consulting, Verification-as-a-Service (VaaS), risk management, risk business underwriting (KYB)
Target market	Financial institutions, payment services providers, government services, online communities/web merchants, other online businesses, cryptocurrency
Contact	sales@4stop.com
Geographical presence	Global
Active since	2016
Service provider type	Digital identity service provider, technology vendor, web fraud detection company, Verification-as-a-Service (VaaS)
Member of industry associations and initiatives	Yes
Services	
Unique selling points	ExampleSolution leverages 4Stop's platform to enable merchants to screen for multiple fraud use cases, including payment, loyalty, and social media reputation. 4Stop's unique capabilities allow customers to be efficiently removed from fraud processes, supporting merchant growth.
Core services	- Fraud and risk management - Decisioning platform - Data provider and intelligence - Transaction verification - Behavioural biometrics - Transactional monitoring - Multi-account association/information sharing - Anti-fraud technology/rule-based methodology - Supervised machine learning - Case management
Pricing Model	Pricing is per 'Core Service' and/or 'Verification KYC' transaction and based on volume and complexity.
Other services	Information available upon request.
Fraud prevention partners	iovation, Jumio
Identity verification	
Identity Document Scanning	Yes
Video scanning	Yes
Personally Identifiable Information (PII) Validation	Yes
Small Transaction verification	Yes
Email verification	Yes
Phone verification	Yes
Social verification	No
Credit check	Yes
Compliance check	Yes

View company profile in online database

Intelligence	
Abuse list	Yes
Monitoring	Yes
Address Verification	Yes
Credit Bureau	Yes
Information Sharing	Yes
Monitoring	
Portfolio cross-check	Yes
Virtual address detection	Yes
Website auto-compliance	Yes
SiteAlert	Yes
KYC compliance	
Money laundering detection	Yes
Compliance sanctions & PEP screening	Yes
Deceptive traffic detection	Yes
Predictive risk analysis	Yes
Offering: authentication and verification technology used	
Technology used for authentication	API, data services, machine learning, and back-office platform
Technology used for verification	API, data services, machine learning, and back-office platform
Authentication context	
Online, Mobile, ATM, POS, Call centre, other	Online, mobile
Issuing proces (if applicable)	
Assurance levels conformity	Proporietary risk and confidence scoring technology
Online issuing process (incl lead time in working days)	Digital onboarding and proofing of digital identities supporting several identity methods from photo, image recognition, and forms data of ID documents in conjunction with live web agent and selfie capture, to established national electronic IDs in real-time.
Face-to-face issuing (incl lead time in working days)	Information available upon request.
Issuing network	Data connectiveity for online issuing process includes: - connectivity to governmental data - commercial attribute providers - credit databases - utility - phone service providers - sanctions lists - banks
Attributes offered	
Persons	Full name, address, age, document ID Verify, identity verification (biometrics), email, SSN, phone, bank account, compliance watchlist screening, compliance watchlist monitoring, adverse media screening, adverse media monitoring
Companies	business ID information, business address, business registration number, tax number, group structure, financial strength indicators, UBO's/directors identified, KYC on UBO's/directors, linked UBO's/directors, KYC on UBO's/directors, credit rating and report, compliance watchlist screenings, compliance monitoring, business documentations (e.g. articles of association), web presence screening, adverse media screening, adverse media monitoring

Reference data connectivity	
Connectivity to governmental data	Citizens register, company register, IDs
Other databases	Commercial attribute providers, credit databases, utility, phone service providers, sanctions lists, banks
Certification	
Type	No
Regulation	KYC, GDPR compliant, AML4 & 5, PSD2
Other quality programs	No
Other remarks	Information available upon request.
Clients	
Main clients / references	Mifinity, Draglet, Gatehub, Paysend, Paymentz
Future developments	Machine learning/enhanced smart rules hub, enhanced KYB/KYC solutions, on-going data aggregation and integrated KYB/KYC data services, enhanced UI/UX experience

Company	Global Data Consortium
GDC GLOBAL DATA CONSORTIUM	GDC is a leading provider and industry expert in global electronic identity verification. Our highly customisable solution provides verification of name, address, date of birth, national ID, and phone number against the highest quality data sets available, via one single API.
Website	www.globaldataconsortium.com
Keywords for online profile	identity verification, KYC, AML, eIDV, digital identity, onboarding, customer due diligence, compliance
Business model	Simple per transaction pricing. No volume commitments or recurring fees.
Target market	Fintech (challenger banks, payments platforms), sharing economy, trading platforms (comodities, crypto, forex), online gaming, online gambling, age restricted markets, ecommerce
Contact	sales@globaldataconsortium.com
Geographical presence	Global
Active since	2014
Service provider type	Digital identity as a service, software as a service, platform as a service
Member of industry associations and initiatives	Information available upon request.
Services	
Unique selling points	Our consortium of data providers allows us to access and understand international data on a local level. This pairing of high quality data and expertise drives industry leading match rates for customers, through one API.
Core services	Information available upon request.
Pricing Model	Pricing is per transaction and based on volume.
Other services	PEP/watchlist screening, INTE, manual review tool
Fraud prevention partners	Information available upon request.
Identity verification	
Identity Document Scanning	No
Video scanning	No
Personally Identifiable Information (PII) Validation	Yes
Small Transaction verification	Yes
Email verification	No
Phone verification	Yes
Social verification	No
Credit check	No
Compliance check	Yes
Intelligence	
Abuse list	Yes
Monitoring	Yes
Address Verification	Yes
Credit Bureau	Yes
Information Sharing	N/A

View company profile in online database

Monitoring	
Portfolio cross-check	No
Virtual address detection	No
Website auto-compliance	No
SiteAlert	No
KYC compliance	
Money laundering detection	Yes
Compliance sanctions & PEP screening	Yes
Deceptive traffic detection	No
Predictive risk analysis	No
Offering: authentication and verification technology used	
Technology used for authentication	Information available upon request.
Technology used for verification	Information available upon request.
Authentication context	
Online, Mobile, ATM, POS, Call centre, other	Information available upon request.
Issuing proces (if applicable)	
Assurance levels conformity	Information available upon request.
Online issuing process (incl lead time in working days)	Information available upon request.
Face-to-face issuing (incl lead time in working days)	Information available upon request.
Issuing network	Information available upon request.
Attributes offered	
Persons	Name, address, date of birth, national ID, phone number
Companies	N/A
Reference data connectivity	
Connectivity to governmental data	Drivers liscense, court records, national tax registers (think SSN and IRS), and national censuses
Other databases	Commercial, consumer, utility, credit, telco, postal
Certification	
Type	Information available upon request.
Regulation	KYC, AML, CDD
Other quality programs	Privacy compliance
Other remarks	Information available upon request.
Clients	
Main clients / references	Information available upon request.
Future developments	Information available upon request.

GDC
GLOBAL DATA
CONSORTIUM

DO YOU KNOW YOUR CUSTOMER?
Global Data Consortium Does.

Take the Guess Work Out of Identity Verification.

WE KNOW YOUR CUSTOMER.

Worldview, GDC's Electronic Identity Verification Platform is a single access point to **70+ Data Partners and 200+ Data Sources across countries all over the world.**

Financial service organizations and various businesses all over the world need to verify parties in every transaction while also adhering to privacy rules and different laws in each country.

Visit ***GlobalDataConsortium.com***
to learn more and have a Proof of Concept demo with our team.

Company	HID Global
	HID Global is the leading provider of trusted identity and access solutions for people, places, and things. We enable organisations and enterprises in a variety of industries, such as banking, healthcare, and government, to protect digital identities in a connected world and assess cyber-risk in real-time to deliver trusted transactions while empowering smart decision-making. Our extensive portfolio offers secure, convenient access to on-line services and applications and helps organisations to meet growing regulatory requirements while going beyond just simple compliance.
Website	www.hidglobal.com
Keywords for online profile	electronic signature, digital signature, identity vetting, e-ID, trusted digital identity, MFA, RBA, biometry, risk management
Business model	Perpetual or subscription per user or subscription based per transaction
Target market	Financial institutions, government, internal security for enterprise, US healthcare
Contact	IAM_Finance@hidglobal.com
Geographical presence	Global
Active since	2010
Service provider type	Identity and access management solution provider
Member of industry associations and initiatives	FIDO Alliance, OATH https://www.pcscworkgroup.com/members/member-list/ The PC/SC Workgroup https://www.securetechalliance.org/alliance-members/2702/ The Smart Card Alliance https://www.globalplatform.org/membershipcurrentfull.asp GlobalPlatform http://oixuk.org/members/ Open Identity Exchange – IdenTrust is a general member https://www.ukfinance.org.uk/ IdenTrust is an Associate Member UK Finance https://www.openbanking.org.uk/ IdenTrust is an active participant in the development of Open Banking standards in the UK Open Banking Stakeholder Group Membership PSD2/RTS Implementation Third Parties Open Banking Working Group Membership Customer WG, Information Security WG, Regulatory & Legal WG, Standards WG Operational Governance Agreement and Services WG
Services	
Unique selling points	HID Global proposes an Identity Vetting solution that is integrated with HID authentication solution allowing to issue the authentication credentials just after the identity verification has been validated increasing the level of security. It also allows to smooth the user experience by using the face recognition step of the identity verification for onboarding of the user in the face recognition for authentication. And finally it allows using some of the data gathered during the identification in order to improve the authentication process later on.
Core services	Mobile identity verification solution for digital onboarding of banking end-customers
Pricing Model	Monthly subscription based on transaction volume
Other services	HID develop and sell a full risk based authentication solution for user authentication and transaction signature.
Fraud prevention partners	HID proposes his own threat and fraud detection service.

View company profile in online database

Identity verification	
Identity Document Scanning	Yes
Video scanning	No
Personally Identifiable Information (PII) Validation	Yes
Small Transaction verification	No
Email verification	No
Phone verification	Yes
Social verification	No
Credit check	No
Compliance check	Yes
Intelligence	
Abuse list	No
Monitoring	No
Address Verification	Yes
Credit Bureau	No
Information Sharing	Yes
Monitoring	
Portfolio cross-check	N/A
Virtual address detection	N/A
Website auto-compliance	N/A
SiteAlert	N/A
KYC compliance	
Money laundering detection	N/A
Compliance sanctions & PEP screening	N/A
Deceptive traffic detection	N/A
Predictive risk analysis	N/A
Offering: authentication and verification technology used	
Technology used for authentication	PKI, biometry, push notification, OTP, transaction signature, behavioral biometry
Technology used for verification	Machine learning algorithms
Authentication context	
Online, Mobile, ATM, POS, Call centre, other	Online and mobile banking, call center, payment channel, in-branch
Issuing proces (if applicable)	
Assurance levels conformity	N/A
Online issuing process (incl lead time in working days)	N/A
Face-to-face issuing (incl lead time in working days)	N/A
Issuing network	N/A
Attributes offered	
Persons	Address, age, DOB, name
Companies	N/A

Reference data connectivity	
Connectivity to governmental data	Yes
Other databases	Credit, commercial, utility, consumer, telco, postal and proprietary
Certification	
Type	ISO 27001 (stage 1)
Regulation	CIP, KYC. AML - (MLD 4 & 5), SAFE
Other quality programs	No
Other remarks	No
Clients	
Main clients / references	No
Future developments	No

HID
ONBOARD YOUR CUSTOMERS WITH CONFIDENCE
IDENTITY VERIFICATION AND COMPLIANCE MADE SIMPLE

HID® Identity Verification Service is an off-the-shelf, end-to-end solution for digital onboarding and KYC compliance. Running a suite of advanced technical checks against every customer submission, HID Identity Verification Service ensures that identities are thoroughly authenticated and verified.

Global anti-money laundering directives are becoming more stringent, requiring regulated firms to verify the identities of their clients prior to engaging in any commercial activities. Protect your business from fraud and meet compliance requirements while providing a more user-friendly onboarding experience.

Powering **Trusted Identities** | Visit us at hidglobal.com/**iam**

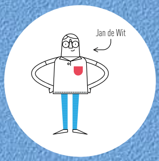
Company	iDIN BV
	iDIN BV is a joint initiative of Dutch banks. With iDIN, Dutch banks contribute to a secure and safe digitisation of the Dutch economy, based on many years of experience with online banking and security and the iDEAL online payment service. iDIN increases usability without compromising security and privacy. iDIN secures and protects personal data.
Website	www.idin.nl
Keywords for online profile	electronic identity solution, login, identification, authentication, age verification, e-ID, electronic signature, QR, GDPR
Business model	Transaction fee
Target market	Financial services, insurance, utility, telecom, online gambling, ecommerce
Contact	idin@currence.nl
Geographical presence	The Netherlands
Active since	2016
Service provider type	Scheme and product owner
Member of industry associations and intiatives	Information available upon request.
Services	
Core services	Scheme owner and solution developer for e-identity solutions
Other services	N/A
Unique selling points	Trustworthy, reliable, user friendly solution for login, identification, authentication, age verification, and electronic signature solution with a reach to almost all Dutch citizens.
Pricing model	Transaction fee
Partners	iDIN issuing licensee: ABN AMRO, ASN Bank, bunq, ING, Rabobank, RegioBank, SNS, Triodos Bank; iDIN acquirer licensee: ABN AMRO, ING, Rabobank, de Volksbank; iDIN DISP (digital identity service provider): Bluem, CM.com, Evidos, Maestro Soft SA, PAY., Rabo eBusiness, Reviva, Signicat
Offering: authentication technology used	
Technology used	https://betaalvereniging.atlassian.net/wiki/spaces/IIDIFMD/overview ; https://github.com/Currence-Online
Authentication context	
Online	Yes
Mobile	Yes
ATM	N/A
Branch/Point of Sale	Via QR code
Call Centre	N/A
Other:	Information available upon request.
Issuing proces (if applicable)	
Assurance levels conformity	LOA3/eIDAS substantial
Online issuing process (incl lead time in working days)	Can be instant, depends on issuing licensee.
Face-to-face issuing (incl lead time in working days)	Can be instant, depends on issuing licensee.
Issuing network	Via Issuing licensees

View company profile in online database

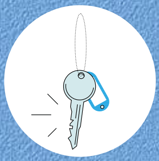
Attributes offered	
Persons	Unique number for logging in: - BIN - Bank Identification Number, suitable for repeat log ins (number is allocated by the user's bank (issuer) and gives the user a unique identity in their dealings with merchants); Transient_ID for one-off use (one-off number allocated by the issuer to the message in question). Verified user data Originating from an independent source, the legal identity document: - name: initial(s), prefixes, last name (legal last name); - age indication (18 years or older) or date of birth; - gender. Data issued to the bank by the user: - user's preferred last name (preferred/partner last name); - residential address: street, house number, postcode, city/town; - email address; - telephone number.
Companies	N/A
Reference data connectivity	
Connectivity to governmental data	Waiting for legislation from the government: Wet digitale overheid.
Other databases	Additional services and combinations are offered by the iDIN partners.
Certification	
Type	https://www.idin.nl/over-idin/regelgeving-compliance/
Regulation	iDIN BV is partly regulated by the Dutch central Bank and all scheme participants are certified by iDIN BV.
Other quality programs	N/A
Other remarks	Information available upon request.
Clients	
Main clients / references	https://www.idin.nl/bedrijven/gebruikerservaringen/ https://www.idin.nl/consumenten/waar-idin-gebruiken/
Future developments	iDIN Signature

iDIN

Easy, safe and reliable!

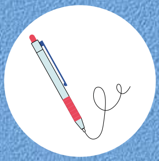


identify



log in

confirm age



sign

With the secure and trusted login method of your bank

WWW.iDIN.NL

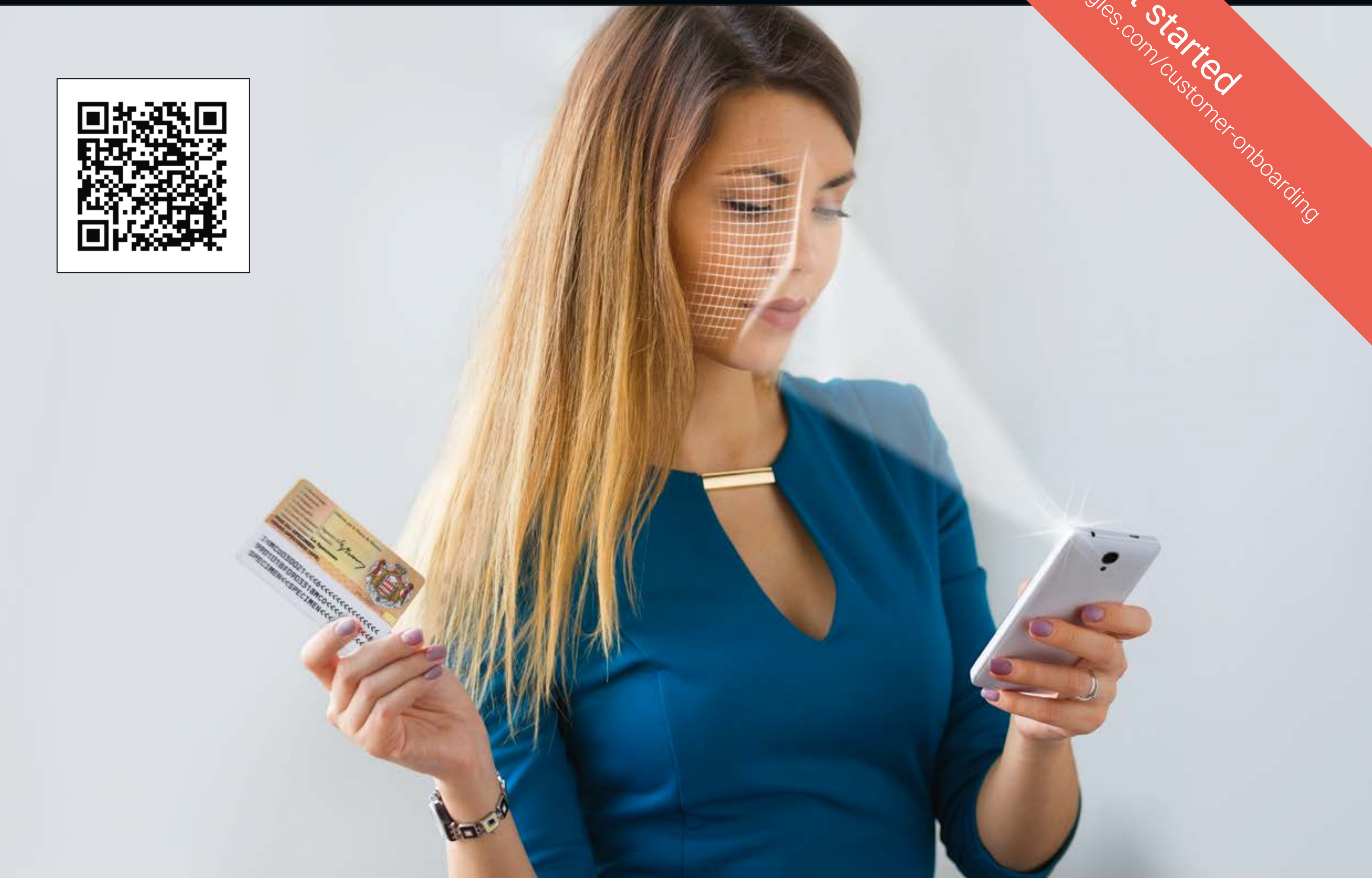
Company	Keesing Technologies
KEESING Technologies	Keesing Technologies is a database publisher and software service provider that is able to capitalise on its unrivaled knowledge on international identity documents for the purpose of identity proofing by combining biometric checks with ID Document verification based on the established Keesing Documentchecker Database.
Website	www.keesingtechnologies.com
Keywords for online profile	ID document verification, identity proofing, digital onboarding, KYC
Business model	Subscription-based or transactional
Target market	Card issuers, acquirers, payment processors, government services, business services (webmerchants, utilities, telco's, accounting, financial, agriculture, chemical, transport)
Contact	sales@keesingtechnologies.com
Geographical presence	Global
Active since	1911
Service provider type	Software services, database publishing
Member of industry associations and initiatives	N/A
Services	
Unique selling points	Based on Keesing's core competence; the most comprehensive database of international identity documents 'Keesing Documentchecker', Keesing understands identity documents like no other company in the market and adds best of breed solutions from 3rd parties for biometric screening and identity verification to its offering.
Core services	The Keesing AuthentiScan WEBAPI service, which combines biometric identity verification with extensive ID document verification based on the Keesing Documentchecker database.
Pricing Model	Pricing is either per subscription or per transaction based on volume and complexity.
Other services	Training and cosultancy on the subject of ID document verification; Keesing Platform for industry news on secured documents
Fraud prevention partners	N/A
Identity verification	
Identity Document Scanning	Yes
Video scanning	Yes
Personally Identifiable Information (PII) Validation	Yes
Small Transaction verification	No
Email verification	No
Phone verification	No
Social verification	No
Credit check	No
Compliance check	Yes
Intelligence	
Abuse list	Yes
Monitoring	No
Address Verification	No
Credit Bureau	No
Information Sharing	Yes

View company profile in online database

Monitoring	
Portfolio cross-check	No
Virtual address detection	No
Website auto-compliance	No
SiteAlert	No
KYC compliance	
Money laundering detection	No
Compliance sanctions & PEP screening	Yes
Deceptive traffic detection	No
Predictive risk analysis	No
Offering: authentication and verification technology used	
Technology used for authentication	Yes
Technology used for verification	Yes
Authentication context	
Online, Mobile, ATM, POS, Call centre, other	Online, mobile, remote, on premises, offline
Issuing proces (if applicable)	
Assurance levels conformity	N/A
Online issuing process (incl lead time in working days)	N/A
Face-to-face issuing (incl lead time in working days)	N/A
Issuing network	N/A
Attributes offered	
Persons	Identification, liveness detection, age check, right to work, AML/PEP & Sanctions screening
Companies	N/A
Reference data connectivity	
Connectivity to governmental data	Yes
Other databases	Keesing Documentchecker Database, Lost & Stolen travel documents, PEP & Sanctions lists, Watchlists
Certification	
Type	ISO 27001, ISO 9001
Regulation	Fully GDPR compliant
Other quality programs	Code of Ethics and business conduct; Commitment to Sustainable Development Goals
Other remarks	Keesing Technologies is part of IN GROUPE with additional certifications available.
Clients	
Main clients / references	More than 1,500 clients in the commercial and governmental sector. Keesing client portfolio includes global FI's, Fintech's, PSP's, and system integrators.
Future developments	Keesing Technologies will enhance its solutions by adding safe and secure user authentication to its AuthentiScan portfolio with the ambition to expand further into the digital identity space.

KEESING Technologies

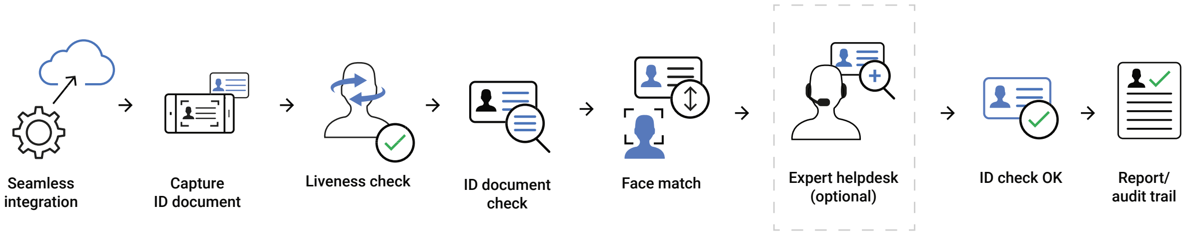
Get started
keesingtechnologies.com/customer-onboarding



Keesing AuthentiScan

Secure, digital identity proofing

Combining biometric checks with Keesing's trusted ID document verification



Seamless integration → Capture ID document → Liveness check → ID document check → Face match → Expert helpdesk (optional) → ID check OK → Report/ audit trail

Keesingtechnologies.com/customer-onboarding

Company	LexisNexis Risk Solutions
LexisNexis® RISK SOLUTIONS	LexisNexis Risk Solutions leverages comprehensive digital and physical identity intelligence, machine learning, and advanced big data analytics to accelerate risk management decisions and fortify fraud defences businesses worldwide. Our solutions combine innovative technology and intuitive analytics to deliver a concise 360-degree view of risk at any point in the customer lifecycle.
Website	risk.lexisnexis.com/EMEA
Keywords for online profile	financial crime compliance, anti-money laundering, KYC due diligence, risk assessment, fraud detection, identity verification, regulatory reporting, customer data management
Business model	N/A
Target market	Financial services (banks and other financial regulated entities including PSPs, money service businesses, and investment firms), corporations from a wide range of sectors including ecommerce and retail, telco and media, aviation, gaming and gambling, public sector and NGO/NFPs
Contact	Alex Norton, Senior Marketing Manager EMEA
Geographical presence	Global
Active since	1970
Service provider type	Financial crime compliance (customer and vendor risk assessment, KYC and due diligence, watchlist screening – sanctions and enforcement, PEP political exposed persons, adverse media, SOE state owned and goverment linked entities). Fraud and identity management (digital identity, fraud analytics, identity verification and authentication).
Member of industry associations and intiatives	MRC, ACAMS, Vendorcom, ACSEL, aDigital, EPSM, Holland FinTech, GSMA, CFCA, France Fintech, ACCPA, plus many more worldwide
Services	
Unique selling points	LexisNexis Risk Solutions combines cutting-edge technology, unique data, and advanced analytics across fraud and identity, financial crime compliance, and customer data management. Through the most advanced technology, we enable our customers to perform real-time background checks on individuals and businesses, and ultimately make critical onboarding and compliance decisions.
Core services	Fraud and identity management; and financial crime compliance (AML/ABC)
Pricing Model	N/A
Other services	N/A
Fraud prevention partners	N/A
Identity verification	
Identity Document Scanning	Yes
Video scanning	N/A
Personally Identifiable Information (PII) Validation	Yes
Small Transaction verification	Yes
Email verification	Yes
Phone verification	Yes
Social verification	N/A
Credit check	Yes
Compliance check	Yes

View company profile in online database

Intelligence	
Abuse list	N/A
Monitoring	Yes
Address Verification	Yes
Credit Bureau	Yes
Information Sharing	Yes
Monitoring	
Portfolio cross-check	No
Virtual address detection	No
Website auto-compliance	No
SiteAlert	No
KYC compliance	
Money laundering detection	Yes
Compliance sanctions & PEP screening	Yes
Deceptive traffic detection	Yes
Predictive risk analysis	Yes
Offering: authentication and verification technology used	
Technology used for authentication	A private SaaS application suite, employing global data centre facility recovery.
Technology used for verification	A private SaaS application suite, employing global data centre facility recovery.
Authentication context	
Please select what context applies to your company out of Online, Mobile, ATM, POS, Call centre, other	Other
Issuing proces (if applicable)	
Assurance levels conformity	N/A
Online issuing process (incl lead time in working days)	N/A
Face-to-face issuing (incl lead time in working days)	N/A
Issuing network	N/A
Attributes offered	
Persons	N/A
Companies	N/A
Reference data connectivity	
Connectivity to governmental data	N/A
Other databases	N/A
Certification	
Type	N/A
Regulation	N/A
Other quality programs	N/A
Other remarks	N/A
Clients	
Main clients / references	N/A
Future developments	N/A

Company	Mitek Systems
Mitek	Mitek brings the future to business with patented solutions and intuitive technologies that bridge the physical and digital worlds. Our leadership in identity verification, including facial biometrics, image capture technology, and ID card verification enables customers to confidently onboard users, verify identities within seconds, and strengthen security against cybercrimes. Mitek products power and protect millions of identity evaluations as well as mobile deposits every day, around the world.
Website	www.miteksystems.com
Keywords for online profile	identity verification, digital identity verification, biometrics, id verification, Mitek
Business model	SaaS, per transaction pricing
Target market	Finantial institutions
Contact	info@miteksystems.com
Geographical presence	Global
Active since	1986
Service provider type	Digital identity services
Member of industry associations and initiatives	Information available upon request.
Services	
Unique selling points	Making user onboarding convenient, fast, and safe, Mitek's identity verification solution delivers forensic-level authentication of ID documents from more than 190 countries, and confidently compares the user's facial biometrics to the document. Loved by over 80 million users, Mitek's capture technology encourages user adoption – making the verification process intuitive and easy for all users.
Core services	Digital identity verification through identity document authentication and facial biometrics comparison with liveness detection.
Pricing Model	SaaS, per transaction pricing
Other services	Information available upon request.
Fraud prevention partners	Information available upon request.
Identity verification	
Identity Document Scanning	Yes
Video scanning	N/A
Personally Identifiable Information (PII) Validation	Yes
Small Transaction verification	Yes
Email verification	Yes
Phone verification	Yes
Social verification	Yes
Credit check	Yes
Compliance check	Yes
Intelligence	
Abuse list	N/A
Monitoring	N/A
Address Verification	N/A
Credit Bureau	N/A
Information Sharing	N/A

View company profile in online database ▶

Monitoring	
Portfolio cross-check	N/A
Virtual address detection	N/A
Website auto-compliance	N/A
SiteAlert	N/A
KYC compliance	
Money laundering detection	N/A
Compliance sanctions & PEP screening	N/A
Deceptive traffic detection	N/A
Predictive risk analysis	N/A
Offering: authentication and verification technology used	
Technology used for authentication	Articial intelligence as computer vision and machine learning
Technology used for verification	Biometrics, articial intelligence
Authentication context	
Online, Mobile, ATM, POS, Call centre, other	Online, mobile, desktop
Issuing proces (if applicable)	
Assurance levels conformity	Information available upon request.
Online issuing process (incl lead time in working days)	Online identification verification and authenticate goverment issued identity documents, like passports, ID cards, and driver´s licenses, around the globe.
Face-to-face issuing (incl lead time in working days)	Information available upon request.
Issuing network	Information available upon request.
Attributes offered	
Persons	Personal data
Companies	N/A
Reference data connectivity	
Connectivity to governmental data	N/A
Other databases	N/A
Certification	
Type	ISO 27001, ISO 9001
Regulation	KYC, AML
Other quality programs	Information available upon request.
Other remarks	Information available upon request.
Clients	
Main clients / references	MoneyGram, Experian, CaixaBank
Future developments	Information available upon request.

Company	InnoValor/ReadID
READID POWERED BY INNOVALOR	ReadID is the leading NFC-based mobile identity verification provider. ReadID originated from research at the Dutch fintech company InnoValor and is now a solution for mobile identity verification using NFC and smartphones that is adopted quickly in different sectors and application areas where fraud prevention and data quality are key.
Website	www.readid.com
Keywords for online profile	identity document verfication, NFC, mobile, passport, KYC, AML, onboarding, reverification
Business model	Different models possible. Typically per transaction
Target market	Banking, card issuers, pension funds, government services, border control, qualified certificates, tourism, HR, rental services
Contact	readid@innovalor.nl
Geographical presence	Europe. Global sales partners
Active since	2014
Service provider type	Mobile identity document verification
Member of industry associations and initiatives	Holland Fintech, Biometrics institute, Hague Security Delta, MyData Global
Services	
Unique selling points	Unrivalled quality of verfication, integration with face matching, reliable data extraction resulting in no OCR mistakes, access to high-res face image. Long experience in the field with detailed knowledge on all identity documents and smartphones. Easy starting process through whitelabel app. Highlevel API as well as low level integration options through SDK.
Core services	Identity document verfication, orchestration with face matching partners, available as SDK or whitelabel app with SaaS backend
Pricing Model	Pricing is per transaction and based on volume and complexity, plus fixed fee.
Other services	Professional services to support implementation
Fraud prevention partners	Information available upon request.
Identity verification	
Identity Document Scanning	Yes
Video scanning	Through partners
Personally Identifiable Information (PII) Validation	Yes
Small Transaction verification	No
Email verification	No
Phone verification	No
Social verification	No
Credit check	No
Compliance check	No
Intelligence	
Abuse list	N/A
Monitoring	N/A
Address Verification	N/A
Credit Bureau	N/A
Information Sharing	N/A

View company profile in online database

Monitoring	
Portfolio cross-check	N/A
Virtual address detection	N/A
Website auto-compliance	N/A
SiteAlert	N/A
KYC compliance	
Money laundering detection	N/A
Compliance sanctions & PEP screening	N/A
Deceptive traffic detection	N/A
Predictive risk analysis	N/A
Offering: authentication and verification technology used	
Technology used for authentication	Facial matching with face image in chip (through partners)
Technology used for verification	NFC based on ICAO 9303/PKI
Authentication context	
Please select what context applies to your company out of Online, Mobile, ATM, POS, Call centre, other	Mobile
Issuing proces (if applicable)	
Assurance levels conformity	N/A
Online issuing process (incl lead time in working days)	N/A
Face-to-face issuing (incl lead time in working days)	N/A
Issuing network	N/A
Attributes offered	
Persons	Passport data from chip (name, face image, date of birth, doc number etc.)
Companies	N/A
Reference data connectivity	
Connectivity to governmental data	No
Other databases	No
Certification	
Type	ISO27001
Regulation	Information available upon request.
Other quality programs	GDPR, DPIA, pen testing
Other remarks	Information available upon request.
Clients	
Main clients / references	Examples include: UK Home Office (EU Settlement Scheme), ING Bank (onboarding), Rabobank (onboarding, verification), DNB Norway (onboarding), SK (qualified signatures)
Future developments	Strong focus on innovation

The information below was sucessfully scanned.

Scanned info

Document Number	219856633
Date of birth	10 03 65
Dat of expiry	

Company	Signicat
SIGNICAT Trusted Digital Identity™	Signicat is a pioneering, pan-European digital identity company with an unrivalled track record in the world's most advanced digital identity markets. Its digital identity platform incorporates the most extensive suite of identity verification and authentication systems in the world, all accessible through a single integration point. The platform supports the full identity journey, from recognition and onboarding, through login and consent, to making business agreements which stand the test of time. Signicat was founded in 2007 and is headquartered in Trondheim, Norway.
Website	www.signicat.com
Keywords for online profile	digital identity lifecycle, verification, authentication, electronic signing, eID
Business model	Subscription-based, one off, per transaction
Target market	Card issuers, acquirers, payment processors, government services, business services (webmerchants, utilities, telco's, accounting, financial, agriculture, chemical, transport)
Contact	katinka.forbord@signicat.com
Geographical presence	Norway Sweden Denmark Finland The Netherlands Portugal UK Germany Belgium
Active since	2006
Service provider type	Digital identity service provider
Member of industry associations and initiatives	ETSI, EEMA, OIX, IAPP, Norstella, Standard Norge, ISF, Cloud Signature Consortium (CSC)
Services	
Unique selling points	Signicat's digital identity platform incorporates the most extensive suite of identity verification and authentication systems in the world, all accessible through a single integration point. The platform simplifies digital customer engagement, including onboarding, identity verification, authentication and electronic signing, and a digital archive.
Core services	identity verification (onboarding), identity validation, authentication (login), electronic signatures and seals, timestamping
Pricing Model	Setup fee, montly fee, transaction fee
Other services	Information available upon request.
Fraud prevention partners	Information available upon request.
Identity verification	
Identity Document Scanning	Yes
Video scanning	Yes
Personally Identifiable Information (PII) Validation	Yes
Small Transaction verification	No
Email verification	Yes
Phone verification	No
Social verification	Yes
Credit check	Yes (we have attributes providers offering this)
Compliance check	Yes

View company profile in online database

Intelligence	
Abuse list	N/A
Monitoring	N/A
Address Verification	Yes
Credit Bureau	N/A
Information Sharing	N/A
Monitoring	
Portfolio cross-check	N/A
Virtual address detection	N/A
Website auto-compliance	N/A
SiteAlert	N/A
KYC compliance	
Money laundering detection	N/A
Compliance sanctions & PEP screening	Yes
Deceptive traffic detection	N/A
Predictive risk analysis	N/A
Offering: authentication and verification technology used	
Technology used for authentication	2 factor authentication, SMS OTP, MobileID (Secure back-channel)
Technology used for verification	Onfido, ReadID, ElectronicID, and more
Authentication context	
Online, Mobile, ATM, POS, Call centre, other	Online
Issuing proces (if applicable)	
Assurance levels conformity	N/A
Online issuing process (incl lead time in working days)	N/A
Face-to-face issuing (incl lead time in working days)	N/A
Issuing network	N/A
Attributes offered	
Persons	Signicat offers a range of attributes such as name, age, address. Signicat enables several registry lookups to provide additional information about a user (B2C) or an organisation (B2B). More concretely, we enable registry lookups such as looking for individuals on Politically Exposed Person (PEP) and sanction lists.
Companies	Signicat offers a range of attributes, also business-to-business checks, including: **Basic company information:** Name of organisation Organisation Number Address Company Format Ownership Structure **Individual roles within the company:** Name and date of birth of the general manager Official Authorisations (e.g.: Signing authority) Real rights holders (owners with more than 25%) Shareholder structure (ownership rate in percentages) PEP and sanctions for the company (for the legal entity)

Reference data connectivity	
Connectivity to governmental data	Yes, Signicat connects to governmental data in various countries: https://www.signicat.com/identity-methods
Other databases	Information available upon request.
Certification	
Type	QTSA
Regulation	eIDAS
Other quality programs	ISO 27001
Other remarks	SOC2
Clients	
Main clients / references	Rabobank, Western Union, Telia, Santander, Klarna, Bank Nowegian
Future developments	Anti-Money Laundering + Validation, CRM Sign, Self-Service

Company	Trulioo
	Trulioo is a global identity and business verification company that provides secure access to reliable, independent, trusted data sources to instantly verify customers and merchants online. The Trulioo instant online verification platform, GlobalGateway, helps organisations comply with AML and KYC requirements by automating due diligence workflows across borders through a single solution.
Website	www.trulioo.com
Keywords for online profile	regtech, KYC, Know Your Customer, AML compliance, identity verification, ultimate beneficial owners, identity checks, customer due diligence
Business model	Per transaction (verification)
Target market	Financial services providers/banks, online marketplaces/ecommerce, gaming/gambling, exchange platforms (wealth, stocks, crypto), payment processors, card issuers, acquirers
Contact	media@trulioo.com
Geographical presence	Global
Active since	2011
Service provider type	Digital identity service providers
Member of industry associations and initiatives	DIACC, Fintech Growth Syndicate, MaRS
Services	
Unique selling points	Trulioo GlobalGateway offers a single point of integration to access over 400 global data sources to instantly verify and authenticate 5 billion people and 330 million companies in over 100 countries.
Core services	Digital identity verification for AML, KYC, and CDD requirements, and fraud prevention and risk mitigation.
Pricing Model	Pricing is per transaction and based on volume and complexity.
Other services	Information available upon request.
Fraud prevention partners	Offers mobile ID, business verification, and ID document verification.
Identity verification	
Identity Document Scanning	Yes
Video scanning	No
Personally Identifiable Information (PII) Validation	Yes
Small Transaction verification	No
Email verification	Yes
Phone verification	Yes
Social verification	No
Credit check	No
Compliance check	Yes
Intelligence	
Abuse list	No
Monitoring	No
Address Verification	Yes
Credit Bureau	Yes
Information Sharing	No

View company profile in online database

Monitoring	
Portfolio cross-check	N/A
Virtual address detection	N/A
Website auto-compliance	N/A
SiteAlert	N/A
KYC compliance	
Money laundering detection	Yes
Compliance sanctions & PEP screening	Yes
Deceptive traffic detection	No
Predictive risk analysis	Yes
Offering: authentication and verification technology used	
PIN	No
Password/phrase	Yes (for API)
Token	Yes
Card	No
Digital certificates (hosted yes/no)	No
Multifactor authentication	Yes (in the portal)
Biometrics	Yes
Authentication context	
Online	Yes
Mobile	Yes
ATM	No
Branch/Point of Sale	Yes
Call centre,	Yes
Other	N/A
Issuing proces (if applicable)	
Assurance levels conformity	N/A
Online issuing process (incl lead time in working days)	N/A
Face-to-face issuing (incl lead time in working days)	N/A
Issuing network	N/A
Attributes offered	
Persons	First, middle, and last name; DOB; minimum age; gender; address; mobile/telephone number; email address; driving licence number and expiry; national IDs
Companies	Date of incorporation, jurisdiction of incorporation, shareholder list document, financial information document, address, mobile/telephone number, email address
Reference data connectivity	
Connectivity to governmental data	Citizens register, company register, national IDs
Other databases	Utility bills, mobile network operators, electoral roll, credit bureau, fraud, telco, watchlists, consumer files

Certification	
Type	ISO27001
Regulation	KYC, AML, 5AMLD, PSD2, FCA, Fintrac, MiFID II, GDPR and FinCEN, AUSTRAC
Other quality programs	N/A
Other remarks	N/A
Clients	
Main clients / references	Trulioo is a trusted verification provider for more than 500 companies, including some of the world’s top payments, ecommerce, technology and financial services providers.
Future developments	N/A

Company	Web Shield
WEBSHIELD®	Web Shield, founded in 2011, is a leading regtech company, offering real-time onboarding and risk-based monitoring solutions. As the trusted partner of international players in the field of merchant acquiring and payment processing, we assist our clients by enabling exceptionally fast onboarding and compliance in an increasingly complex regulatory landscape.
Website	www.webshield.com
Keywords for online profile	onboarding, monitoring, underwriting, due diligence
Business model	SaaS, training
Target market	- financial institutions - acquiring banks - payment services providers - cryptocurrency merchants
Contact	compliance@webshield.com
Geographical presence	Germany, Poland, UK
Active since	2011
Service provider type	Technology vendor
Member of industry associations and initiatives	Merchant Acuirers' Comittee, Electronic Transactions Association, European Financial Coalition, International RegTech Association, Vendorcom, Internet Watch Foundation, European Payments Service Providers for Merchants
Services	
Unique selling points	In addition to their unrivalled speed and precision, the modular design of our high-end SaaS solutions can be adapted to an organisation's individual risk appetite and compliance requirements.
Core services	Merchant onboarding and monitoring SaaS solutions for acquiring banks and payment service providers
Pricing Model	Subscription and on-demand
Other services	Training for underwriters, cryprocurrency compliance solutions for acquirers and merchants
Fraud prevention partners	N/A
Identity verification	
Identity Document Scanning	N/A
Video scanning	N/A
Personally Identifiable Information (PII) Validation	N/A
Small Transaction verification	N/A
Email verification	N/A
Phone verification	N/A
Social verification	N/A
Credit check	N/A
Compliance check	N/A
Intelligence	
Abuse list	Yes
Monitoring	Yes
Address Verification	Yes
Credit Bureau	Yes
Information Sharing	Yes

View company profile in online database

Monitoring	
Portfolio cross-check	Yes
Virtual address detection	Yes
Website auto-compliance	Yes
SiteAlert	Yes
KYC compliance	
Money laundering detection	Yes
Compliance sanctions & PEP screening	Yes
Deceptive traffic detection	Yes
Predictive risk analysis	Yes
Offering: authentication and verification technology used	
Technology used for authentication	No
Technology used for verification	Yes
Authentication context	
Online, Mobile, ATM, POS, Call centre, other	Other
Issuing proces (if applicable)	
Assurance levels conformity	N/A
Online issuing process (incl lead time in working days)	N/A
Face-to-face issuing (incl lead time in working days)	N/A
Issuing network	N/A
Attributes offered	
Persons	Yes
Companies	Yes
Reference data connectivity	
Connectivity to governmental data	Yes
Other databases	LexisNexis World Complicance, OpenCorporates
Certification	
Type	N/A
Regulation	N/A
Other quality programs	Official Mastercard Merchant Monitoring Service Provider
Other remarks	N/A
Clients	
Main clients / references	Wirecard, Paysafe, Sberbank, Concardis (onboarding and monitoring)
Future developments	PayTracer transaction analysis for correspondence banks, Versatile Customer Underwriting enhanced due diligence tool for notaries.

WEBSHIELD®

KNOW YOUR MERCHANTS

At Web Shield, we know how important speed is for your underwriting team – because as clichéd as it sounds: in our business, time is money.

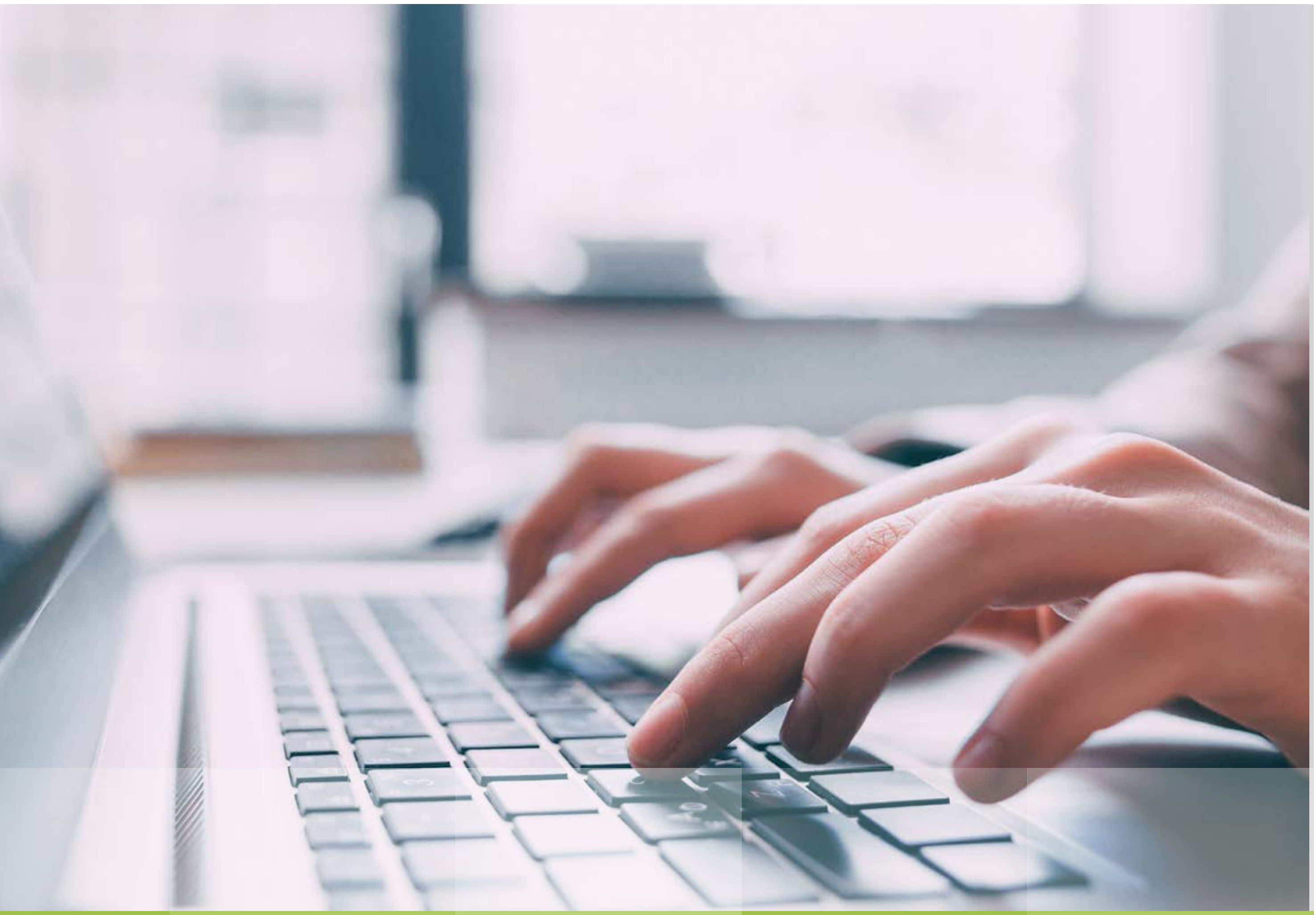
That's why we developed a solution that gathers all risk intelligence in ONE place and made it real-time: With **InvestiGate**, you can work on your cases as soon as they enter the system. Its enhanced automation makes sure you get to your results with minimal manual input.

Our **Monitor** solution uses the same analytical framework to enable automated monitoring routines to keep your portfolio compliant and your business profitable in the long run.

Stay one step ahead of fraudsters and the competition – with **Web Shield**.

SEE OUR SOLUTIONS IN ACTION

Interested in a demonstration?
Just contact us and we will set one up!
https://www.webshield.com/about-us/contact



Glossary

Glossary

A

AML/CFT Returns

Regular or ad hoc requests to companies for quantitative data relating to key ML/TF risk indicators AML/CFT returns are different from offsite inspections in that they are frequently automated and often not comprehensive; their aim is often to help supervisors gain a better understanding of the ML/TF risks to which their sector is exposed, rather than to assess the adequacy of a firm's AML/CFT systems and controls.

Anti-Money Laundering Program

The system designed to assist institutions in their fight against money laundering and terrorist financing. In many jurisdictions, government regulations require financial institutions, including banks, securities dealers and money services businesses, to establish such programs. At a minimum, the anti-money laundering program should include:

- Written internal policies, procedures and controls;
- A designated AML compliance officer;
- On-going employee training; and
- Independent review to test the program

Authenticity

In the context of information security, authenticity refers to the truthfulness of information and whether it has been transmitted or created by an authentic sender. Authenticity can be achieved by digitally signing a message with the sender's private key. The recipient can verify the digital signature with the matching public key.

Authorisation

The process of giving someone or something permission to do something, for example to gain access to services, data or other functionalities.

B

Basel Committee on Banking Supervision (Basel Committee)

The Basel Committee was established by the G-10's central bank of governors in 1974 to promote sound supervisory standards worldwide. Its secretariat is appointed by the Bank for International Settlements in Basel, Switzerland. It has issued, among others, papers on customer due diligence for banks, consolidated KYC risk management, transparency in payment messages, due diligence and transparency regarding cover payment messages related to cross-border wire transfers, and sharing of financial records among jurisdictions in connection with the fight against terrorist financing.

C

Criminal Proceeds

Any property derived from or obtained, directly or indirectly, through the commission of a crime.

Currency Smuggling

The illicit movement of large quantities of cash across borders, often into countries without strict banking secrecy, poor exchange controls or poor anti-money laundering legislation.

Customer Due Diligence

Identification and verification of customers and beneficial owners.

D

Data Model

Description of how data can be stored, processed and accessed.

Data Self-determination

The capacity of an individual or organisation to control who has access to his/her/its (personal) data and under what conditions (see also: Data Sovereignty).

Data Sovereignty

The capability of an individual or organisation to be entirely self-determining with regard to his/her/its data.

Digital Signature

A digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted document to verify its contents and the sender's identity.

E

eIDAS

An EU regulation on electronic identification and trust services for electronic transactions in the European Single Market. This regulation covers important aspects related to electronic transactions, such as qualified electronic certificates. eIDAS provides a safe way for users to conduct business online. ➔

Glossary

Electronic Funds Transfer (EFT)

The movement of funds between financial institutions electronically. The two most common electronic funds transfer systems in the U.S. are FedWire and CHIPS.

Electronic Money (E-Money)

Electronic cash represents a series of monetary value units in some electronic format, such as being stored electronically online, on the hard drive of a device, or on the microchip of a plastic card.

Electronic Signatures

An electronic signature, or e-signature, refers to data in electronic form, which is logically associated with other data in electronic form and which is used by the signatory to sign.

Electronic Seals

An electronic seal is a piece of data attached to an electronic document or other data, which ensures data origin and integrity.

Enhanced Due Diligence (EDD)

In conjunction with Customer Due Diligence, EDD calls for additional measures aimed at identifying and mitigating the risk posed by higher risk customers. It requires developing a more thorough knowledge of the nature of the customer, the customer's business and understanding of the transactions in the account than a standard or lower risk customer. A financial institution should ensure account profiles are current and monitoring should be risk-based.

F

Federated Identity

A federated identity is the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems. Without federated identity, users are forced to manage different credentials for every site they use.

Related to federated identity is single sign-on (SSO), in which a user's single authentication ticket, or token, is trusted across multiple IT systems or even organizations. SSO is a subset of federated identity management, as it relates only to authentication and is understood on the level of technical interoperability and it would not be possible without some sort of federation.

Financial Action Task Force (FATF)

FATF was chartered in 1989 by the Group of Seven industrial nations to foster the establishment of national and global measures to combat money laundering. It is an international policy-making body that sets anti-money laundering standards and counter-terrorist financing measures worldwide. Its Recommendations do not have the force of law. Thirty-five countries and two international organizations are members. In 2012, FATF substantially revised its 40 + 9 Recommendations and reduced them to 40. FATF develops annual typology reports showcasing current money laundering and terrorist financing trends and methods.

Financial Action Task Force on Money Laundering in Latin America (GAFILAT)

A FATF-style regional body for Latin America, established in 2000.

I

Identity Service Provider

An identity provider (IdP) is a system entity that creates, maintains, and manages identity information for principals while providing authentication services to relying party applications within a federation or distributed network.

Usually it offers user authentication as a service. Relying party applications, such as web applications, outsource the user authentication step to a trusted identity provider. Such a relying party application is said to be federated, that is, it consumes federated identity.

An identity provider is considered a trusted provider that enables consumers use single sign-on (SSO) to access other websites. SSO enhances usability by reducing password fatigue. It also provides better security by decreasing the potential attack surface.

Identity Verification

Checking the provided information about the identity with previously corroborated information and its binding to the entity. ➔

Glossary

K

Know Your Customer (KYC)

The term refers to due diligence activities that financial institutions and other regulated companies must perform to ascertain relevant information from their clients for the purpose of doing business with them. Know your customer policies are becoming increasingly important globally to prevent identity theft, financial fraud, money laundering, and terrorist financing.

L

Levels of Assurance

Within online authentication, depending on the authentication protocol used, different Levels of Assurance give the server different degrees of certainty about the client's identity. Depending on parameters such as the quality of the registration process, quality of credentials, use of biometrics or multiple authentication factors and information security, an authentication protocol can provide a server with high or low confidence in the claimed identity of the client. For low-interest products, a low Level of Assurance might be sufficient, while for sensitive data it is essential that a server is confident that the client's claimed identity is valid.

M

Monitoring

An element of an institution's anti-money laundering program in which customer activity is reviewed for unusual or suspicious patterns, trends or outlying transactions that do not fit a normal pattern. Transactions are often monitored using software that weighs the activity against a threshold of what is deemed "normal and expected" for the customer.

O

Offshore

Literally, away from one's own home country – if one lives in Europe, the US is 'offshore'. In the money laundering lexicon, the term refers to jurisdictions deemed favourable to foreign investments because of low or no taxation or strict bank secrecy regulations.

Offshore Banking License

A license that prohibits a bank from doing business with local citizens or in local currency as a condition of its license.

P

Politically Exposed Person (PEP)

In financial regulation, a politically exposed person (PEP) is one who has been entrusted with a prominent public function. A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold.

R

Risk-Based Authentication (RIBA)

Risk-Based Authentication is where issuing banks apply varying levels of stringency to authentication processes, based on the likelihood that access to a given system could result in it being compromised.

As the level of risk increases, the authentication process becomes more intense.

S

Shell Bank

Bank that exists on paper only and that has no physical presence in the country where it is incorporated or licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision.

Smurfing

A commonly used money laundering method, smurfing involves the use of multiple individuals and/or multiple transactions for making cash deposits, buying monetary instruments or bank drafts in amounts under the reporting threshold. The individuals hired to conduct the transactions are referred to as 'smurfs'.

Structured Data Assets

Data that adheres to a pre-defined data model which is primarily useful for interpretation by machines. ➔

Glossary

Suspicious Transaction Report (STR)

A government filing required by reporting entities that includes a financial institution's account of a questionable transaction. Many jurisdictions require financial institutions to report suspicious transactions to relevant government authorities such as its FIU on a suspicious transaction report (STR), also known as a suspicious activity report or SAR.

T

Tax Haven

Countries that offer special tax incentives or tax avoidance to foreign investors and depositors.

Terrorist Financing

The process by which terrorists fund their operations in order to perform terrorist acts. There are two primary sources of financing for terrorist activities. The first involves financial support from countries, organizations or individuals. The other involves a wide variety of revenue-generating activities, some illicit, including smuggling and credit card fraud.

U

Unique Identity

A set of identifiers/attributes forms an unique identity. Furthermore, an identifier such as a unique number or any set of attributes, can determine precisely who or what the entity is.

Unstructured Data Assets

Data that does not have a pre-defined data model or is not organised in a pre-defined way, making it primarily interpretable by humans.

V

Virtual Currency

A medium of exchange that operates in the digital space that can typically be converted into either a fiat (e.g., government issued currency) or it can be a substitute for real currency.

THE | PAYPERS

Don’t Miss the Opportunity of Being Part of Large-Scale Payments Industry Overviews

Once a year, The Paypers releases four large-scale industry overviews covering the latest trends, developments, disruptive innovations and challenges that define the global online/mobile payments, e-invoicing, B2B payments, ecommerce and web fraud prevention & digital identity space. Industry consultants, policy makers, service providers, merchants from all over the world share their views and expertise on different key topics within the industry. Listings and advertorial options are also part of the Guides for the purpose of ensuring effective company exposure at a global level.

THE PAYPERS
Insights into Payments
B2B Payments and Fintech Guide 2019
Innovations in the Way Businesses Transact

B2B Payments and Fintech Guide 2019

Payment Methods Report 2019

Open Banking Report 2019

THE PAYPERS
Insights into Payments and Beyond
Fraud Prevention and Online Authentication Report 2019/2020
Managing Risks and Preventing Fraud with New Technologies and the Right Expertise

Fraud Prevention and Online Authentication Report 2019 / 2020

For the latest edition, please check the Reports section