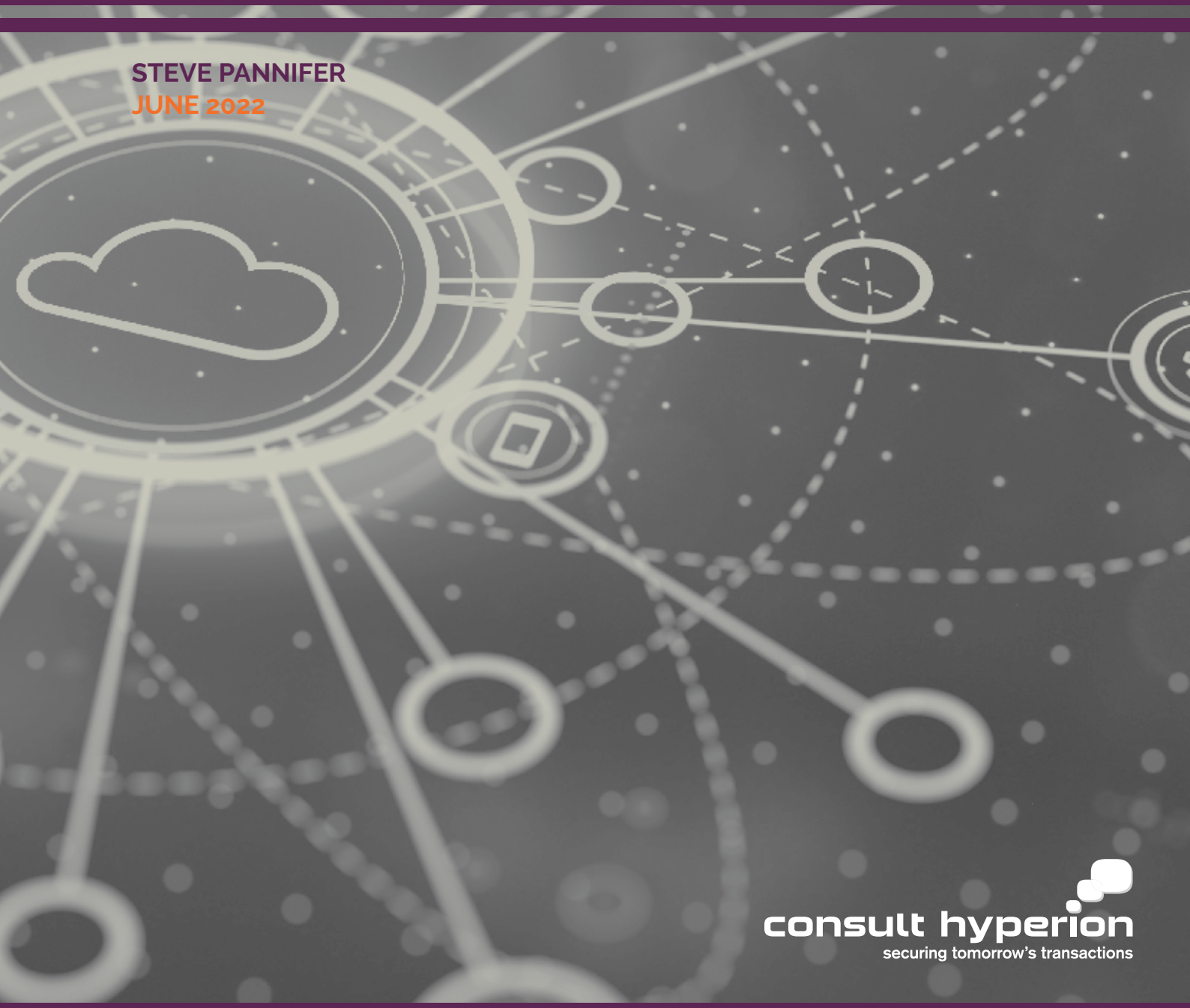
Data: The Key to Inclusive Digital Identity

STEVE PANNIFER

JUNE 2022



consult hyperion
securing tomorrow's transactions

EXECUTIVE SUMMARY

Identity checks are important but often become a barrier for people wishing to legitimately access digital services. Sometimes people get put off by the inconvenience of these checks. Of more concern, some people are not able to complete identity checks because either they do not possess the right documents or because they do not have a sufficiently complete credit file. These people can then find themselves excluded from essential digital services.

This paper considers the issues that face many regulated and high value services is finding an optimal way to check the identity of customers. These issues affect financial services, insurance, car rental, online gambling and more besides. The paper explains why current identity checks often fail and shows how through alternative data sources and emerging digital identity solutions will help address these pain points – both improving the customer experience and reducing fraud.

The "Maximising your chances of success" section provides practical step-by-step guidance on what you should do to address these issues in your service – enabling you to reach more customers and reduce the cost of expensive manual fallback solutions.

The paper concludes that the traditional approaches to identity checks are not good enough for the digital world where customers demand speed, simplicity, transparency and inclusion.

It is imperative that potential users of emerging identity solutions engage with both industry and the government to ensure that the solutions delivered meet the needs of business, enabling them to provide simpler, more inclusive and more secure services to their end-customers.

The trust framework being created by the UK government provides an opportunity to bring such solutions to market within a cohesive network through independent and structured certification. As with many government initiatives, it will only work to facilitate change if those affected hear the call to action and work together to build joined-up transformation.

THE NEED FOR INCLUSIVE DIGITAL IDENTITY

Sub-optimal processes

Digital services continue to be seriously hampered by sub-optimal digital identity solutions. The solutions that do exist often fall short on user experience, accessibility or security. Customers end up being confused, losing confidence or worse still being excluded from digital services altogether. This is bad for customers and bad for business.

Part of the problem is that customers are required to go through essentially the same identity checks for each service that they sign up to. The same information is handed over and the same checks performed by every service provider. There is massive duplication of effort with no real benefit to either the customer or the service provider. It is like asking customers to have a different payment card for every site that they wish to shop at. Not only is it inefficient, but this duplication also increases the risk of fraud – with data more likely to be leaked or phished and used by fraudsters to open accounts.

These issues are most prominent in regulated services such as financial services, insurance, online gambling but can impact many other areas such as employment, housing and health – any sector or service where there is a need to ensure that the identity of the customer is verified.

Application abandonment

One recent study[1] suggests that two of the main reasons that customers abandon applications for financial products are a cumbersome process and being asked for too much information. Of course, identity checks cannot be completed without asking customers to share personal information. And whilst most customers will not understand the finer points of AML regulation, most will appreciate the need for identity checks to prevent fraud. So, the problem is not the need for identity checks but the way that they are being done.

Inclusion issues

Today many digital identity solutions rely on evidence that is linked to economic activity. This creates a viscous cycle of exclusion. Without access to financial services people cannot build the history that is required to gain access to those services in the first place. The number of people that this affects is not small. In its recent study[2], OIX estimated that there are as many as 5.9 million people in the UK who are "ID challenged" – people who for a variety of reasons cannot get through typical identity checks and are therefore excluded from the financial services that they need.

There is therefore a pressing need for inclusive identity solutions that are clear, simple and trustworthy.

1 Signicat Battle to Onboard 2022
2 https://openidentityexchange.org/networks/87/item.html?id=498

WHY IS DIGITAL IDENTITY NOT ALWAYS INCLUSIVE?

UK context

In the UK, the tools we currently have for undertaking identity checks directly affect how difficult it can be for some people to prove their identity when needing to access digital services. The same issues exist when accessing physical services but are more pronounced in the digital world where customers often are left to figure out what to do by themselves.

Many other countries maintain a national identity register, providing a single list of all citizens that can be referenced directly or indirectly when onboarding to services. Whilst not the whole solution, such registers can provide a foundation for universally accessible digital identity solutions. However, no such register exists or is likely to exist in the UK in the foreseeable future – due to the UK's values, culture and politics.

The UK does have registers which have defined purposes, but they are not universal in the same way that national registers are. The national insurance number, for example, is primarily used in the administration of social security and for a limited number of tax-related purposes. The NHS number, on the other hand, is used to access health services in England and Wales – and equivalent but different numbers are used in Scotland and Northern Ireland. These numbers cannot be used outside of their defined purposes, such as in the opening of a bank account.

Instead, in the UK, identity has to be checked through a process of "triangulation". Evidence from enough sources needs to be compared so that the identity can be inferred. The more evidence that is checked, the more likely it is a real legitimate identity and the harder it is for a fraudster to fool the system. Those evidence sources come in the form of documents or data.

CASE STUDY

As financial services become increasingly digital, it is becoming more difficult for some communities and groups to access financial services. OneBanks is addressing this by providing in-person access to everyday banking on behalf of all banks in communities where branches continue to close. They provide pop-up kiosks where people can access cash based services (e.g. deposits, withdrawals and bill payments) and get support getting onto online banking with fully trained staff on hand to provide help as required. Even with this help getting access to online banking is not always straightforward.

Up to 30% of people who turn up to a OneBanks kiosk to onboard are unable to complete the typical identification processes employed in online banking services – whether to open a bank account or set up online access to an account the customer already has. This is due to these digital services placing a heavy reliance on documents such as passports, which many OneBanks' customers do not have. Whilst passports or driving licences are fine for many people they often do not work for the financially excluded. Instead these customers are forced to go through more cumbersome manual identification processes, perhaps requiring a bank branch in another town. For a person who is disabled or on a low income, this can be a significant barrier.

Identification processes that leverage a wider range of data sources, and address the gaps in credit bureau data, will enable OneBanks to help its customers to onboard to online banking more easily and access the financial services that many people take for granted.

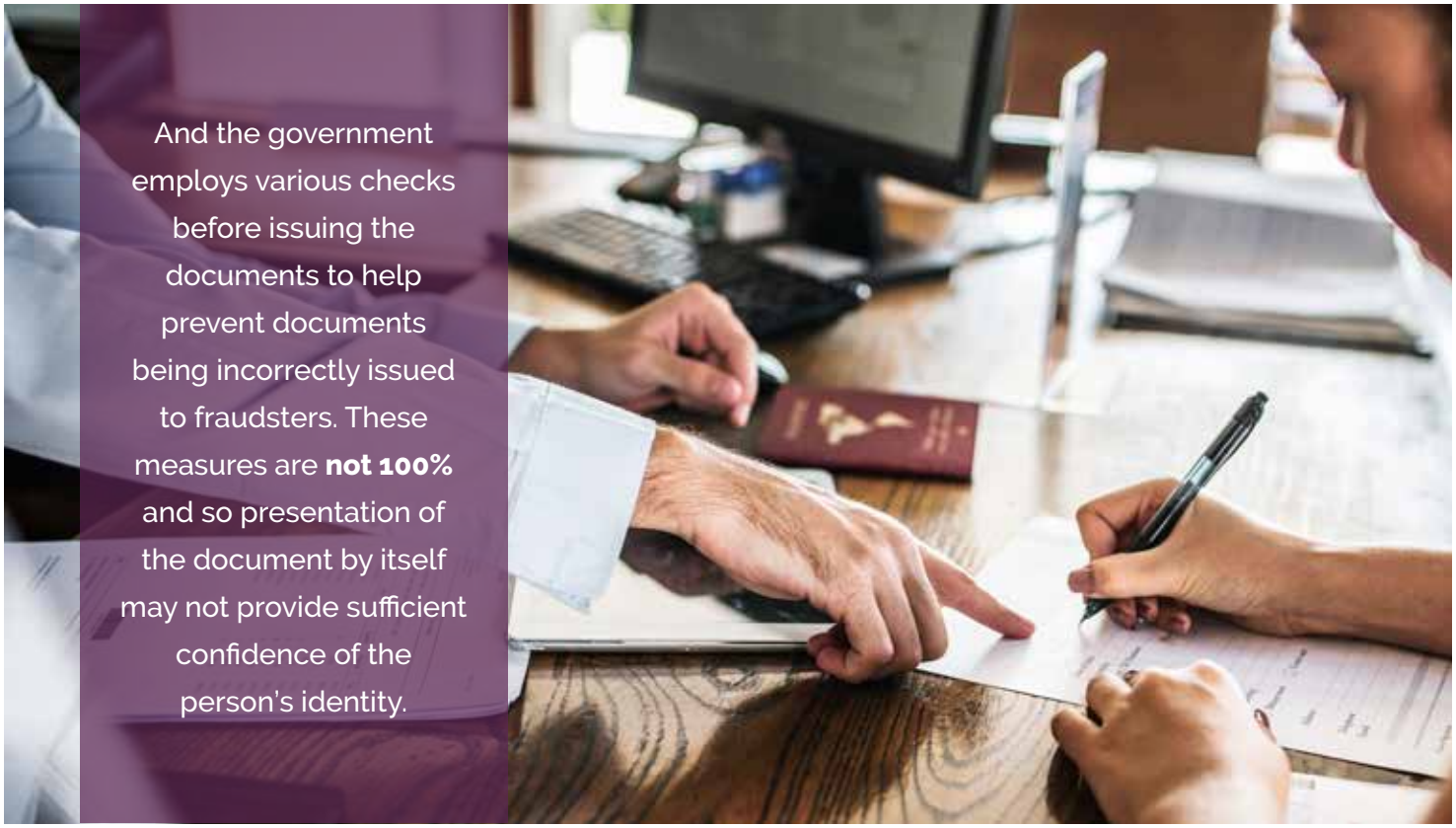
OVER RELIANCE ON FINANCIAL DATA

The most common documents used are passports and driving licences. These are not identity documents per se but are used as a good indicator of someone's identity. The physical documents themselves contain security features making them harder to alter or forge. And the government employs various checks before issuing the documents to help prevent documents being incorrectly issued to fraudsters. These measures are not 100% and so presentation of the document by itself may not provide sufficient confidence of the person's identity.

The most commonly used data is held by the credit reference agencies. These organisations maintain pools of data, recording credit-related financial history – taking out a loan, getting a credit card, obtaining a mobile subscription (post-paid) contract and so on.

The problem is that neither of these document or data sources have universal coverage. Far more from it:

- The most recent figures available from the electoral commission[3] suggest at 24% of the electorate have neither a passport nor photographic driving licence.
- Over 5 million people have insufficient credit file history for it to be a suitable evidence source for them in an identity check[4].



3 https://www.electoralcommission.org.uk/sites/default/files/pdf_file/Proof-of-identity-scheme-updated-March-2016.pdf
4 https://www.experianplc.com/media/latest-news/2022/meet-the-5-million-credit-invisible-brits-still-at-risk-of-exclusion-from-the-financial-system/

MANY ALTERNATIVE EVIDENCE SOURCES HAVE ISSUES

The only way to address the gaps in current digital identity solutions is find alternative evidence sources that fill the major gaps that exist today. Typically, this means finding new data sources and several have been proposed over the years.

Social media data

Social media has often been touted as an alternative source of identity evidence. The data is of course all self-asserted with no formal checks being performed and often deliberately wrong – on some platforms people use variants of their names in an attempt to protect their privacy.

However, by looking at what people post and who they are connected with (their social graph) it is often possible to infer a person's real identity. And when a social media account has been active over an extended period of time, especially when combined with ongoing interactions with a network of other users, some degree of confidence can be placed in the inferred identity.

Social data does have its issues, however. There is the obvious issue of privacy concerns around the platforms and the sustainability of the business models which are still heavily reliant on targeted advertising. It is unclear how well social data can plug the gaps that exist in current identity solutions. Some of the groups not well served by existing identity solutions will also make lower use of social networks.

Last but not least, there is no recognised methods to measure the quality (or assurance) of the identities inferred from social data. This is why several providers of identity solutions based on social data have ended up pivoting back towards more conventional methods of identity verification, retaining social data as an additional risk-based input to the process but not being the foundation of the process itself.

Public sector data

To date public sector data has not been available to use as a source of identity evidence in the private sector. This is changing as the government looks to open up access to passport data . Whilst this is welcome it will not help excluded people who do not possess either of these documents. But there are other public sector data sources that could help.

Local authorities are a potentially valuable source of identity evidence. They hold a lot of data relating the people that they serve for things like council tax, concessionary travel passes, housing benefit, parking permits and so on. Though, the quality of data varies depending on the data type.

Stronger identity checks are performed for housing benefit than for the electoral roll for example. A study undertaken by the Electoral Commission in 2019 suggests that electoral registers are only 85% complete and 89% accurate. Coverage will vary too, with many of the services (e.g. concessionary travel, blue badges) only being applicable to certain groups within the community.

5 https://www.gov.uk/guidance/apply-for-the-document-checking-service-pilot-scheme
6 https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/our-views-and-research/our-research/accuracy-and-completeness-electoral-registers/2019-report-accuracy-and-completeness-2018-electoral-registers-great-britain

It is likely to some extent that there is a correlation between people who lack conventional identity evidence and people who obtain assistance from their local authority.

The primary issue with local authorities is the sheer number of them. There are 333 local authorities in England made up of 5 different types[7]. The only practical and meaningful way to leverage their data will be in an aggregated form, such as that provided by the NFI[8].

Another issue is that some data sources may have legal limitations on their use, making it more difficult to extend their use. In 2015, for example, the Scottish Government proposed extending the use of the Scottish NHS Central Register to support identity verification which it had to abandon after the consultation process[9]. This does not mean that data sources cannot be used, but that care should be taken. NFI data is already used in the private sector for fraud prevention, for example[10].

Vouching

Where a person is unable to provide sufficient evidence of their identity, another alternative could be for someone else to vouch for that person's identity. For example, the person may be known to a doctor, social worker or other professional. The goal would be able to create and store a verifiable digital version of the "vouch" that acts as the evidence of the person's identity. The process would need to be controlled to ensure that the "voucher" is sure of who they are vouching for. And the voucher may need to use a digital identity of their own, perhaps a professional digital identity that includes information showing that the voucher is qualified to undertake the task.

Vouching has some benefits – it will likely be something people are familiar with and if done face-to-face it may allow for additional support to be provided to people who lack confidence with digital technology. But there are also challenges. Firstly, vouching introduces friction and inconvenience into the identity checking process, especially where the person is required to make a vouching appointment and then travel to meet the voucher. And equally as important, no network of vouchers currently exists and creating one will take time.

Ensuring consistency across the network may be challenging or expensive if there is a need for training, certification and monitoring. Funding may also be a challenge – according to NHS England each GP appointment costs on average £30, so it is reasonable to think that an appointment to obtain a vouch would have a similar cost. Vouchers will need to be paid, but charging individuals for the service will be wrong. That would exclude the people who would need to use a vouching service the most.

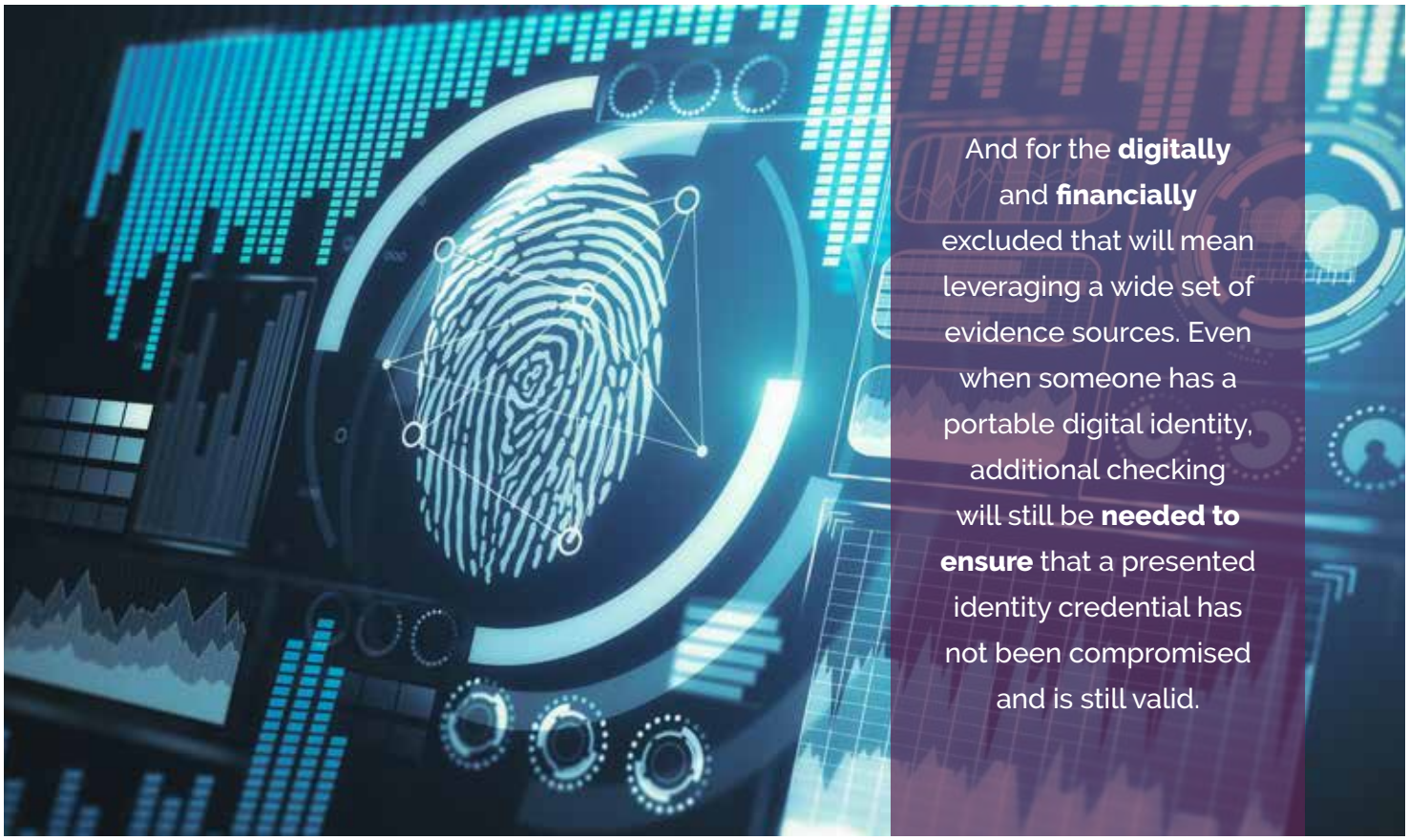
7 https://www.gov.uk/guidance/local-government-structure-and-elections#:~:text=In%20total%20there%20are%20333,district%20councils
8 https://www.gov.uk/government/collections/national-fraud-initiative
9 https://www.parliament.scot/chamber-and-committees/written-questions-and-answers/question?ref=S5W-07384
10 https://www.synectics-solutions.com/our-thinking/qbe-insurance-group-wins-claims-initiative-of-the-year-at-the-british-insurance-awards

Portable digital identities – the future?

In the future portable, re-usable digital identities may allow people to seamlessly access the services that they need. At least that is something that the UK government is seeking to enable through its identity and attribute framework . The UK is not alone in this regard. Re-usable digital identities already have widespread adoption in certain European markets . And in Europe and elsewhere, decentralised identity solutions are being developed whereby people will have digital wallets that they use to store and present their "identity credentials".

These will however not do away with the need for data. To issue a portable digital identity in the first place, it will be necessary to have documents and data that triangulate the person's identity. And for the digitally and financially excluded that will mean leveraging a wide set of evidence sources. Even when someone has a portable digital identity, additional checking will still be needed to ensure that a presented identity credential has not been compromised and is still valid.

What portable digital identities should do is reduce friction and improve security, enabling people to access digital services with confidence and ease. This will be good for customers and good for business.



11 https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version/uk-digital-identity-and-attributes-trust-framework-alpha-version-2
12 E.g. Bank and mobile operator led schemes in the Nordic countries and Belgium

MAXIMISING YOUR CHANCES OF SUCCESS

Building a digital identity solution is easy. Building a digital identity solution that works for all customers is much harder. The conventional documents and datasets used for identity verification only get you so far. To ensure good coverage of the UK adult population it is necessary to leverage a complex patchwork of datasets of varying quality.

What can you do to maximise the chance of success?

STEP 1: Obtain high quality data sources and lots of them

The first step is to obtain high quality data sources that can be used to help triangulate the identity of your customers. The OIX report identified 11 potential sources of data. Most of these are public sector data sources including health, education, local authority and other data. A number of these are also included as part of the NFI data set.

There may be other sources in the private sector that can be leveraged to maximise the coverage of your customers such as mobile operator data and utility data.

STEP 2: Understand the processes that sit behind the data

Data sources exist as a result of services being offered to consumers. Each of these services will have their own policies and processes regarding the identity checks that they perform on their customers. Some will need to comply with strict legal requirements, others will be based on the business needs and risks to the service concerned.

The level of reliance you can place on any particular data source will be determined by the policies and processes of the source organisation. It is therefore essential that you understand the checks and balances in place at the source. For regulated organisations this will be easier, as the regulation itself or associated guidance[13] will indicate the level of identity checks that can be expected.

For aggregated sources, such as syndicated databases, you will need to understand the provenance of the inputs to the aggregated source.

STEP 3: Build sophisticated business rules

To maximise the chance of success, you need to ensure that you are able to choose the right data sources for the customer in question. To do that it will be necessary to have flexible business, taking into consideration the different possible ways to achieve the desired outcome.

13 Such as the AML/KYC guidance published by the JMLSG

Identity verification guidelines, such as the UK Government's GPG45[14] and the JMLSG guidelines[15], support different ways to check a person's identity. GPG45 defines a number of profiles which describe different ways of combining data sources to achieve a level of assurance. The JMLSG guidelines, in line with AML regulation, require reporting entities[16] to take a risk-based approach.

Consistency across data sources will likely be an issue. Differences may exist for a variety of reasons. Data may have been entered incorrectly in the first place. Formats of names and addresses can vary. And sometimes the same person can have two legitimate versions of their data, e.g. if their name is in the process of being changed or if they have recently moved address. The business rules need to take account of potential consistency issues recognising that such differences can also be a sign that something untoward is going on.

STEP 4: Design a forgiving process

Last but not least, the process as presented to the customer must be simple to use but also flexible to support different types of customer – not assuming a particular identity verification journey but at the same time communicating clearly what the customer will be asked for and why.

14 https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual
15 https://www.jmlsg.org.uk/guidance/current-guidance/
16 Financial institutions and other organisations that call under AML regulation

GETTING IT RIGHT

As well as building digital identity solutions that work for customers, there are some important supporting considerations.

You must obviously comply with data protection regulations. This will include, but not be limited to, ensuring a proper basis for collecting and processing data. A trusted digital identity system may need to go further, for example by providing assurances that the data will not be exploited against the wishes of end users.

Data governance and the commercial model go hand-in-hand – the commercial model must support and incentivise responsible use of data. Too often in the digital world, the commercials incentivise behaviour that is detrimental to end users.

Another key concern is the prevention of fraud. Identity theft has long been a vector for fraud in financial services. As the utility of digital identity increases, it is inevitable that organised crime will target digital identity systems. This includes creating networks of synthetic identities – highly realistic but fake identities that are manufactured by criminals using combinations of real and false data.

Fraud intelligence sharing platforms are a critical defence against this criminal activity, allowing participants to signal when a digital identity is suspected to be fraudulent and to monitor for behaviour across services that could indicate fraud.

A CALL TO ACTION

Digital services in the UK have been significantly hampered by sub-optimal digital identity solutions that are cumbersome to use and exclude many people. New solutions that leverage wide datasets beyond the traditional credit bureau data combined with advanced portable digital identities provide a route to address these problems. The trust framework being created by the UK government will help further by enabling those new solutions to be independently certified.

It is imperative that potential users of these new identity solutions – any regulated or high value digital service – engage with both the industry and the government within the UK to ensure that the solutions delivered meet the needs of business, enabling them to provide simpler, more inclusive and more secure services to their end-customers.

consult hyperion
securing tomorrow's transactions

Head Office: Consult Hyperion | Tweed House | 12 The Mount | Guildford | Surrey GU2 4HN | UK
US Office: CHYP USA Inc, a Consult Hyperion company | 234 5th Ave | New York | NY 10001