COULD DIGITAL IDENTITIES HELP TRANSFORM CONSUMERS' ATTITUDES AND BEHAVIOUR TOWARDS SAVING?

The findings of a Discovery Project

By Rob Laurence (Innovate Identity)
May 2016

Participants

Formatting of report. Use of text boxes

Coloured text boxes are used to provide the reader with supporting information to assist with understanding of the context of this project.

Footnotes are provided with links to external references and URLs.

Executive summary

It has long been recognised that people are not saving enough to support their short, medium and long-term needs. We live in a society where instant gratification has become the norm, borrowing and credit fueling a spending culture at the expense of saving and investment for our futures.

But even if people want to save more, they face numerous challenges to take out a new savings product. Opening a new savings account, even a journey that starts online, often results in asking savers to complete the process offline as providers ask for evidence of our identity and complete the appropriate anti-money laundering checks before they accept our money. Contrast this to obtaining a personal loan, a process that can often be completed online in minutes with the money in your bank account within hours. It is far easier to borrow money than save!

This paper, sponsored by the Tax Incentivised Savings Association (TISA), reports the findings of an OIX Discovery Project to explore the use of a digital identity scheme in the savings sector. The project principally explored users' perceptions and expectations about digital identities and whether they could be used to enable greater consumer awareness and change behaviour towards saving. The project team also considered whether a digital identity scheme in a wider context could lead to savings in identity assurance and regulatory compliance checks and underpin the transformation of business processes.

The lack of a savings-fueled economy is creating significant problems for individuals, local and central government and the wider UK economy. This is particularly relevant within the context of the pressures on household budgets and significant demographic changes taking place associated with increased life expectancy and the increasing costs of public services.

TISA, on behalf of its members in the financial services sector, recognises that concerted action is now required. Early in 2015 it established the TISA Savings and Investment Policy (TSIP) project, an unprecedented collaboration of more than 50 firms in the savings sector, together with professional services, trade associations and consumer bodies.

> *30% of households have no savings at all and a further 20% have less than £1,500 to cope with an unexpected event without going into debt.*
>
> *2035 is set to mark a tipping point when consumers aged 45 today will start entering retirement and will be less well off than earlier generations.*
>
> TISA

The TSIP project has been considering what measures should be taken to avert the coming crisis and re-establish a savings culture in the UK. The TISP report, *Saving our financial future*, sets out a number of recommendations.[1]

---

[1] http://www.tisa.uk.com/downloads/TSIP%20Policy%20Proposal%20Report%202015.PDF

The Open Identity Exchange (UK) and TISA have commissioned this Discovery project to explore one of these recommendations within the hypothesis:

If customers had an easy to use and trusted way of opening a savings product and transferring their savings, using a digital identity, people would be inclined to save more and manage their money better. ("Trusted" in this context is about the customer's view of trust).

The discovery project involved a collaboration between TISA, Legal & General, Liverpool Victoria, the Government Digital Service (GDS) and EY-Seren, a design consultancy specialising in digital business transformation. Innovate Identity provided project management services and subject matter expertise in the field of digital identities, privacy and money laundering regulation.

This project researched users' experiences of the savings market and tested their views and perceptions of digital identities and whether they could underpin the development of new, ground breaking services that could transform attitudes and behaviour towards saving.

A number of significant findings resulted from the user research.

1. Almost half of the participants in the research had abandoned a savings account signing-up process. Reasons cited included it was too much hassle, the need to provide documents to prove their identity and the safety of documents in transit.
2. Participants were positive about using digital identities as a convenient way of confirming their identity with savings providers; this was particularly strong if government was involved as it created a sense of trust.
3. Most participants who undertook the registration process thought the digital identity was worth the 10 minutes spend registering, as they could re-use it later.
4. In addition to the identity attributes (name, address, date of birth and gender) returned by the digital identity provider, some participants in the research expected further attributes to be returned (eg contact details) to populate the application. The savings sector will need to consider how such data might be provided.
5. Digital identities can be a catalyst to transform services, as is being demonstrated by central government. Designing end-to-end processes focused on the needs of the user (user rather than business-centric) can, from the evidence of the research, leave customers very happy and engaged.
6. Digital identities, by themselves, are unlikely to measurably improve the overall level of savings.
7. However, through new products enabled by a common digital identity, such as ways to view an entire savings portfolio or seeing the progress of a savings transfer,

customers may be encouraged to save more or take advantage of better interest rates thus leading towards a more competitive and dynamic market. Simulations of these services during the research were perceived by the participants to have high value.

The project team also recognised that digital identity schemes may have far reaching benefits in the wider financial services sector that go beyond the just savings.

Regulatory AML Customer Due Diligence processes could be streamlined and delivered at much lower cost. The financial services industry would be prepared to invest in a solution to meet identity verification, AML and KYC requirements, utilising new technology. Customers would benefit from much simpler and less time consuming processes.

Digital identity schemes could underpin a raft of new consumer services leading to more competitive and dynamic markets.

Digital identity schemes have the potential to transform business processes through real-time data sharing across organisations, with the customer present in the journey, completing applications in real time and thus reducing the need for back office off-line fulfilment.

The financial services sector, working in conjunction with government, has the opportunity to lead this.

* The OIX white paper, Economics of Identity, estimates that the cost of identity assurance to organisations in the UK is £1.65B. This comprises £550M as the cost of creating identities in the first place and £1.1B as the cost of using them across billions of transactions every year. A further cost of £1.65B is estimated to fall on the consumer in terms of time to create and use identities.

The future cost of identity assurance could be reduced to £150M through the adoption of digital identity schemes.

Furthermore, the research estimates that some 18 million account opening transactions are completed each year, costing between £30 and £120 each. **In financial services, an estimated 4 million high-cost transactions, costing between £30 and £120 each, are conducted manually which could be handled digitally if the identity assurance aspect of the process was fixed. The total savings of taking these transactions online would exceed £250M.**

Background and context

Today, consumers taking out a new financial savings product, or transferring savings between one provider and another, are faced with the daunting prospect of having to prove who they are and where their money has come from.

Even in the Internet-connected world we live in, with the proliferation of online services and real time communications, consumers are still frequently being asked to provide identity documents as they were 20 years ago (with the only concession being that these can be scanned and uploaded rather than being posted or presented in person). Whilst "progress" has meant we can complete applications online in minutes, identity checks can still take weeks!

This discovery project was scoped around replacing the traditional approach to identity checking with a new online approach using digital identities.

Since 2012, the UK government, through its Government Digital Service, has been leading the way to develop a digital identity scheme, GOV.UK Verify, for citizens to access government services. This forms part of the Government Digital Strategy[2] to transform the delivery of government services to the citizen. It sets out a 'digital by default' approach designed to ensure digital services are designed so well that citizens prefer to use them.

GOV.UK Verify is currently being rolled out across many Beta projects and is due to go live in May 2016. Over 500,000 citizens have created a digital identity through GOV.UK Verify and those digital identities have been used 1.3 million times to access central government services (as at 1st May 2016).

GOV.UK Verify
The UK government has developed GOV.UK Verify, a new way for citizens to safely and securely prove they are who they say they are entirely online when accessing digital public services provided by central government. GOV.UK Verify uses certified private sector companies to conduct identity verification checks according to published government standards. The user chooses which certified company they would like to use to establish their digital identity. A set of nine principles guides the design of the identity assurance system. A digital identity created with a certified company through GOV.UK Verify can currently be used to access an increasing range of central government services on GOV.UK. In principle, certified companies might also enable users to assert a digital identity that meets government standards in transactions with local government, NHS and the private sector. How this would operate in practice has yet to be established.

---

2 https://www.gov.uk/government/publications/government-digital-strategy

GOV.UK Verify could, potentially, meet the account opening identification and anti-impersonation checks and account access authorisation for the majority of low and medium risk money laundering scenarios. (Note that additional anti-money laundering checks would need to be carried out at account opening. These are discussed later in this paper).

Two use cases were explored and user journeys were designed with a view to testing users' views on using a digital identity to prove who they were. Two hypothetical scenarios were considered. The first involved using a digital identity that had previously been created in GOV.UK Verify in a completely different context – an online government service such as applying for a passport or driving licence. The second involved using a digital identity that had been created in a previous financial services transaction, such as opening a bank account, and was branded as MONEY.UK Verify.

The project also tested users' views on a 'companion' service to determine what impact real-time access to all of a user's savings accounts would have – presented as an online view of the user's portfolio – and whether this would change users' behaviour towards saving.

What is a digital identity?

A digital identity is the Internet equivalent to the real identity of a person or entity. For the purposes of accessing UK government services, using GOV.UK Verify, the digital identity contains the minimum number of identity attributes that uniquely identify a person online to an acceptable risk-based level of assurance and trust. These attributes are the person's full name, date of birth, gender and current address. Minimising the number of attributes held respects the person's privacy and safety online.

The TSIP project (referred to in the Executive Summary), has a different interpretation of a digital identity. In addition to the identity attributes listed above, TSIP envisages further attributes being made available at the time the digital identity is obtained. These attributes may include the results of regulatory checking processes that the Anti-Money Laundering legislation demands, including checks against Financial Sanctions lists and Politically Exposed Persons lists.

This is discussed further in the section Future Considerations.

Research objectives and methodology

A qualitative research project was undertaken to discover the potential benefits and value to consumers and providers that a digital identity could deliver in the context of people's attitudes and behaviour towards saving.
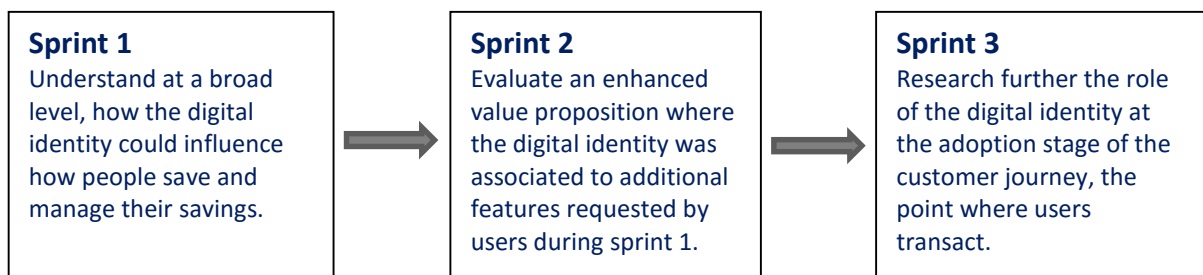
The research was designed to uncover issues and users' perceptions around key topics. It was not designed to evaluate user experience of specific journeys or draw statistical conclusions.

A carefully selected sample of 15 participants were selected based on a broad social claim with an even spread of gender and age between 20 and 65. Other criteria included use of online banking at least once in each period of 3 months and taking-out a new savings product in the past 12 months.

The research was undertaken in 3 sprints (rounds), each with 5 participants in a controlled environment with audio visual recording of each session. Each session required the participant to verbalise their thoughts whilst making use of two mocked-up prototypes that used digital identity functionality in the account opening and transferring processes.

Changes were applied to the prototypes between rounds to explore perceptions on a comparative basis (for example, of two different brands of the digital identity service) and to include feedback from users in the preceding round that had an impact on their perceptions (for example, clearer signposting within parts of the journey).
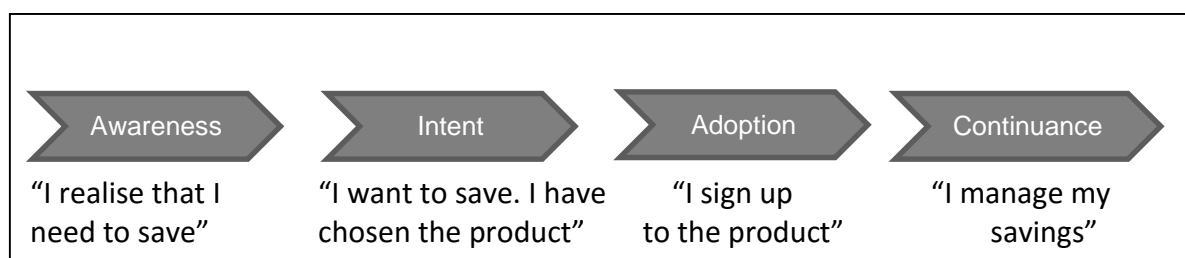
An overview of the 3 sprints and the principal aims is as follows.

Sprint 1
Understand at a broad level, how the digital identity could influence how people save and manage their savings.

Sprint 2
Evaluate an enhanced value proposition where the digital identity was associated to additional features requested by users during sprint 1.

Sprint 3
Research further the role of the digital identity at the adoption stage of the customer journey, the point where users transact.

User research and findings

Attitude towards savings

When choosing to open savings products, customers go through 4 key stages of behaviour. Despite the particularities of each personal context, these steps are consistent across the savings journey observed during the research and with many studies into savings behaviour carried out elsewhere (a good example of such research is the report *Raising Household Savings* published by the British Academy for the Institute of Fiscal Studies[3]).

Awareness	Intent	Adoption	Continuance
"I realise that I need to save"	"I want to save. I have chosen the product"	"I sign up to the product"	"I manage my savings"

---

[3] http://www.ifs.org.uk/publications/6028

Digital identity has relevance in the Adoption and Continuance stages, once there is an intent to open a new savings product or manage an existing one. Whilst the Awareness and Intent stages were explored in some detail during the research the focus of this paper is primarily on user experience and perceptions of the digital identity itself.

Adoption – opening a new savings product

Participants discussed different experiences and perceptions when opening new savings products. These tended to polarise as either

(1) A time consuming and laborious experience to prove one's identity
(2) A simple and straightforward process

These differences depended on each provider's account opening procedures and whether the customer already had a product with them.

The participants were asked whether they had abandoned a signing-up process in the past. Many had, mainly for reasons concerning the hassle, perceived lack of safety or the need to provide documents to satisfy the necessary identity checks. Other reasons given included a lack of clarity around the specific savings proposition.

"To provide my identity I usually scan and send my passport by email. You always feel uneasy to send your passport or driving licence."

Continuance – managing existing savings

Participants discussed how they managed their existing portfolio of savings. The majority of participants checked financial services websites or had access to an App, and then collated information by creating their own spreadsheets or hand-written records.

"I have a filing system that I created, at home. It's a cabinet where I keep all the printed documents for at least 5 years. I keep it very organised."

"I have a spread sheet where I write down all my savings accounts, how much I have in each one and the maturity dates. That way I always know when I have to start shopping around for a new product."

There was widespread agreement that a quick and easy way to access all their savings products in one site would be helpful.

As one user said when shown the simulated portfolio service, perhaps suggesting a change of behaviour:

"I hate saving but when you are doing it well, I find it addictive as well because I feel like I am winning."

And for another user:

"After doing the transfer, I would like to go to my portfolio page to see if it's added on…… There you go! You can see you have done your job! You know that it's successfully transferred."

In summary, the research shows that users would like these services, which could be better delivered once a digital identity is in place.

Perception of digital identity within financial transactions

Brand perception and trust
The perception of digital identity was tested in two forms. The first was using GOV.UK Verify[4], the second replicated this scheme with a fictional MONEY.UK Verify brand.

Both brands were presented in the same way, with the four current certified GOV.UK Verify identity providers included.

The government brand was widely perceived as safe and trustworthy. Some privacy concerns were considered but largely accepted as "government already knew everything anyway".

> *"£76k is a lot of money to transfer online. I would be quite worried, but I am reassured by GOV.UK Verify."*

> *"I don't know how secure it is at the moment but because it is Gov you make the assumption that it should be secure".*

> *"If I see GOV.UK Verify it means my data has been checked."*

In comparison, the private sector MONEY.UK brand was a little less trusted, the principle reason being that the participants had never heard of it. They would be prepared to trust a brand that they were familiar with, through TV advertising for example. They also commented that trust would grow with repeated use, initially within low-value transactions, as confidence built. Analogies were drawn with the take-up of other online services, such as PayPal.
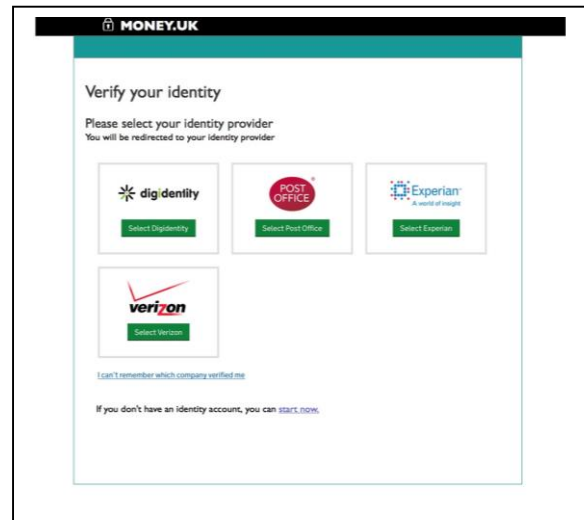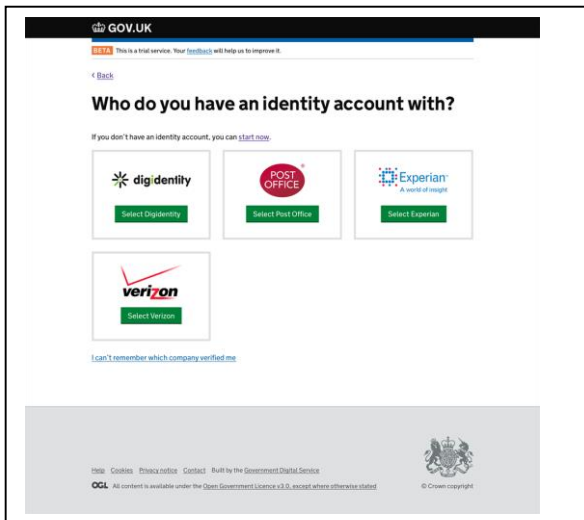
> *"Details should go to MONEY.UK [Verify] as it is safe, not on the company website as there could be fraud. MONEY.UK feels safer."*

> *"I would prefer institutions which use MONEY.UK by opposition to the ones that don't."*

> *"It's like PayPal. They are not getting my details; it feels safe."*

---

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

GOV.UK Verify and MONEY.UK Verify were presented in near-identical pages.

Using Verify to populate application forms

Verify returns the individual's forename, surname, date of birth, gender and address. Participants strongly welcomed the convenience of using this data to pre-populate forms. Where a form was presented on one page that required more data entry, such as their contact details, participants commented that they would have expected these to have been pre-populated as well.

> *"It's quicker than putting details in manually."*

> *"It avoids errors."*

On questioning and reflection, though, participants weren't so sure, with questions arising over who held the data and what it could be used for being an issue. This could have been due to a lack of clear explanation and transparency as to the purpose of the data collection.

> *"I wouldn't want to share my email or mobile number. Why do they need this? I am afraid it would be used for marketing purposes and I would end up receiving loads of emails and messages. Otherwise, I would be ok with it. I think there should be something that says that my data will not be shared with marketing companies."*

Verify returns information that can be used to populate forms. Users found this very convenient but had some reservations about how data would be used.

Participants' perception of the identity providers

During Sprint 1, participants were only asked to authenticate themselves (sign in) with the assumption being that they had previously registered with an identity provider for a government service.

Sprint 2 was as for Sprint 1 with the exception that they had previously registered for a financial service.

In Sprint 3, participants were asked to create a digital identity with an identity provider of their choice.

The brands selected were very important, based on trust which in turn was based on what was known about the identity provider. Adverse experience (eg Post Office queues) or perceptions of the brand (eg Experian associated with debt collection) also came into the trust equation.

Unsurprisingly,

Well-known brand + good experience = High degree of Trust

Well-known brand + poor experience / perception = Lower degree of Trust

Unknown brand = No degree of Trust

Participants were unclear about the role of identity providers. Some were confused about private sector companies having access to personal data being used with a financial transaction. This was even more evident during the registration phase when participants were being asked more probing questions about who they were interacting with and where the data was being held.

Although perceptions of the identity providers were clouded somewhat by a lack of brand awareness or past experiences, the participants were generally positive about Verify as a service and the involvement of private companies.

> *"Gov and private companies? Not too much of a problem. I am happy with anything that is more secure."*

> *"With MONEY.UK, Experian does not have all my details so they can't sell them. They are only checking that it is really me and confirming my details."*

Perception of the value of GOV.UK Verify digital identity

Value whilst signing-up with financial institutions

Participants generally found the digital identity useful as it saved them having to prove their identity through traditional means. The digital identity was often compared to PayPal because it acted as a third party enabling financial transactions whilst not processing all customer details. This association was positive.

Most participants, including those who undertook the registration process, thought the digital identity was worth the 10 minutes spent registering, as they could re-use it later.

The association between the government and financial services was explored. Most participants were comfortable with this and saw the government as the legitimate entity to provide means of identification.

> *"The process is very straightforward: the system picked up my info from Verify and double checked it. Other processes would be longer than that."*

> *"I would use Verify as it is a government thing, I expect it to be useful and trustworthy."*

Participants qualified this position of comfort, though, when asked to consider the question: "Who do you think is responsible if something goes wrong?". In this situation there was no clear view on who this should be. This is an area where further user research into the transparency and understanding would be useful.

> *"In the case of a problem Verify would be responsible. I signed up and trust them."*

Would the digital identity entice people to save more?
This question was evaluated in two forms.

The first used the digital identity as a means to prove one's identity and retrieve details to populate an online form. The second used digital identity as a companion service enabling users not only to prove their identity but also to underpin added-value services, such as a means to access and retrieve their savings accounts across multiple providers.

The interviews suggested that there was no direct relationship between the digital identity as a pure identification means and the savings behaviour, there has to be an intent to save in the first place.

> *"Having an easier or more complicated route to open an account would not make me save more."*

> *"Having a digital identity has nothing to do with saving more [...] it is not related."*

Following feedback from Sprint 1, a prototype of a companion service was developed to demonstrate a use case: using a digital identity to access and display all of a user's savings portfolio. Generally, participants felt this was a useful service. The portfolio enabled them to be aware of their current position and act upon it – although a decision to save more was ultimately dependent on current financial circumstances.

> *"[I would save more] because I can see what I have and what I am going to have."*

> *"To save more, I need to earn more, living in London is expensive."*

Offering users a clear multi-provider overview seemed to create greater awareness of the need to save, perhaps increasing the motivation to increase savings for both short and longer term needs.

Would the digital identity help people to manage their savings better?
This question was evaluated in two forms, as above. Generally, findings were in line with those above.

> *"You have a clear overview of all your financial products in one page"* … *"The portfolio thing, I like that bit, I love that bit really, I see all the providers in one place."*

Would people choose providers making use of the digital identity?
In Sprint 3, the prototype was developed to represent a market comparison site to gauge participants' views on the value of a digital identity when comparing providers. Providers who made use of the digital identity could be favoured by users compared to others who did not; the provisos being the terms of the offer were relatively equivalent (mostly interest rate and FSCS cover) and the brands were known.
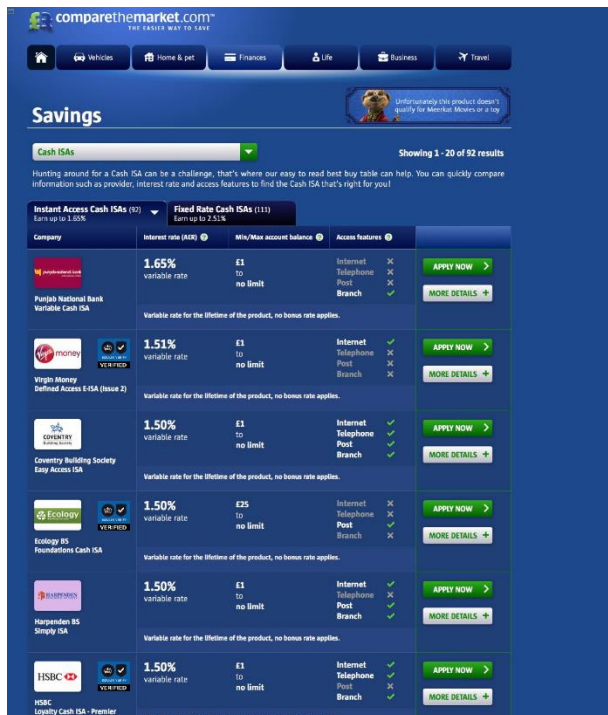
Simulation of a comparison site used in Sprint 3

Conclusions

The project set out to research the use of a digital identity within two prototype digital services: the first to open a new pension and the second to transfer a savings account.

Participants were asked to discuss their perceptions, expectations and concerns.

The conclusions drawn were as follows.

Using a digital identity. Participants were positive about using a digital identity as a convenient way of confirming their identity. They welcomed the involvement of government, through the GOV.UK Verify brand, as this gave a sense of comfort, security and trust.

Trust was extremely important to participants. In the scenario where the financial services industry 'owned' and branded the digital identity scheme, participants commented that it would take time to build trust as they became more familiar and confident with the brand and service.

Participants raised some concerns and questions in a couple of areas. One of these was with regard to who held their identity data and how it could be used. Another was that of liability and responsibility – who do you go to if something goes wrong?

Companion services. Participants were very positive about companion services that could be developed, such as the mocked-up savings portfolio page built for the research. These services, underpinned with a digital identity, negates the need for users to identify themselves

separately to each provider. Participants recognised the convenience of this, saving them time and effort.

Encouraging users to save more. Participants agreed that a companion service that enabled them to view their savings portfolio and understand whether they were saving at an appropriate level, was helpful to them. Whilst it encouraged awareness, personal circumstances would often dictate whether they could and would save more.

If a participant had made the decision to save more, the decision on choice of provider was driven initially by interest rate, brand awareness and membership of the FSCS. Thereafter, participants were more likely to choose a provider who accepted a digital identity.

Half of the participants had abandoned a savings account opening process in the past 12 months due to difficulties encountered, chiefly with proving their identity but also because the offer wasn't what they thought it was at the outset.

Taken together, the findings would suggest incorporating a digital identity into a digital service could reduce abandonment rates and reduce delays in opening or transferring a savings account. Whether the overall level of savings would rise cannot be directly inferred.

Future considerations

During the course of this Discovery project, a number of matters arose that were deemed to be outside the immediate project scope. They would need to be addressed, however, if the concept of a digital identity in financial services is to move forward. The work to date of the Government Digital Service and the transformation of public services programme, together with the findings of previous OIX Discovery and Alpha projects, would provide valuable insight into these areas for future consideration.

Two of these areas are discussed below. Other matters, such as legal and commercial models and arrangements, and technical standards, were not addressed.

Suitability of a Verify-issued digital identity in the financial services industry

Identity verification is only one part of a financial institution's Customer Due Diligence (CDD) process. That said, a digital identity infrastructure based on government standards could be of value to financial institutions in Customer Due Diligence (CDD) processes but it does not relieve them of their full regulatory obligations which includes compliance with Know Your Customer (KYC) and Anti Money Laundering (AML).

Being able to accept a digital identity would greatly simplify the identity assurance process for financial services firms and their customers alike. Identity providers, contracted to Cabinet Office for GOV.UK Verify, are developing new data sources for evidence of identity beyond those traditionally used by banks when opening an account. These new data sources will help, for example, people with little or no credit history obtain a digital identity, an area that has been traditionally weak in the financial services market.

A digital identity, issued by an identity provider, is assured to a level that is defined in the government document GPG 45[5]. GOV.UK Verify currently provides identity proofing to Level of Assurance (LoA) 2. An LoA 2 Identity is defined as "*a claimed identity with evidence that supports the real world existence and activity of that identity. The steps taken to determine that the identity relates to a real person and that the applicant is the owner of that identity might be offered in support of civil proceedings*".

The focus of this project has been on conducting customer insight research into the use of a digital identity when opening a new savings product. It is recognised that this forms only part of the wider TISA initiative that is looking for a comprehensive digital solution to opening a new savings account that is fully compliant with identity assurance, KYC and AML requirements.

A separate OIX white paper, *Digital Identity Across Borders: Opening a Bank Account in Another Country[6]*, looks at digital identities created under the new EU Regulation: Electronic Identity and Authentication Services (eIDAS). It reports on the use of digital identities by foreign nationals opening a bank account in the UK.

Other industry matters such as branding, legal positions, commercial models and technical standards enshrined in trust frameworks would also need to be addressed.

Addressing data protection and privacy

Post the identity card era and at the outset of the government's journey to develop an identity assurance service (ie GOV.UK Verify), the government approached a number of privacy and security experts to establish the Privacy and Consumer Advisory Group. This group was asked to develop a set of guiding principles that would allow individual users of the identity assurance service to control when to reveal their own identifying information and the minimum data to reveal. These principles were published in 2013 as the Identity Assurance Principles[7] and were applied to the design of Verify (referred to as privacy by design).

These guiding principles could be considered as part of an identity assurance scheme adopted by the savings industry.

---

[5] See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/370033/GPG_45_identity_proofing_v2_3_July_2014.pdf
[6] See http://oixuk.org/wp-content/uploads/2016/02/Digital-Identity-Across-Borders-FINAL-Feb2016-2.pdf
[7] See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/361496/PCAG_IDA_Principles_3.1__4_.pdf