Digital Identity in the UK:
The cost of doing nothing

Innovate Identity

April 2018

Contents

Executive Summary

Improved digital identity solutions could solve numerous identity challenges across a range of industries. Sectors as diverse as healthcare, banking, the sharing economy, gambling and air travel all suffer from a common problem - it is difficult to remotely identify a customer, with confidence, as is required online. Many identity checking processes still rely on physical documents, more traditional proofs of age or entitlement, or digital workarounds in the absence of access to the trusted attribute data necessary to build effective digital identity solutions. This creates unnecessary friction for customers, and costs for businesses.

There remain a number of legal, regulatory and operational challenges facing the application of any digital identity scheme. The way the European Fourth Money Laundering Directive has been interpreted in the UK, banks need to keep a clear record of how they have verified a customer - in a way that some identity schemes could not easily provide. Data protection law, payments regulation and new initiatives make the UK's identity ecosystem a dynamic space:

- Data Protection regulations are set to significantly change how personal data is used
- Open Banking is revolutionising how personal financial data can be shared with the customer's consent
- Payment regulation will set more stringent rules for establishing identity for electronic transactions
- New Anti-Money Laundering legislation will require stronger checks on customers, and significantly increase the fines for firms that fall foul of the rules.

The UK's identity solutions are currently lacking. Many fintech businesses and private sector companies are delivering innovative but tactical identity solutions, and the GOV.UK Verify scheme exists in the public sector, yet none of these provide a universal digital identity solution. The UK is amongst an ever-smaller group of developed nations without a national digital identity infrastructure. The UK has few identity standards, and the market remains fragmented.

Identity fraud is projected to rise substantially, with a cost of £billions. Identity fraud is fast growing in the UK, having increased by 50% to record levels over the last three years alone, with most of this activity taking place online. If identity fraud continues to rise at the current rate, the cost to the UK in 2021 could be as much as £8billion directly related to identity fraud alone.

Digital identity is a potentially multiplier of future economic value. Digital identity schemes can enable the development of new products and services, as well as reducing operational costs for relying parties. The potential value to the UK economy of utilising smart technology, including digital identity, has been estimated to be as high as £58billion by 2020.

The costs of continued inaction are projected to far outweigh the likely cost of delivering solutions. The potential benefits via fraud reduction alone run to multiple £billions / year. When balancing the potential value creation and efficiency savings a scheme might deliver, against the likely development costs (based on international examples), the economic balance lies heavily in favour of seeking improved identity solutions.

Further research is needed to understand costs, and potential scheme models. It is clear that the understanding of current identity costs and how they may be displaced or eliminated by digital identity, amongst a range of industries, is patchy at best. Without a clearer view of existing costs, scheme development costs, and potential future value, decision makers will not have access to the data they need to consider a course of action.

International experience can provide insight, and a number of successful examples to learn from. There is no challenge faced in the UK in developing a digital identity solution that has not been faced, and successfully overcome, in one of the 60+ counties around the world where a scheme has been launched. Whether considering trust frameworks, commercial models or technical scheme architecture, the UK can learn from success elsewhere, as well as from the considerable lessons from our own domestic experience.

Recommendations

If the cost of inaction proves too great, successful practice elsewhere points to the following recommendations:

1 Engage widely

A multi-sector approach, with a wide range of identity uses, is a key factor in any scheme's success. A narrow approach would limit efficiencies of scale seen in other successful examples.

2 Explore the economics and trust arrangements

There remains insufficient analysis undertaken, or shared across sectors, of the potential future value of a scheme, nor detailed discussion of the crucial liability and trust arrangements.

3 Agree a range of use cases and their requirements

Wide and frequent utility is vital for a scheme to succeed - customer convenience is key. Potential uses, and the data and authentication level required, need to be mapped and agreed.

4 Banks to engage fully in the discussions

In successful international examples, the banking industry has played a key role in both developing and utilising schemes. In the UK banks have yet to assume a leading role.

5 Government and regulators to facilitate, not lead

There are international government-led schemes, but more often the role played by government and regulators is as public/private partner, or as facilitator or standard setter.

6 If all else fails, consider a regulatory stimulus

Given the compelling economic case for a digital identity solution to be developed, if the private sector is unwilling to develop a scheme, a regulatory catalyst may be required.

1 Digital Identity in the UK

Introduction

The relatively under-developed digital identity ecosystem in the UK has been the topic of a long and increasingly frustrated discussion. In recent times that conversation has grown more involved, and across a wide range of sectors and industries - whether in banking and insurance, air travel, health, welfare distribution, mobile and telecoms, or online gambling. The question of digital identity, and how to develop more effective solutions, is growing ever more acute.

Customers expect privacy, security and convenience when they are online. Yet despite the fast development of the digital economy in other ways, a more complete identity solution remains elusive. Without a better way to prove identity online, the regulatory controls needed to provide security and privacy will inevitably create friction for customers and service providers alike.

The technical methods of digitally verifying a user's identity have been studied at length. But in considering whether to pursue the options, what often remains poorly understood by both industry and Government is the potentially high cost of doing nothing.

> *"There is a great deal of focus on the potential cost involved in developing a digital identity scheme in the UK. However, I believe the costs of inaction will prove to be far greater."*
>
> Don Thibeau, Chairman, Open Identity Exchange

Objectives

The aim of this white paper is to give senior stakeholders and decision makers - and those that brief and advise them - the insight and tools needed to engage in a more informed digital identity conversation. It sets out the potential costs of inaction, identifies the drivers shaping future identity needs, and draws on international experience to begin to explore potential solutions if the cost of inaction proves too great to bear.

What is digital identity?

A digital identity is a set of personally identifiable data which can be used by a relying party to establish who an entity is. Establishing a person's identity has traditionally been achieved with passports, driving licenses and in-person checks; digitally this is more challenging.

Confirming a person's identity to a given level of confidence (the 'level of assurance') is necessary for many activities. For example, the level of authentication needed in order for someone to gain access to a website will differ from that needed for them to make a payment, or to buy a house. In addition, to gain access to digital services usually requires not only that an individual's identity is established, but also that a number of the person's attributes (e.g. age, address, credit rating, or legal residency status) be provided to the relying party, whether for them to carry out a risk-based assessment, or to demonstrate entitlement.

What is a digital identity scheme?

A digital identity scheme is an agreement between organisations that enables an individual to 'unlock' the attributes needed to be shared with a third party, to then access a product or service. A scheme allows an individual to assert their identity sufficiently for their attributes to be made available by the organisations that hold the data. The more sensitive the data, the greater the initial confidence in the individual's identity needed for the holding organisation to be able to share it. This is undertaken within an agreed framework of rules and standards.

The Identity Challenge

The challenge of establishing identities with confidence, particularly online, is felt across a wide range of sectors:

Financial services

Banks and building societies, as well as pension and insurance providers, all have stringent identity and personal data requirements - often known as the ‘Know Your Customer’ (KYC) requirements. Whether opening a bank account, switching accounts, taking out life insurance or accessing pension records, a customer’s identity and a number of attributes are required to be gathered and verified as part of a firm’s risk-based assessment and legal obligations.

Airlines and travel

International travel, particularly air travel, has stringent identity and security requirements. Air travel is expected to grow rapidly over the next two decades, driving the industry to streamline processes. The collection and verification of passenger information is a significant point of friction for passengers and operators alike, and new identity solutions are being explored.

Public services

When members of the public wish to access a number of government services, they must be able to assert who they are, and with varying levels of detail and confidence. This may be simply to log onto a government website, to file a tax return, or to change their driving licence details. Online access to government services requires digital identity solutions, and a number exist across departments, but each with limited interoperability or utility elsewhere.

Health

Of all public service uses, identity in healthcare is a particular challenge. The increasing trend towards accessing online healthcare services, such as healthcare files, ordering a prescription, registering with a practice or merely engaging in a support group, gives rise to a variety of digital identity requirements, with stringent security standards required.

Gambling

Online gambling sites and casinos have a number of rules regarding the due diligence that they must undertake before access, such as establishing proof of age and identity, and controls to prevent money laundering or financial crime.

Age restricted activities

There are other day to day activities that require proof of age or identity to be given, either in person and increasingly online - one of the most common is to purchase age restricted goods, for example for a customer to prove they are 18 when purchasing alcohol. Digital identity schemes can help to solve ‘low level’ but frequent points of friction, such as age verification.

Sharing Economy

A fast-growing sector, the Sharing Economy is based on peer-to-peer transactions, often involving renting something not in use (such as the AirBnB model), social enterprises such as car sharing schemes, or even internet dating. In each case it is necessary to identify the people or organisations digitally prior to a transaction to establish a degree of trust and find out whether they have been vetted to ensure security and provide customer confidence.

Legislative and Regulatory Drivers

Regulation	Date of Implementation
Electronic Identification and Trust Services (eIDAS)	July 2016
EU Payment Account Directive (PAD)	August 2016
EU 4th Money Laundering Directive (4MLD)	June 2017
Second Payment Services Directive (PSD2)	January 2018
Open Banking	January 2018
General Data Protection Regulations (GDPR)	May 2018
EU 5th Money Laundering Directive (5MLD)	2019/2020
PSD2 Strong Customer Authentication (SCA)	H2 2019
Trusted KYC Data Sharing for SMEs	2020

eIDAS

eIDAS provides a common and robust set of standards, which enable digital identities and signatures to be relied upon across national boundaries to specific, pre-determined levels of authentication. However eIDAS is focused only on allowing access to public services at present.

PAD

By requiring banks to extend their services to legally resident customers applying from elsewhere in the EU, PAD exposed the international and digital limitations of banks' current onboarding processes. It highlighted the growing need for banks to remotely identify individuals and organisations securely and with confidence, wherever they may be located.

4MLD

4MLD introduced higher levels of security and customer due diligence required of a wider range of organisations, introduced the recognition of electronic signatures, and raised the fines that can be applied to firms. These factors are pushing organisations to explore new identity processes, in order to keep abreast of their 4MLD obligations in a more efficient way.

PSD2

As well as introducing changes to payment and data sharing regulation, PSD2 crucially introduces several requirements concerning increased identity and authentication checks, via the Technical Standards on Strong Customer Authentication (see below).

GDPR

GDPR is designed to enable individuals to exert more control over their personal data, how it is used or shared, and with whom, and sets out significantly higher fines for any transgressions.

5MLD

As well as strengthening the core provisions introduced by the previous directive, 5MLD will amend the rules to allow organisations to accept digital identities under simplified Customer Due Diligence rules, provided they are derived from eIDAS-notified national identity schemes, or from national schemes recognised by the national regulator.

SCA

A delayed element of PSD2, the Strong Customer Authentication Technical Standards will in 2019 introduce several measures concerning increased identity and authentication checks required for online payments, requiring payment providers to find new identity authentication processes.

Drivers from industry

Legislation directly impacts firms, whether in the form of revised payment regulations for banks, or entirely new regimes affecting sectors such as online gambling, now caught under 4MLD. Alongside this a number of industry initiatives are also shaping identity. Some of these have been prompted by regulators such as the Competition and Market Authority (CMA), Financial Conduct Authority (FCA) and the Payment Services Regulator (PSR). Other drivers are coming more directly from industry, such as via the recommendations of the Payment Strategy Forum (PSF), or the development of the global air industry's OneID initiative.

Open Banking

As part of the wide-ranging remedies following its inquiry into competition in the retail banking sector, the CMA introduced 'Open Banking'. In part built on the PSD2 legislation, the Order required the nine biggest UK banks to allow registered organisations direct access to a range of information. This includes 'static' data such as ATM locations and branch opening, as well as access to their customers' data, where the customer explicitly agrees, down to the level of individual products and transactions. An Open Data environment has been created via the use of common API standards.

The Open Banking initiative has required banks to create a data sharing topology that could be extended to other customer attributes. An open data environment that includes the sharing of a customer's KYC data would facilitate a much wider range of identity solutions.

Trusted KYC Data Sharing for SMEs

In addition to a range of payment and fraud initiatives, including some highly innovative proposals, the industry representatives that made up the PSF recommended that banks develop a bank-to-bank trusted KYC data sharing solution. This is intended to ease the friction suffered by SMEs when they seek to satisfy a bank's KYC process, whether opening a new product or service, or switching accounts. This friction has been identified by the CMA as a significant issue affecting competition in the market.

The recommendation requires banks to agree a framework to allow for trusted KYC data relating to SMEs to be exchanged between banks, under the consent of the customer. UK Finance has been tasked with arranging the delivery of the recommendation, which would see the creation of an identity and KYC scheme, albeit potentially limited to banks as relying parties and attribute providers, and only extending to SME data.

If a bank-to-bank KYC data sharing project is delivered in some form it will create the skeleton framework required for the sharing of personal attribute data, and thereby digital identity solutions. Given the significant interest of the PSR in progressing the recommendation, significant future developments are becoming more likely, at least as related to SMEs.

Identity and Air Travel: IATA's One ID Programme

The One ID programme, led by the International Air Transport Association (IATA), aims to reduce repetitive identity checks and create a more seamless flow for passengers, while maintaining high privacy and security standards. One ID pilot projects are exploring robust, integrated identity management solutions for airports and border control. For instance, the scheme introduced at Aruba Airport is based on self-enrolled, tokenised facial recognition technology, delivering an end-to-end passenger identity solution for the airport.

2 Inertia in the UK

The importance of identity

Establishing an organisation or person’s identity is critical in order to carry out a wide range of day to day activities - be that making a payment, checking in to travel, or accessing a government service. If establishing identity digitally is not possible securely, quickly, at the control of the individual, and in an efficient and controlled way, friction will result in a poorer customer experience, operational inefficiency, and regulatory challenges.

As a result, there has been widespread international development of digital identity schemes. But while over 60 countries around the world have developed or are close to launching a digital identity scheme, digital identity developments in the UK have been more limited.

We have seen the Government’s own identity scheme GOV.UK Verify emerge, but it has yet to reach the wide-spread adoption it was targeting. Private sector solutions are in the market, but none can claim to have universal use, and many struggle to satisfy more heavily regulated identity requirements.

What are the reasons behind this apparent inertia? Let us consider developments in the public and private sectors, and the existing barriers that may be holding back new initiatives.

A public sector identity solution?

GOV.UK VERIFY

The Government Digital Service (GDS) has led the development of a digital identity scheme in the UK, GOV.UK Verify. The resulting digital identities enable individuals to assert who they are when seeking to access certain public services. The standards are robust and are aligned to Authentication Level 2 (LoA2) in the European eIDAS framework, which equates to or exceeds the level of confidence commonly required by banks[i]. The scheme provides relying parties with four attributes - name, address, date of birth and gender[ii].

Public sector limitations

Despite significant funding and a number of years in development and roll-out, the GOV.UK Verify scheme has so far fallen short of the targets GDS originally agreed.

Low levels of public adoption **-** Take-up by the public has been below target, with less than 2 million identities created to the end of 2017. Access issues, a lack of public recognition and a challenging customer journey all played a part, alongside the limited range of use cases.

- Target of 4.4 million users by March 2017
- Target of 25 million users by April 2020
- **Fewer than 2 million users by February 2018**

Limited utility - Slow take-up and low levels of identity re-use have been caused in part by the limited adoption by government departments, which have yet to move away from their own native solutions.

- In 2014, GDS expected over 100 departmental services to be using GOV.UK Verify by 2016
- In October 2016, GDS predicted that 43 services would be using GOV.UK Verify by April 2018
- **In February 2017, just 12 services were using GOV.UK Verify, and fewer than 20 services by February 2018[iii]**

Public sector-only uses - The Verify scheme has yet to be adopted by the private sector. Use by the financial sector is perceived to be challenging in the scheme's current form, due to the banks' interpretation of their AML requirements.

- Wide engagement and research into other potential industry uses for GOV.UK Verify
- **0 private sector uses as of February 2018**

Private sector identity solutions?

There continue to be a number of private sector identity solutions available in the UK, many developed by fintech organisations. However, while a few might claim to be true identity solutions, many represent narrower, more focused solutions intended for particular uses. They are commonly based on scanned documents and on access to publicly available registries and databases, often combined with biometric and facial recognition technologies. Many are also sector-focused, and only a minority have international coverage.

TISA Digital Identity Project

Working closely with Experian, TISA is developing a digital identity scheme to enable the onboarding of customers onto savings products, initially by their 160+ member organisations.

The scheme will enable customers to create an identity which can then be relied upon by an organisation when the customer seeks to open a savings account with them. By so doing it aims to reduce customer friction and the time taken to open a product. The identity is authenticated to a level sufficient for an organisation to satisfy their AML and KYC obligations for onboarding to a savings product.

Private sector limitations

The growing market for identity and attribute products demonstrates an underlying demand for improved online identity solutions, for both individuals and organisations. However, private sector identity services continue to share some common limitations, some of which are particularly important factors when considered for use by more heavily regulated industries:

***Little interoperability and few common standards* -** There is limited interoperability between the various schemes in the market, and very few national or international standards within which they can operate. Some progress is being made - eIDAS begins to provide an international framework but to a limit degree of granularity, while the BSI's work to develop a digital identification and authentication code of practice ('BSI PAS 499') is a promising initiative.

***Reliance on contextual data sources* -** Many private sector solutions rely on contextual information (often in the form of high-volume, low-authentication data from non-regulated sources) that many regulated organisations would not traditionally rely upon for identity purposes. While such methods can provide a great deal of statistical confidence in validating an identity, 'soft' data derived from non-regulated sources is not yet widely accepted as being sufficiently robust by regulated industries, at least as primary data for their KYC purposes.

No access to restricted Government databases or trusted attribute data - Private sector schemes commonly lack a facility to access and validate identity attributes against key pubic databases, such as Passport Office or DVLA data (which is accessible for GOV.UK Verify Identity Providers). Until regulated industries such as banking are willing or able to place greater reliance on contextual data, their failure to find a way to share existing trusted identity and KYC data more widely will remain a crucial, and as yet unresolved issue.

Barriers to Digital Identity

Trusted attributes are not being shared

The provision of only four attributes by GOV.UK Verify, even at LoA2, can alone only satisfy a small part of the data needs that many uses would require. A key issue for any identity scheme is that of attribute availability, or rather the current lack of it. There is no arrangement in place between the potential attribute providers and relying parties to enable individuals to put the KYC data held about them to wider use. A GOV.UK Verify identity may in future be used to 'unlock' wider KYC data held about an individual for wider sharing, but Verify IDs are not in themselves a 'standalone' solution.

Regulatory barriers

The participation of banks is often seen as central to the success of digital identity schemes. Yet UK banks point to regulatory barriers that need to be addressed for them to use a digital identity. The provisions of 4MLD and previous Directives are perceived to have created regulatory and possibly legal barriers to digital identity use, given the manner they have been interpreted in the UK, and in subsequent industry guidance.

Liability questions

The complexity of agreeing liability arrangements or a trust framework remains an often-cited challenge to the development of a solution. Without liability outcomes being explored in more detail, the commercial model for a wider digital identity scheme will remain elusive, albeit that solutions have been found in a wide range of international contexts.

Little public understanding of personal data issues

Despite Open Banking and GDPR putting individuals in control of their personal data and enabling a range of new uses for that data, customer understanding of the new personal data environment and how it affects them remains very limited. This may improve over time; however public education remains an issue to be addressed.

Public ID concerns

The failed and costly UK initiative to develop a national identity card scheme a decade ago is still reflected in an ongoing public distrust of national identity initiatives. Together with rising social concerns regarding data privacy and security, unless addressed, public reticence could create a strong cultural barrier to future digital identity take-up.

No clarity on costs and savings

There remains very little robust or detailed research into the potential costs, savings, or operational impacts of potential digital identity solutions, nor of the costs or benefits of ongoing inaction.

Lack of transparent standards or guidance

For identity solutions already in the market, there are few identity standards for providers to work towards, whether internationally, or specifically covering the UK identity market. The lack of standards limits interoperability. This could further limit the positive impact expected of 5MLD while there remains no UK identity scheme formally notified under eIDAS, nor domestic identity standards recognised by the FCA.

3 The Cost of Doing Nothing

Private sector identity solutions have yet to provide a universal solution, and GOV.UK Verify has not been widely adopted, and therefore proving identity digitally remains a big challenge for individuals and SMEs alike.

If stakeholders wished to develop a scheme or schemes, there may be technical or regulatory challenges that prove tough to overcome. There may also be political, legal, regulatory or economic reasons why a digital identity scheme may be challenging to deliver - the economics may not stack up for some stakeholders.

The true cost of doing nothing remains poorly understood - it is far easier to identify the cost associated with action rather than inaction. The future costs and savings associated with digital identity inaction are not detailed in many industries. This makes business case modelling all the more difficult.

However, while existing research is limited, it is possible to draw together what robust evidence has been carried out regarding current costs and trends, and by so doing begin to assess the likely future costs, savings and value that may be realised.

Avoidable costs to UK plc

There will be costs resulting from inaction to the wider UK economy, borne by a range of sectors and industries. The cost to identify new customers by digital channels and meet money laundering regulation is a significant cost centre for many businesses. Meeting customers' expectations for high security alongside ease of access to digital services is another challenge that organisations already spend a great deal of money addressing. Some current costs will worsen over time, and opportunities for innovation and growth will be lost.

Such scenarios are driving the exploration of identity solutions across the public and private sector. Whether the intended outcome is improving customer experience and trust, meeting tougher security requirements, or process efficiency and cost saving, industries are spending significant time and effort to mitigate costs that could be more effectively addressed via a digital identity scheme.

Missed opportunity costs

Digital Identity could be an economic growth multiplier

By 2020, the UK's digital economy is expected to grow to 33% of GDP (as opposed to 31% currently), which equates to £764 billion, an additional £46 billion

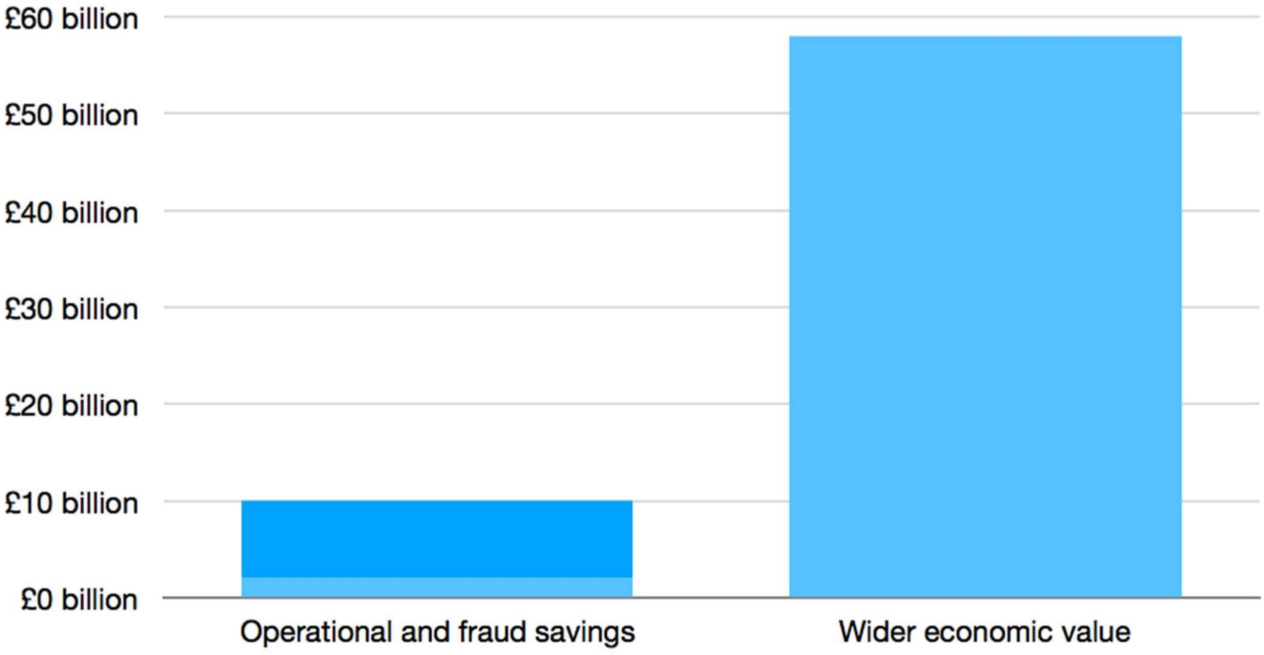
If bigger steps are taken to optimise digital focus through smarter use of technology (including digital identity), the UK could receive an additional £58 billion by 2020[iv]

That equates to a 2.5% uplift to GDP

Potential value to the economy

Digital Identity has significant potential value to the UK economy: it is both a value enabler, growth multiplier, and cost saver.

Direct savings will be derived from lowering identity-related fraud and improving inefficient onboarding and payment processes. Wider value may be derived from the benefits to digital services and innovation supported or facilitated by the use of digital identities.



Graphic: endnotes [v] [vi] [vii]

Projected savings vs value added

Of the potential sums identified above, the Operational and Fraud savings are directly related to identity developments. The potential £10 billion savings pot is made up of direct savings of up to £1.5 billion relating to currently inefficient KYC processes, and up to £8.5 billion in savings to fraud which is related to identity.

Wider economic benefits, projected by studies to be as great as £58 billion in value created, is derived both from value projected to be generated directly from products and services flowing from a digital identity solution, as well as much greater potential value indirectly unlocked by digital identity as part of the wider development of the UK digital economy. Digital identity could play a key part in facilitating, catalyzing and multiplying wider value-adding activities.

Post-Brexit and the global digital economy

As the UK moves towards exiting the European Union and looks to develop new relationships with international trading partners, establishing common ways to conduct digital personal and business transactions across borders will be critical. At present, with upwards of 60 countries having established (or being close to launching) at least one national digital identity scheme rolled out to the private sector, the UK will be increasingly limited in its ability to engage on equal identity terms. This could constrain business activities and reduce future growth.

Sectoral focus

Gambling industry Digital identity needed to tackle identity friction

The remote gambling market was significantly impacted by the implementation of 4MLD. Online operators have had to meet more robust customer due diligence requirements, and in particular for larger transactions. The directive also expanded the coverage of the existing regulations to cover all gambling / gaming operators, not just to casinos, with a direct reference made to online gambling.

As such UK law requires those providing online gambling services to verify a customer's age and identity. Robust age verification is required for other gaming and online entertainment. However, without a common digital identity solution, asserting and verifying identity remains a significant point of friction for customers and businesses. This is reflected in the main cause of failed customer sign-ups across the gaming industry being the length of time and margin for error that occurs during player verification.[viii]

"The remote gambling industry is reliant on effective customer identification and verification processes to meet its regulatory responsibilities and to combat fraud and money laundering. Consequently, there is a constant demand for new, better, and cost-effective digital solutions to help the industry achieve these objectives."
Clive Hawkswood, Chief Executive, Remote Gambling Association

Sharing Economy Trusted identity critical for future growth

The global Sharing Economy is projected to grow from $15 billion in 2014 to $335 billion by the year 2025.[ix] The emerging industry is built on trusted social transactions; however, the lack of digital identity is a significant frustration that could substantially limit future growth.

"The sharing economy is already unlocking substantial value from underused assets, time and skills – but the opportunity yet to be realised is much bigger. Trusting the identity of counter-parties is a crucial element of participation so this is a cornerstone of Sharing Economy UK's 'Trust Seal' mark of good practice. Streamlining ID verification while increasing robustness will help the UK capture the benefits of increasing connectedness between individuals."
Richard Laughton, Chair, Sharing Economy UK and CEO, easyCar

A recent report revealed that the sharing economy is suffering from a lack of trust as consumers are wary of sites offering online peer-to-peer transactions without identity checks.

- UK consumers are cautious - over two thirds (68%) have never entered into the Sharing Economy.
- Overall 61% are uncertain or simply won't share with someone without being able to establish their identity first

Better identity solutions will create trust and grow participation in this fast-developing area of the economy.

Air travel Digital identity to help balance security and growth

Global cross-border travel is forecast to grow a further 50% by 2030, despite the backdrop of security threats, and infrastructure limitations in densely populated countries such as the UK.[x] Ensuring security is achieved, alongside increasing airport capacity and decreasing customer friction is a tough challenge, and new digital identity solutions lie at the heart of the airline industry's thinking.[xi]

As a major contributor to GDP, enabling sustainable future travel growth will provide a significant economic benefit. According to the World Economic Forum the global value of utilising digital technologies to improve safety and security in travel is estimated at $10 billion across airlines, airports and hotels ($7 billion in efficiency gains, $3 billion from increased traffic).[xii] For the same period, it is estimated that the wider value to society could be as great as $20 billion in overall time and cost savings and could be greater than $100 billion due to the avoided costs associated with a major attack.[xiii]

> *"The seamless flow of passengers in airports and between airports is enabled by an analogous flow of data among stakeholders. The OneID Task Force is leading the challenge of developing a new set of "tools and rules," the standards that will enable airports to offer a more secure, privacy protecting and seamless passenger journey in the future."*
>
> Annet Steenbergen (Chair, IATA's Passenger Facilitation working group) and Don Thibeau: A Framework for the Future of Aviation and Trust[xiv]

Sectoral Deep Dive **Cost to the banking sector**

While the evidence remains incomplete at a granular level, within the banking sector the robust evidence of future costs is more developed than in many others.

By choosing not to act, the potential developers of a solution would save themselves the cost of building scheme architecture, and any on-costs such as scheme governance and integrating its use to their systems. In other countries (explored in more detail later in the report) the estimated scheme development costs have ranged from £40-60 million for a limited-use public sector only scheme (e.g. in Finland), to many times that amount. Ongoing costs tend to be much more limited.

However, while inaction would avoid development costs and operational impacts, current KYC processes have been found to be relatively inefficient, and costly, and compliance costs are projected to increase. These KYC costs alone might offset the investment 'savings' based on inaction. In addition to that, identity fraud has been rising for a decade in the UK, and banks are being held increasingly liable for the losses incurred by customers. Without better identity management, fraud-related costs are projected to further increase, for customers and banks alike.

Increasing cost of KYC

Banks' KYC processes have been estimated to range in cost from between **£10 to £100 per check**[xv], however the true cost remains somewhat unknown, and in need of further research.

Current annual core **financial crime compliance costs for banks amount to at least £5 billion** (excluding fines)[xvi]

Inefficient KYC processes are estimated to cost the average bank £47 million a year[xvii]

A typical UK bank **wastes £10m annually** on inefficient KYC checks, post-4MLD[xviii]

Banks' **AML compliance costs increased by 50% over 3 years,** and this trend is projected to continue[xix]

Fines can be as great as **10% of annual turnover** for serious breaches[xx]

If the current trend of rising AML and financial crime compliance costs continues, the banking industry alone will be subjected to **additional costs of £2.5 billion per year** by the end of 2020, **a 50% increase**

Rising fraud and bank liabilities

The cost of fraud against Individuals in the UK (2016) was estimated to be **£9.7 billion**

Identity fraud was identified as the largest contributor, at close to **£5.4 billion**

There were an estimated **3.25m victims**, and this is predicted to increase[xxi]

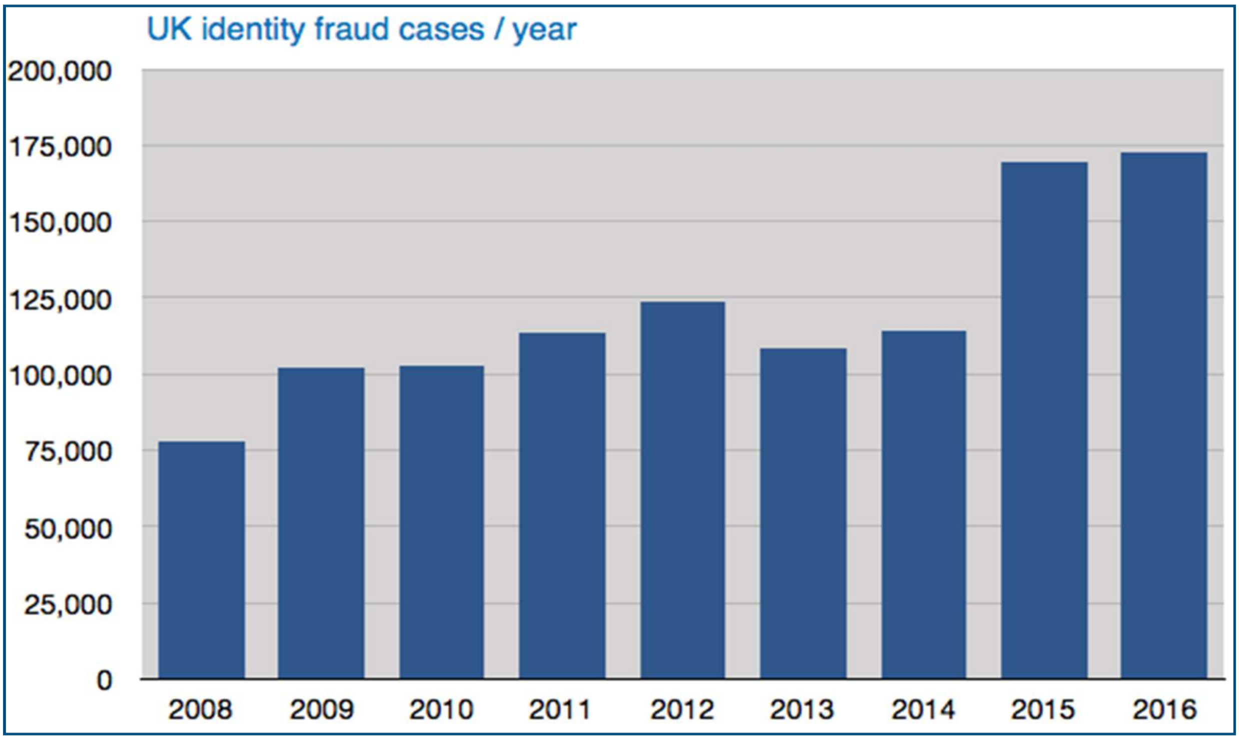
A record **89,000 cases of identity theft** were reported in H1 2017, **almost exclusively taking place online**

Identity fraud now accounts for **56% of all fraud** reported by Cifas members[xxii]

The Payments Systems Regulator recently proposed to **extend banks' liability for losses** incurred by customers via 'push transactions', following the Which Super Complaint

In excess of £100m was lost to these types of scam in the first half of the 2017

It was reported that consumers lost an average of **£3,000** and businesses **£21,500**[xxiii]



Graphic: endnote [xxiv]

Digital friction

Digital service users experience an increasing degree of identity friction when transacting online. The lack of a digital identity solution is creating friction for customers, and high levels of friction has been identified not only as a customer frustration, but as a competition concern by both the CMA and FCA.

> *"A key driver of effective competition in a market is consumers' ability to exercise choice. If consumers can switch easily between different products and providers, firms will have strong incentives to improve the products and services they offer to retain and attract customers."*
>
> Financial Conduct Authority[xxv]

Growing demand for digital banking

Over the past five years customers' app-based banking activities have increased by 354%

Apps are now the most favoured way for individuals to access their current accounts, rising from 21% of us in 2012 to 61% by 2017

Rapid growth in a wide range of services accessed by customers via apps (2015 to 2016):

- **Savings products rose by 30%**
- **Credit cards increased by 46%**
- **Mortgage and investments accounts increased by 86%**[xxvi]

In the UK 25% of bank applications are abandoned due to KYC friction[xxvii]

Competition concerns

Digital friction risk further regulatory action

The UK banking industry, and particularly the current account market, has been subject of a series of initiatives in recent years seeking to encourage greater competition, often at significant industry cost. Many initiatives have focused on reducing KYC friction, and increasing customer account mobility.

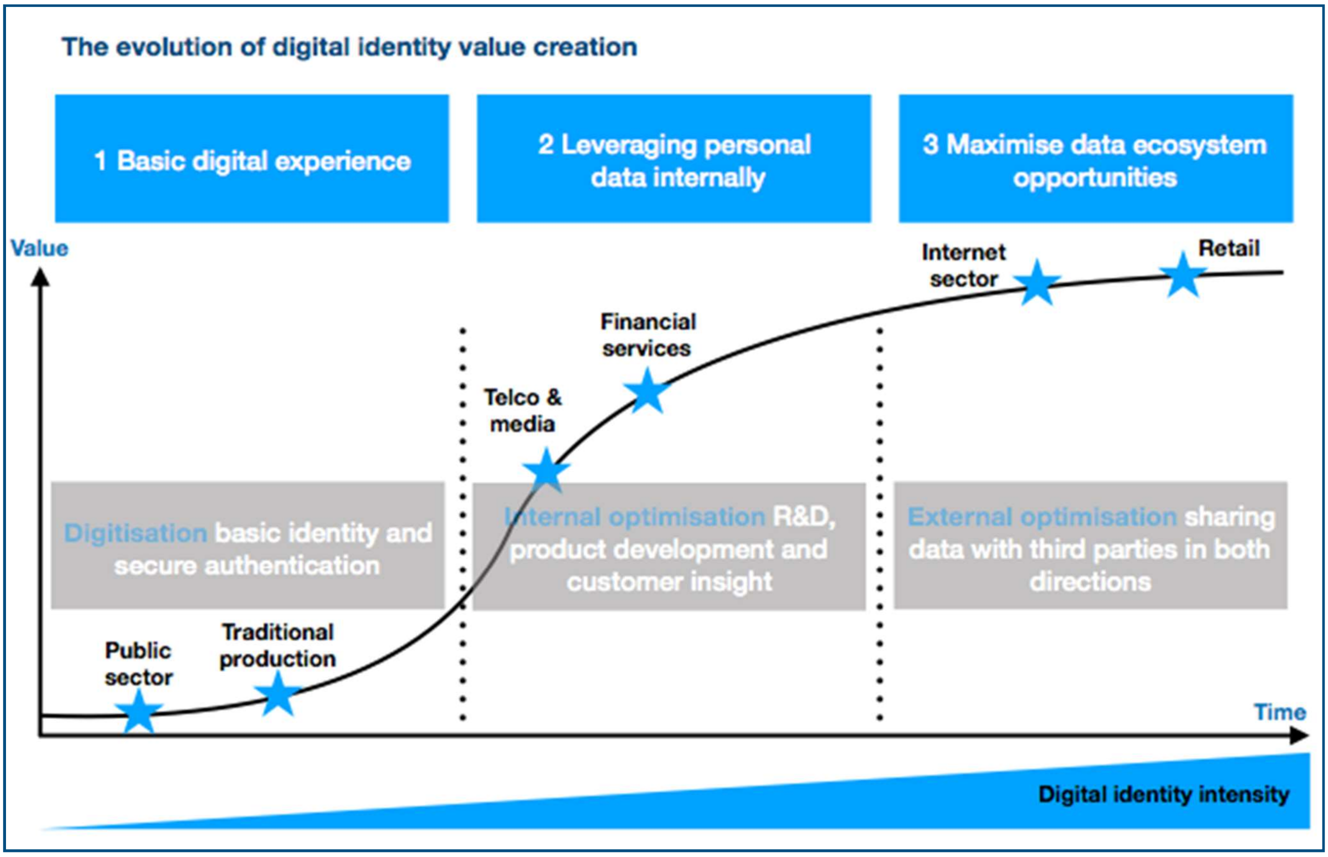
While identity and KYC challenges continue to frustrate customers, and while they cannot access a full range of services in a digital environment, the banking industry risks being mandated to deliver a digital identity solution by regulation, and not necessarily to a model of its choosing. The PSF's proposal concerning SME trusted KYC data sharing, now that it has been taken up by the PSR with a deadline of 2020 given for delivery, is the first such example.[xxviii]

The cost of lost opportunity

Unlocking the value of attribute data for banks and customers

Banks and other trusted personal data holders (of which there are many) currently incur significant KYC-related costs, simply to establish and maintain a relationship with customers, and to store the customer's data securely. At present, relatively little is done to extract further value from the costly checks and validation processes the organisations have gone through to establish confidence in the data they hold about customers, nor to enable customers to unlock the value of the data that organisations hold about them.

Without a willingness by banks to find ways to share customers' attribute data, and thereby enable digital identity solutions to be created from that sharing environment, the considerable value of KYC and identity data will remain unrealised.


The evolution of digital identity value creation
1 Basic digital experience
2 Leveraging personal data internally
3 Maximise data ecosystem opportunities
Value
Internet sector
Retail
Financial services
Telco & media
Digitisation basic identity and secure authentication
Internal optimisation R&D, product development and customer insight
External optimisation sharing data with third parties in both directions
Public sector
Traditional production
Time
Digital identity intensity

Graphic: endnote [xxix]

Constrained payment innovation

The Payment Strategy Forum has heralded a drive towards payment innovations, many of which would be facilitated significantly by digital identity. The focus of the Payment Systems Regulator is to see a number of innovative and far-reaching payment proposals delivered, many of which are likely to encourage banks to consider better ways to deliver payment authentication. There is a risk of further regulatory action if the ongoing lack of digital identity solutions is seen to frustrate the regulator's efforts to reboot the UK's payments ecosystem.

Limiting branch network transformation

As branch closures continue to hit communities and make political and media headlines, an ongoing lack of a digital identity solution will further frustrate customers' ability to access alternative online banking activities. This may limit the ability of banks to further transform their branch networks, or bring about renewed political pressure to maintain their physical networks or to deliver enhanced digital services.

4 Exploring Potential Solutions

If the costs of inaction prove too great to bear, and a solution is to be explored, the UK can learn a lot from other digital identity schemes that have been developed around the world.

Learning from international experience

Digital identity schemes have been developed outside of the UK via a wide range of models and routes to market. Some examples have significant government involvement and are in effect government-led, centralised schemes, which have delivered some mixed results:

Estonia is successfully leveraging its existing ID card / mobile ID scheme to provide access to over 600 digital government services including electronic voting. The scheme was introduced as part of a programme to digitise government services and the wider economy.

The **Singapore** government is incorporating biometric security and open API interfaces enabling private companies to utilise the digital identity scheme it is developing. The country has a long history of significant government involvement and change leadership in both the economy and banking.

In **India**, the Government's Aadhaar scheme has scaled very rapidly, with over a billion identities created. It provides unique identifiers for citizens to access services, and is seen as an accessibility tool for those unable to provide more traditional means of identification. Since late 2017 the Indian Government has required every bank customer to link their accounts with their Aadhaar identifier, creating new services and opportunities to leverage the national scheme.

In **Finland**, a heavily government-led digital identity scheme built on the existing national identity register featured poor market penetration, relatively few use cases, and those predominantly in the public sector. The poor take up and significant development costs resulted in a very high cost per use. However, recent developments via a mobile-based digital identity platform offer new dimensions and a new lease of life for the scheme.

"Digital identity management has the potential to foster economic benefits but only if some degree of coherence/co-ordination is brought to the currently fragmented landscape."
OECD Working Party on Security and Privacy in the Digital Economy[xxx]

Do banks hold the key to success?

There are a range of successful examples where the level of government involvement has been less to the forefront, with the government's role instead being to act in partnership with the private sector, to act as standard-setter, or merely to facilitate and support industry-led action. In all successful international examples of this type, banks have been directly involved, and usually from the inception of the project. The banking sector has frequently played a key role in scoping the required outputs, have featured as identity and trusted KYC attribute providers within the scheme, and just as vitally, as relying parties.

The Nordic countries have been leaders in the development of bank-led digital identities, although not without some difficulties, as seen in the case of Finland.

In **Norway** BankID is an electronic identity scheme used by banks, and across both the public and private sectors, and has been in operation for over a decade. Banks initially actively enrolled their customers onto the scheme, ensuring a rapid provision of identities into the market. As time has gone on, a much wider range of uses outside of banking have been established, and the scheme is very frequently used by a large proportion of the population. Over 80% of the adult population in Norway has a BankID and uses it on average twice a week, with the ability to use it for day to day banking and payments being a factor that has significantly accelerated adoption. Since 2014 BankID has been spun off as a commercial entity, with the banks as shareholders.

In **Denmark**, the NemID scheme has been in operation since 2010, and allows access to a range of services such as online banking and single log in to government and bank websites. It has experienced significant public take-up and high accessibility. This has resulted in around 4.7 million Danish citizens using NemID (of a population of 5.7 million), with more than 55 million transactions taking place using NemIDs in a typical month. There has been some criticism of the scheme's security features, and partly as a result the scheme is due for an update in 2018.

In **Sweden** a programme of rapid digitisation of public services has increased both the opportunity and need for digital identity solutions. A range of innovative private sector solutions continue to emerge, and the leading identity scheme, BankID, has a user base of over 7.5 million people. The scheme was developed by a number of large banks in 2003, and can be used to access a wide range of public and private services, and across smart card-based, online and smart device-based channels. The IDs are used to identify individuals as well as providing legal signatures.

The DigiID scheme in **Holland** was initially created to allow digital access to government services. Following this, the IDIN scheme has been launched by the Dutch Payments Association, a membership organisation comprised of Holland's biggest banks. The scheme provides identity credentials at a number of authentication levels for different types of transactions.

In **Germany** the Verimi scheme is being developed by a consortia of private sector companies, from the banking, insurance, automotive, aviation, technology and media sectors. It will initially offer users a single-sign-on solution for log-in to participating organisations' websites, seeking to increase security and improve customer experience, while embedding it in day to day activities. Further uses to access a wider range of services, including digital payments, financial services and public services have been planned for further staged releases.

Canada has seen a number of digital identity developments in recent years. The Digital Identity and Authentication Council of Canada (DIACC), a not-for-profit organisation comprising both public and private sector interests, is delivering an open framework for the development of identity solutions. There are now both public and private-led schemes in place, led by a consortia of leading banking and telecoms companies in the private sector.

Success Factors	Failure Indicators
Private sector involvement (particularly banking sector) in the scheme design and delivery	Government-led with little or no private sector involvement
A shared vision for delivery between Government and industry, and clarity of roles	No shared vision, competing roles
Wide range and availability of services able to utilise the ID • Government / civil services • Private sector services	Limited service availability, lack of ubiquity
Banking services are accessible using the ID	Public services access only
High frequency of use - application to high-volume low-authentication purposes (e.g. website log-ins, age verification) and less frequent higher authentication uses (e.g. bank account opening)	Low frequency uses only
Existence of a mandatory ID for all citizens - e.g. social security number, national ID card.	Voluntary or no national ID scheme in existence.
An accepted history of national identity schemes	Public distrust of Identity schemes / 'big brother'
A national residential register	No central residential register
Available to be used via a variety of channels including Smart phone	e-Card-based only – particularly if a card-reader is also required
Low population states	Large population states
Using existing KYC data (particularly bank data) to actively enroll customers with an ID	'Organic' enrolment only
Public trust in the security of the scheme	Security breaches / questions
Public trust in how data will be used	Lack of trust in privacy rules
Liability model and trust framework addressed	The lack of clarity on liability
A clear business case - operational savings demonstrated and agreed by industry	Little economic benefit or high costs compared to current processes
Regulatory clarity / confidence	Regulatory ambiguity or barriers
Passive enrolment of customers - a smooth customer journey	Difficult or lengthy enrolment process - a poor customer journey
Well-connected / interoperable existing government IT and databases	Fragmented / unconnected / legacy govt systems
Well-connected citizenry (wifi, mobile, broadband adoption and coverage rates)	Unconnected societies (not that not all channels need to be well developed – e.g. mobile only schemes in Sub-Saharan Africa)
Barriers to access an ID removed or addressed	Low inclusion and low access rates
Strong public awareness and education – and govt and private sector working together to achieve this	Low awareness and or education level, or lack of joined up promotion.

Potential options: Digital identity scheme models

There are a range of possible scheme models capable of forming the basis for digital identity or KYC solutions. The models are not all mutually exclusive, and hybrid or variant models found in other countries often incorporate several elements, each operating as part of the overall solution. Each model has benefits, as well as challenges to overcome. Some may be more appropriate to providing a local or sector-focused scheme, while others can be scaled towards being a more complete and cross-sector identity solution.

OPTION 1: GOV.UK Verify in the private sector

The GOV.UK Verify scheme, while limited in scope at present, does provide fur attributes at an established level of authentication, and could be extended for use in the private sector. This could be as the basis for more data-limited uses such as age verification, or as at the means for customers to demonstrate their identity sufficiently to allow a wider range of attribute data to be shared on their behalf. Opening up the GOV.UK Verify scheme and standards to the private sector could be an important catalyst to the digital identity ecosystem in the UK.

Case study **Transforming air passenger journeys**

GOV.UK Verify IDs have been explored (in principle) for use in the airline industry, in the *Transforming the Airline Passenger Journey* project. Much of the information required to be provided by customer ahead of travel - advanced passenger information - could be provided by use of a Verify ID.

Benefits

- Reduced costs and risk for government
- Reduced operational overheads
- Potentially significant savings

Endnote [xxxi]

OPTION 2: Open Data models

The Open Banking model is built on the use of Application Programming Interfaces (APIs). An open data model built on common API standards could similarly provide the technical means for the secure exchange of identity or KYC data held by regulated organisations, or by government. APIs could provide the means to make this data available to relying parties, either directly or perhaps via private sector attribute hubs, enabling the development of new digital identity applications and KYC solutions.

> *“[Open Banking] is a remarkable project; one with the potential to change retail banking forever. If we get it right we will for the first time anywhere in the world, put the customer in control of their data, their privacy and their finances.”*
>
> Imran Gulamhuseinwala OBE, Trustee of the Open Banking Implementation Entity

As has been predicted for Open Banking, this could unlock significant value. A recent Centre for Economics and Business Research (Cebr) report for Trustpilot predicted that the Open Banking reforms alone will add £1billion to UK GDP and create up to 17,000 jobs.[xxxii]

OPTION 3: Self-sovereign identity

In contrast to centralised 'utility' schemes, the concept of 'self-sovereign' identity is based on individuals storing and controlling the sharing of their identity data locally, on their own devices, and being able to provide it securely to those who need to verify it, as and when they require.

This removes the need for any central data repository, it can provide individuals with greater control over who has access to their data, how it is used (and who benefits from this). Over time such a model could form the basis for a new form of customer-centric personal data market.

OIX BITGov initiative
OIX has developed a new programme to explore Blockchain, Identity Trust and Governance ('BITGov'). A series of workshops and discussion via the OIX Forum is intended to further scope this exciting area of identity development.

www.openidentityexchange.org/forum/

"The attributes required to prove 'identity' will always vary according to context. Therefore the more attributes that a claimant can make available to be discovered, attested to, permissioned, referenced and traced, the easier it is for them to prove their identity to anyone, in any context."
Ben Helps, CEO Factern

OPTION 4: Task-specific solutions

It may be that by focusing innovation on solving specific identity and KYC issues, a series of narrow, task-specific private sector solutions will be developed instead of (or alongside) a wider scheme or data sharing environment. These would not generate the wider customer and economic benefits typically arising from interoperable, multi-sector identity solutions, however cost savings, improved customer experience, faster processing and increased security are all possible to be achieved at a more localised or sector-specific scale.

OPTION 5: Hybrid models

Many emerging international schemes include two or more models explored here. The cross-border, private sector use of digital identity schemes that conform to the eIDAS Standards is an important recent development. This is being encouraged by the European Commission, particularly as part of their drive towards a single European market for financial services and insurance, and via the 5MLD amendments. The UK increasingly looks increasingly isolated amongst an ever-wider range of states with digital identity schemes in place.

Using digital identity schemes cross border
A variant of the API open data model is currently being researched, via the OIX programme, by a consortium of French and British organisations. This is funded in part by the European Commission's Connecting Europe Facility programme. In the project, the data provided by a customer's French digital identity would be used to draw together API-derived attribute data from a number of trusted sources, and then transmitted to a UK bank via a private sector attribute hub. While the research is international in scope, the scheme architecture could easily be applied in a solely domestic context in the UK.

Endnote [xxxiii]

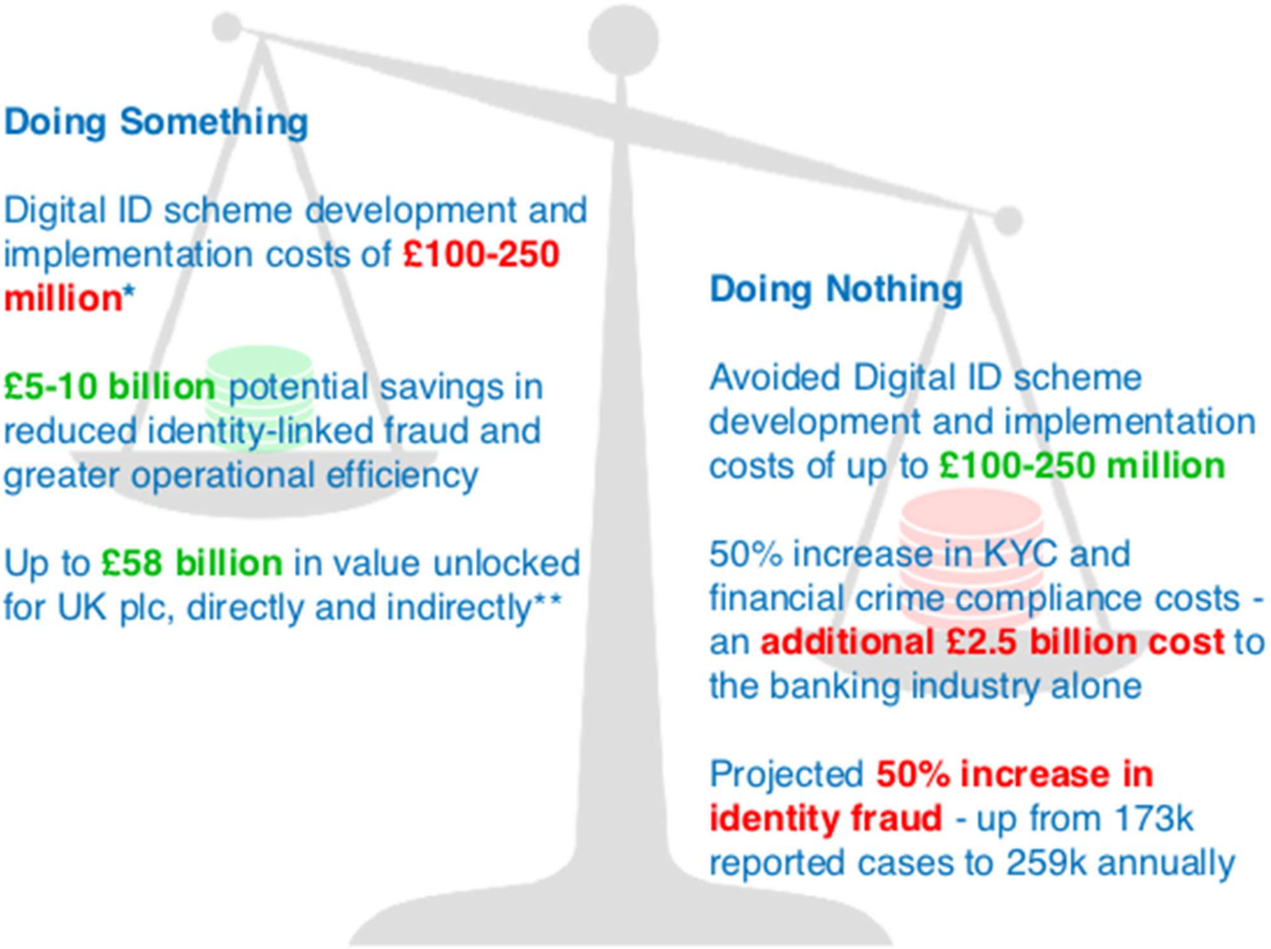
5 Conclusions

The evidence that exists of the likely costs of inaction, born of the ongoing failure to develop better digital identity solutions for the UK, is stark.

The exact costs may not be well defined, however the scale of future challenges, the underlying trends of increasing compliance costs and fraud rates, and the resulting cost headlines are becoming increasingly clear:

- Rising fraud, and increasing identity fraud in particular
- Rising demand for digital services and products, and increasing identity friction
- Tougher KYC standards and AML compliance requirements
- Payments innovation, including the need for stronger payment authentication

The value of action vs inaction: 2021 projections



Doing Something

Digital ID scheme development and implementation costs of **£100-250 million***

£5-10 billion potential savings in reduced identity-linked fraud and greater operational efficiency

Up to **£58 billion** in value unlocked for UK plc, directly and indirectly**

Doing Nothing

Avoided Digital ID scheme development and implementation costs of up to **£100-250 million**

50% increase in KYC and financial crime compliance costs - an **additional £2.5 billion cost** to the banking industry alone

Projected **50% increase in identity fraud** - up from 173k reported cases to 259k annually

* Based on scheme development costs elsewhere, and projected implementation costs across industries.
** Potential value creation includes digital identity as a catalyst to wider innovation in the digital economy.

What needs to happen next?

The rational choice may be to take no action, to hold back from developing more complete digital identity solutions. However, this decision should be taken in clear view of the evidence, and a detailed understanding of the likely costs and benefits.

- Further analysis needs to take place across a variety of sectors, assessing both the cost and value of developing an identity solution, and further analysis of the likely cost and value of inaction.

- The customer detriments associated with a 'no scheme world' also need to be more fully understood. This should include research into the potential role played by digital identity friction in stifling competition.

If the value of doing something is too great to ignore…

1

Engage widely

Develop a wide and collaborative discussion across a number of industries (and government), in particular amongst both potential attribute / identity providers and relying parties. From this a shared vision could be developed, and cross-sector benefits identified in principle.

2

Explore the economics and trust arrangements

The business case and scheme economics need to be openly explored in further detail, across both public and private sector. This would ideally include increased clarity on existing KYC process costs and potential cost savings, as well as deeper discussions concerning liability and trust arrangements.

3

Agree a range of uses and their requirements

Identify a wide range of potential identity uses, the attributes and levels of authentication required for each use case, and from where these attributes may (potentially) be sourced. A comprehensive 'attribute register' could form the basis for a range of identity outputs, thereby increasing utility and frequency of use, both of which have proven to be significant success factors for new identity schemes.

4

Banks to engage fully in the discussions

Encourage banks to engage - in most international schemes banks have taken a significant role, both in designing and delivering schemes, as potential attribute and identity providers, and as relying parties. This has proven to be a major success factor, yet UK banks remain on the sidelines of discussions at present.

5

Government and regulators to facilitate, not lead

Government and regulators can do much to support and facilitate identity development conversations. Government can be a successful standard-setter, and may need to clear any unnecessary regulatory or legislative barriers, and ensure government departments are aligned and encouraged to participate in a scheme.

6

Self-regulate or risk regulatory action

If industry itself fails to find a better digital identity solution under its own initiative, there is a risk that a more direct approach may be taken by government or regulators.

About OIX

The Open Identity Exchange (OIX) is a technology agnostic, non-profit trade organisation of leaders from competing business sectors focused on building the volume and velocity of trusted transactions online.

[i] BBA/PWC report : How Digital Identities Which Meet Government Standards Could be Used as Part of UK Bank's Customer On-Boarding and KYC Requirements (2017)

[ii] https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

[iii] https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify

[iv] https://www.accenture.com/gb-en/insight-digital-disruption-growth-multiplier

[v] https://www.cifas.org.uk/newsroom/identity-fraud-soars-to-new-levels

[vi] The Annual Fraud Indicator 2016, overseen by the UK Fraud Costs Measurement Committee (UKFCMC), supported by Experian and University of Portsmouth's Centre for Counter Fraud Studies

[vii] https://www.accenture.com/gb-en/insight-digital-disruption-growth-multiplier

[viii] http://www.experian.co.uk/blogs/latest-thinking/three-critical-challenges-online-gaming-compliance-regulation-age-verification/

[ix] HooYu Report - Trust & Identity in the Sharing Economy http://contentz.mkt6928.com/lp/40905/238424/HooYu%20report%20on%20Identity%20Trust%20in%20the%20Sharing%20Economy.pdf

[x] The Known Traveller: Unlocking the potential of digital identity for secure and seamless travel - WEF, January 2018

[xi] https://www.iata.org/whatwedo/workgroups/Documents/single-token-pax-facilitation.pdf

[xii] World Economic Forum. Digital Transformation Initiative.

[xiii] The Known Traveller: Unlocking the potential of digital identity for secure and seamless travel - WEF, January 2018

[xiv] http://www.donthibeau.com/tag/iata/

[xv] Consult Hyperion report: Know Your Compliance Costs (June 2017)

[xvi] BBA response to Cutting Red Tape Review: Effectiveness of the UK's AML Regime. https://www.bba.org.uk/policy/bba-consultation-responses/bba-response-to-cutting-red-tape-review-effectiveness-of-the-uks-aml-regime

[xvii] Consult Hyperion report: Know Your Compliance Costs (June 2017)

[xviii] Consult Hyperion report: Know Your Compliance Costs (June 2017)

[xix] https://www.accenture.com/t00010101T000000Z__w__/gb-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_20/Accenture-Reducing-The-Cost-Of-Anti-Money-Laundering-Compliance.pdfla=en-GB#zoom=50

[xx] Consult Hyperion report: Know Your Compliance Costs (June 2017)

[xxi] The Annual Fraud Indicator 2016, overseen by the UK Fraud Costs Measurement Committee (UKFCMC), supported by Experian and University of Portsmouth's Centre for Counter Fraud Studies

[xxii] https://www.cifas.org.uk/newsroom/identity-fraud-soars-to-new-levels

[xxiii] https://www.ukfinance.org.uk/authorised-transfer-scams-data-h12017/

[xxiv] https://www.cifas.org.uk/newsroom/survey-reveals-people-not-protecting-themselves-from-identity-fraud

[xxv] https://www.fca.org.uk/publication/research/making-current-account-switching-easier.pdf

[xxvi] UK Finance - An App-etite for Banking (2017) https://www.bba.org.uk/news/reports/an-app-etite-for-banking/#.WoMb3yOcbfY

[xxvii] Consult Hyperion report: Know Your Compliance Costs (June 2017)

[xxviii] https://www.psr.org.uk/psr-publications/news-announcements/PSR-sets-out-progress-on-tackling-scams

[xxix] 'The Value of our Digital Identity' BCG / Liberty Global (2012)

[xxx] https://one.oecd.org/document/DSTI/ICCP/REG(2015)12/en/pdf

[xxxi] http://oixuk.org/wp-content/uploads/2017/09/Transforming-the-AIrline-Passenger-Journey.Sept17.pdf

[xxxii] http://press.trustpilot.com/news/2018/2/26/open-banking-expected-to-contribute-over-1-billion-annually-to-uk-economy-supporting-17000-new-jobs

[xxxiii] http://oixuk.org/opening-a-bank-account-cross-border-id-authentication/