OIX United Kingdom

The value of digital identity to the financial service sector

Exploring the reuse of a GOV.UK Verify digital identity in a financial service application process

Sponsored by:

BARCLAYS

Contributors:

AVIVA Experian HiFX meeco POST OFFICE innovate identity verizon

Author: Bryn Robinson-Morgan

Published: December 2016

Executive Summary

Contents

Readership

This white paper is for senior leaders responsible for customer due diligence within:

- *Financial service sector*
- *Government and regulators*
- *Identity community*
- *User experience / design community*

"The digitisation of banking is potentially one of the biggest single changes to the banking sector in recent memory. The sector has long since digitised the holding of money. Yet for many years this operated in the background. The advent of the internet and the smartphone has transformed the ability of the customers to access their accounts digitally."
Anthony Browne, Chief Executive, British Bankers Association[1]

Digitisation of services brings great benefits to customers: immediacy and convenience, access to new services, greater choice and market competitiveness. It also brings concerns and fears: it can create barriers to entry and a lack of inclusion, along with the threat of data breaches[2], misuse of personal information[3]; identity theft, fraud[4], and sometimes financial loss.

These concerns could undermine customers' confidence[5] [6]and patience in using services online. They are challenges for the banking and wider finance industry to address and overcome. One root problem to these concerns and challenges is that of identity. How can we provide an understandable, convenient, safe and trusted solution to manage and protect our identities online?

The UK market for identity solutions to meet these requirements is highly fragmented[7]. The financial services industry is highly regulated when it comes to identity requirements and it is recognised there is a need to embrace innovation in this area.

"The government ... has agreed with the Joint Money Laundering Steering Group (JMLSG) that they will modernise their guidance on electronic ID verification to support the use of technology to access financial services"
Philip Hammond, UK Chancellor[8]

In May 2016, the UK government formally launched their new digital identity program, GOV.UK Verify[9]. It aims to provide a safe, simple and secure means of citizens proving that they are who they say they are when transacting online with government services. This service currently has 1 million users, with an ambition to scale to 25 million users by 2020.

Both the government and the private sector believe that the market place for identity should not be sector specific and that economies of scale could be reached through the reuse of a trusted citizen digital identity, driving down the cost of identity for the UK as a whole.

[1] https://www.bba.org.uk/publication/bba-reports/digital-disruption-uk-banking-report-2/
[2] http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
[3] http://www.ibtimes.co.uk/facebook-faces-eu-court-justice-over-user-data-misuse-wake-prism-spying-scandal-1493265
[4] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudstatistics/yearendingmarch2016
[5] http://www.encodegroup.com/industry-news/consumer-confidence-rattled-by-data-breaches
[6] https://www.nccgroup.trust/uk/about-us/newsroom-and-events/press-releases/2016/january/63-of-consumers-think-their-financial-information-will-be-hacked-within-the-next-year/
[7] http://oixuk.org/wp-content/uploads/2016/06/UK-Private-Sector-Needs-for-Identity-Assurance.pdf
[8] http://citywire.co.uk/new-model-adviser/news/autumn-statement-treasury-looks-to-boost-access-to-online-financial-firms/a973301
[9] https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify

This report focuses on the challenges faced in enabling trusted online transactions within the financial service sector, and explores whether digital identity reuse offers a solution. Specifically, the project looked at three areas:

- Firstly, feedback was taken through user testing from customer participants around their inclination to reuse a government endorsed digital identity to open a bank current account.
- Secondly, four leading financial service providers were interviewed to understand their views around identity reuse, and the strengths, weaknesses, opportunities and threats of such a proposal.
- And thirdly, the target model for implementation was assessed to ascertain the practical steps that would need to be taken, and by which stakeholders, to make identity reuse across multiple sectors a reality.

The principal findings were as follows:

User Research

Users' initial views and expectations were mixed, with many describing past experiences and frustrations trying to transact online with a financial services provider. Proving one's identity being one such example. However, most users were positive about the experience of reusing a digital identity within the context of the research.

What did users say?

- Simple
- Easier
- Quicker
- Secure
- Better

As part of the research, users were asked to open a bank account online, reusing a digital identity previously obtained to complete a government digital service. Most expressed delight in the journey being frictionless and easy to complete. The time saving upfront in an application process was a clear incentive. Users became advocates of the process, stating they would recommend it to a friend and they thought it of value that the digital identity was endorsed by government.

Financial Services Providers

"Verify offers the beginnings of a solution which could revolutionise how we and other banks ID our customers."
VP AML Policy, Financial Crime Risk – Barclays

The financial service providers were optimistic about the potential for reuse of a digital identity. One of the key benefits was the support it provided with customer on-boarding and inclusion, enabling more customers through the process with an improved customer experience. They felt it would help with some of the impending regulation faced by financial services firms and with authentication, e.g. payment instructions. They also felt it had the option to reduce the risk of their customers falling victim to scams.

In order to be successfully adopted in financial services, providers felt that digital identity reuse would need to be able to link additional attribute information specific to financial services e.g. proof of income, the ability to report fraud in a simple way and would need customer confidence and understanding.

The providers were acutely aware, however, of the challenges the industry is facing to implement new legislation and regulation (e.g. 4MLD[10], PSD2[11], PAD[12], eIDAS[13], GDPR[14] and the Open Data

[10] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2015_141_R_0003&from=ES
[11] http://ec.europa.eu/finance/payments/framework/index_en.htm
[12] https://www.fca.org.uk/firms/payment-accounts-directive

Standard). Prioritisation of resources and funding will be focussed on implementing these over the next 3 years and that will inevitably have an impact on the adoption of new technology such as digital identity.

Target Model Considerations

There are compelling reasons why an industry approved digital identity scheme is needed by both financial services providers and their customers. The reuse of a GOV.UK Verify digital identity offers a potential opportunity to meet this need.

Target Operating Model Considerations

- Standards
- Governance
- Privacy
- Branding
- Role of Government
- Integrity
- Commercials
- Liability

To make progress, this paper recommends a number of important next steps for government, for financial services providers and for the identity community.

Critically the UK government need to provide their plan for GOV.UK Verify and how they intend to support its scale to 25 million digital identities by 2020. There is also a need for clear alignment of Cabinet Office and the Treasury around financial services regulation to allow digital identity reuse. Additionally, government need to fully address the needs of the private sector and fill any gaps in the model. One example is attribute exchange; this will be imperative for a fully functioning UK wide identity ecosystem.

Financial service providers should start developing a cost benefit analysis for digital identity reuse within their specific organisation.

The identity community needs to create a cross industry working group and develop the commercial model which can be shared with financial services providers. They also need to create a plan to increase customer awareness.

These should be addressed as a priority to support the potential benefits that could be realised of a trusted cross-sector UK digital identity program.

To take the proposition forward with purpose the following needs must be addressed:

- Scale of identities within GOV.UK Verify
- Fill the gaps in the model
- Alignment of Cabinet Office and Treasury
- Regulatory approval
- Creation of a cross industry working group
- Commercial model
- Customer awareness and education

[13] https://ec.europa.eu/digital-single-market/en/trust-services-and-eid
[14] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

Background

What is a Digital Identity?

In very simplistic terms a digital identity is a digital representation of your real-world identity. Digital identities are an essential part of the transformation of online services, the "key to the door" of digital transactions. The utopia is a digital identity that is secure, trusted and accepted by the industry wherever a customer chooses to use it. At present we all have multiple digital identities, typically a unique one with each service provider, designed around traditional company and organisation- centric service delivery and business models. But this model is fast-changing with the emphasis in the digital world now on the age of the customer[15] and user-centric service design. To support this, a new approach for digital identities has emerged. One where the user is in control of their identity. This project explored the use of a single digital identity to access multiple services from the user, provider and industry perspectives.

Financial Services Industry Identity Needs

The financial services industry is required to complete Know Your Customer (KYC) checking for the verification of identity to comply with regulation. This is a risk based approach, which is open to interpretation on a product and institution basis.

The industry is currently undergoing a dramatic transformation as it embraces the digital revolution. Increased customer engagement and better experience, choice, competition, transparency, and new and innovative services are some of the desired outcomes being driven in part by a technology revolution and in part by EU and UK government initiatives and policy. A raft of UK and EU Directives, Regulations and initiatives have to be implemented over the next 3 years.

Regulation / Initiative	Date of Implementation
EU Payment Account Directive (PAD)	September 2016
EU Fourth Money Laundering Directive (4MLD)	June 2017
Open Banking (Competition and Markets Authority)	Early 2018
Second Payment Services Directive (PSD2)	January 2018
General Data Protection Regulation (GDPR)	May 2018

The current approach to these regulations by financial services is to see and satisfy them in isolation. For example, in response to PSD2 and Open Banking financial services firms are building multiple application programming interfaces (API's) to deal with the demands of the requirements. However, the common theme that can be found in the entirety of these changes is that of identity. Whether to open or manage an account, initiate a payment, share personal data between organisations, or protect the customer and prevent the misuse and abuse of personal information and fraud; strong customer identification and authentication is essential. And in the case of the digital revolution, this means that strong customer identification and authentication has to be achieved in a way that is convenient, quick and secure for each and every customer who wishes to use it, otherwise it will fail to be widely adopted.

That being the case, new approaches to how identities are managed, which are consumer centric, rather than organisation centric, could allow improved convenience for users and play a strong role

[15] http://www.forbes.com/sites/jimblasingame/2014/01/27/its-the-age-of-the-customer-are-you-ready/#54b73c095324

in satisfying not only requirements for data portability within PSD2 and Open Banking, but those of privacy regulations such as GDPR too. Additionally, changes in the 4th Money Laundering Directive should allow organisations to rely on each other more for identity, paving the way for these new models to develop. However, the risk based approach to KYC of financial services institutions doesn't easily lend itself to interoperability of customer identities because of the potential for interpretation by each institution.

UK Government Strategy

In May 2016, the UK government formally launched their new digital identity scheme. GOV.UK Verify[16] provides a safe, simple and secure means of citizens proving that they are who they say they are when transacting online with government services.

GOV.UK Verify is a federated identity scheme that uses an approved panel of certified private sector companies to confirm the identity of individuals. The user chooses one of the certified companies to create their identity account or profile. The user provides their name, address, date of birth and optionally, their gender, as identity attributes to be verified, they also have to provide evidence that they are the owner of that identity. The certified company then validates the information and verifies the user's claim to the identity through a detailed identity checking process against multiple authoritative sources of data. The identity is verified to a standards based level of assurance (LoA), as opposed to risk based meaning an identity verified to a certain level is clearly defined and not open to interpretation, this makes interoperability easier.

Once their identity is verified the user is able to assert it by signing in to their chosen identity provider using a two factor authentication method. The user benefits by registering and verifying their identity once, and being able to reuse this trusted digital identity many times. The identity provider delivers ongoing protection and monitoring of the account and the associated identity is re-verified periodically. The GOV.UK Verify service is currently only available for use in government transactions. Currently there are 1 million people in the UK with a GOV.UK Verify digital identity, the ambition of the is to scale this to 25 million by 2020.

A Cross Sector Approach – Government and Financial Services

The Open Identity Exchange (OIX) UK recently published the outcome of research into the UK private sector needs for identity assurance[17]. This report concluded that there was a significant appetite for organisations to collaborate around digital identity needs with 81% of respondents indicating that they wanted to pursue a cross industry approach to this topic.

Perceived benefits of a UK-wide approach to digital identity were the creation of a better customer experience, on-boarding cost savings, portability and economies of scale. There were also challenges cited in the research around regulatory acceptance, liability, competition, standards and privacy. The highest number of respondents to the research were from financial services organisations, indicating that this sector should be the starting point for further discussion. For the government, having private sector opportunities for reuse of a GOV.UK Verify identity extends the benefits for users. It becomes motivational to the user and makes the initial effort of registration more attractive. Having a trusted digital identity is also seen as a key enabler for digital inclusion[18], this aligns with UK government strategy.

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

[17] http://oixuk.org/?page_id=2111

[18] https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

Scope

Context

The context for this project was a real-time application process to open a bank account. It offered users the opportunity to use a GOV.UK Verify digital identity as a means of establishing their identity with the financial service provider. The digital identity was assumed to have been previously obtained to access a government service. This reuse of the digital identity replaced traditional forms of identity verification such as government-issued documents, or one-time digital identity verification as part of the online application process.

Focus

The project explored three areas:

1. Customer Research
   - Users' perceptions and understanding of this approach, including feelings around ease-of-use and safety online.
2. Financial Sector Analysis
   - The implications of a federated digital identity program for financial institutions, including the issues that would need to be addressed in any program, to meet their regulatory and service requirements. The project also considered how other Anti-Money Laundering (AML) Customer Due Diligence (CDD) checks could be accommodated within the real-time application process. These are required in order to ensure a fully compliant process.
3. Target Operating Model
   - How a Target Operating Model for the industry could be reached. This model considered how all stakeholders, that is financial institutions, Identity Providers (IDPs), attribute providers, users and hub providers, could interoperate and the aspects of this model that would need to be addressed. Standards, certification and governance were considered as part of this.

Hypotheses

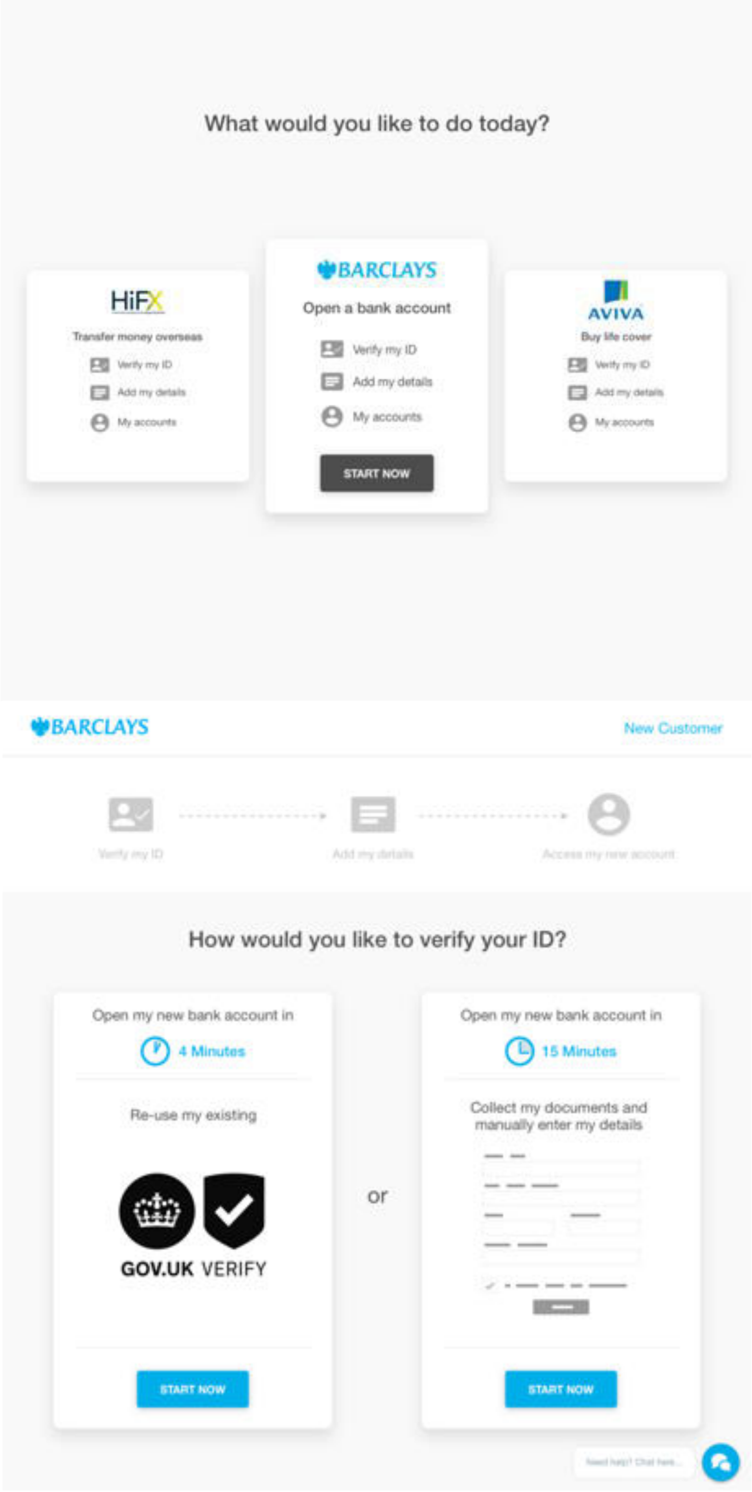
There were two hypothesis tested:

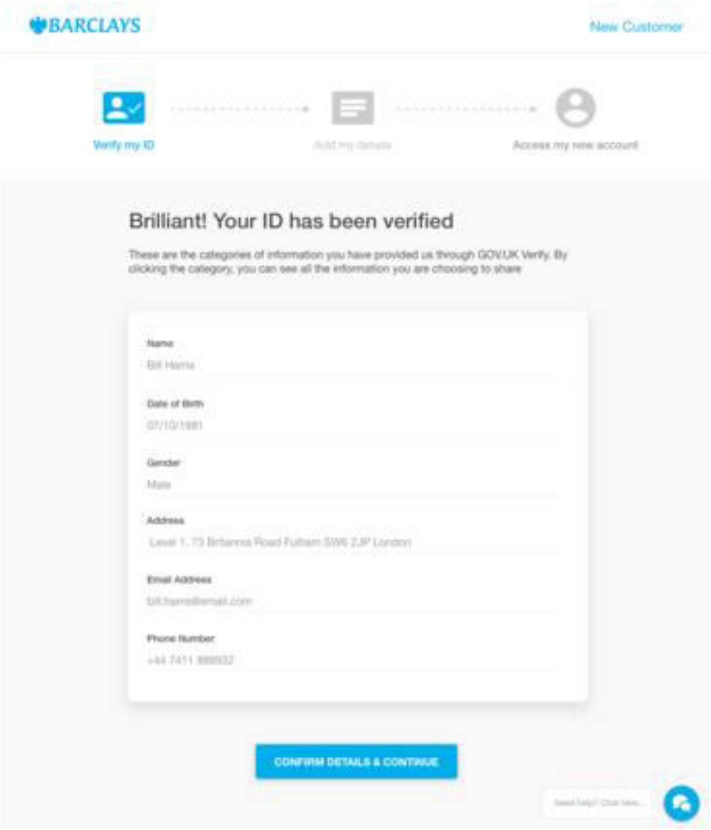
Customers are more inclined to complete the application process for a financial service product that enables them to reuse an existing assured digital identity

Financial service institutions would accept an assured digital identity from a third party provider as part of their product application process if an established trust framework met their regulatory and service requirements

Methodology

To test the customer hypothesis, user experience labs were held using a prototype journey for a bank account opening application. The prototype allowed the reuse of GOV.UK Verify as a means of identity verification. A benefit of time saving was offered as user motivation.





Brilliant! Your ID has been verified

These are the categories of information you have provided us through GOV.UK Verify. By clicking the category, you can see all the information you are choosing to share

Name
Bill Harris

Date of Birth
07/10/1981

Gender
Male

Address
Level 1, 73 Britannia Road Fulham SW6 2JP London

Email Address
bill.harris@email.com

Phone Number
+44 7411 888932

In order to understand the demands and opportunities the reuse of digital identity create, when applied by the financial sector, the user research labs explored:

- What users understand about digital identity
- How they felt using a federated digital identity
- If they felt the process was secure
- Their thoughts about the brand
- How they selected their choice of identity provider

The project sought to understand the needs of the Financial Institutions. Analysis of what would drive them to adopt this new approach versus current methods was undertaken. A series of workshops were held with financial service providers. The workshops gained an insight to the providers needs of a trusted digital identity scheme.

Throughout the project, the role and Target Operating Model of the hub was explored. In collaboration, the financial service providers and identity providers expressed their needs. The role of a hub provider in meeting these needs was considered.

Customer Research

Hypothesis

Customers are more inclined to complete the application process for a financial service product that enables them to reuse an existing assured digital identity

Research approach

In order to test the hypothesis, qualitative research methods were employed through the performance of user labs. 15 participants were recruited to each partake in a one hour 1-1 researcher led session. The participants were required to be digitally active, have recently applied for a financial service product and have an awareness of federated identity.

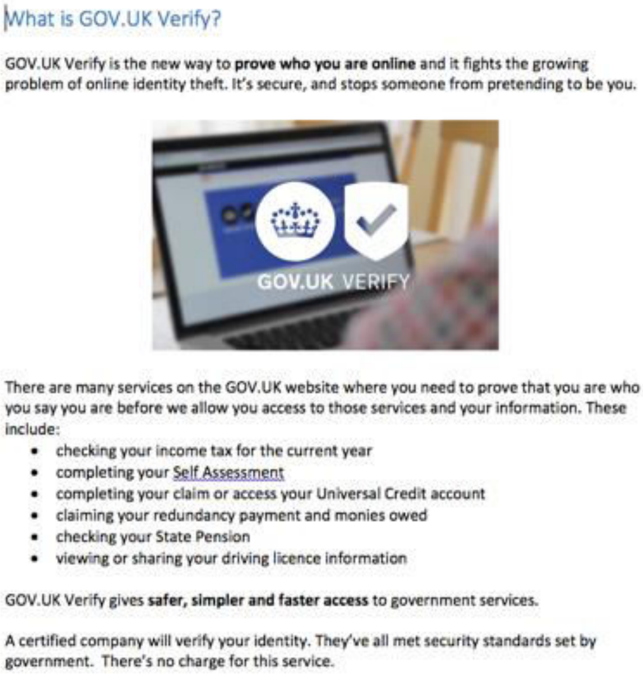
The participant's attitudes towards internet usage, exposure to needing to prove their identity online, and experience of applying for financial service products was gauged by the researcher.

It is important to note that asserting identity is one part of financial service product application. The user testing did not validate whether the application would actually be successful.

Establishing understanding

As the hypothesis assumed the reuse of an existing digital identity, it was important that the participants had a good level of understanding regarding GOV.UK Verify. In order to establish this understanding, the participants were provided with stimulus materials that explained:

- An overview of what GOV.UK Verify is
- Details of how GOV.UK Verify works
- Information on how the identity account/profile is reused and maintained



What is GOV.UK Verify?

GOV.UK Verify is the new way to **prove who you are online** and it fights the growing problem of online identity theft. It's secure, and stops someone from pretending to be you.

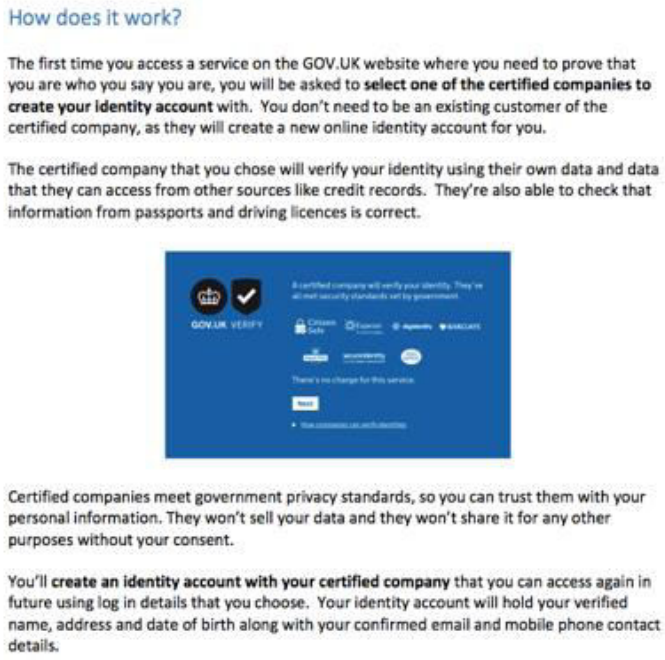
GOV.UK VERIFY

There are many services on the GOV.UK website where you need to prove that you are who you say you are before we allow you access to those services and your information. These include:

- checking your income tax for the current year
- completing your Self Assessment
- completing your claim or access your Universal Credit account
- claiming your redundancy payment and monies owed
- checking your State Pension
- viewing or sharing your driving licence information

GOV.UK Verify gives **safer, simpler and faster access** to government services.

A certified company will verify your identity. They've all met security standards set by government. There's no charge for this service.



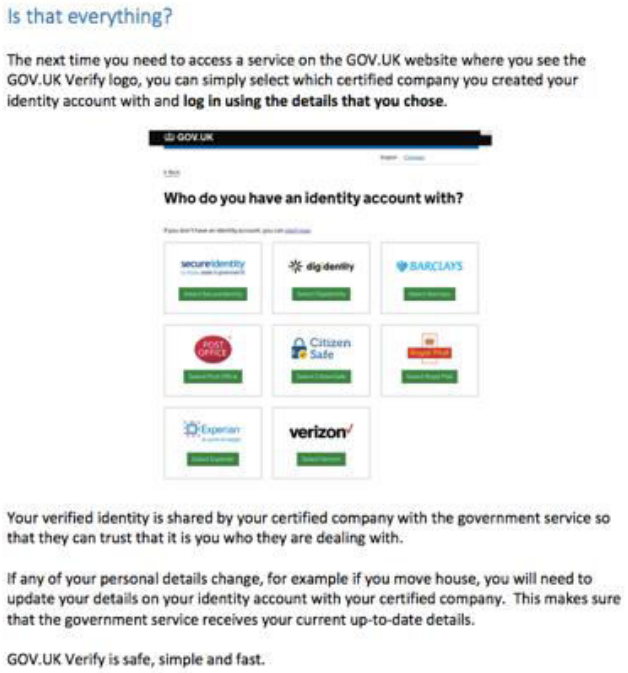
How does it work?

The first time you access a service on the GOV.UK website where you need to prove that you are who you say you are, you will be asked to **select one of the certified companies to create your identity account** with. You don't need to be an existing customer of the certified company, as they will create a new online identity account for you.

The certified company that you chose will verify your identity using their own data and data that they can access from other sources like credit records. They're also able to check that information from passports and driving licences is correct.

Certified companies meet government privacy standards, so you can trust them with your personal information. They won't sell your data and they won't share it for any other purposes without your consent.

You'll **create an identity account with your certified company** that you can access again in future using log in details that you choose. Your identity account will hold your verified name, address and date of birth along with your confirmed email and mobile phone contact details.



Is that everything?

The next time you need to access a service on the GOV.UK website where you see the GOV.UK Verify logo, you can simply select which certified company you created your identity account with and **log in using the details that you chose**.

GOV.UK

Who do you have an identity account with?

secureidentity
digidentity
BARCLAYS
POST OFFICE
Citizen Safe
Royal Mail
Experian
verizon

Your verified identity is shared by your certified company with the government service so that they can trust that it is you who they are dealing with.

If any of your personal details change, for example if you move house, you will need to update your details on your identity account with your certified company. This makes sure that the government service receives your current up-to-date details.

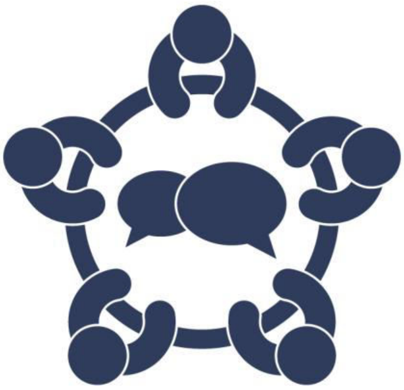
GOV.UK Verify is safe, simple and fast.

The participants were asked to explain to the researcher what GOV.UK Verify was before the reuse task began. The participants were taken through a guided task of applying for a bank account as a new customer. A mid-fidelity clickable prototype was used, without data entry. This introduced the ability to reuse an existing GOV.UK Verify identity by signing into a chosen identity provider.

Participant background

All of the participants felt comfortable using online banking and social media. Typical tasks that the participants had undertaken included having checked balances, set up payees and made payments online. Many of the participants used smartphone apps for their online banking activity. The majority had used their social media accounts to login to another website or service. Those who hadn't were wary of a loss of privacy through sharing information between their social media account and a third party.

All but two of the participants had experience of opening a new bank account within the past year. Many of them encountered both online and offline elements of the application journey. Branch visits, phone calls and online form filling were stated as particular frustrations; with the more stages involved increasing the level of frustration felt. Most participants recalled identity verification as part of the process. This included requirements to scan passports or physically attend a branch to show identity documents. Those participants who had been able to complete the process entirely online expressed the greatest level of contentment in the application process.



"The government account gives me the extra sense of security."
Tasman, 20

"The process was amazing – really simple, I could do It in 20 minutes just before I go to bed"
Tara, 46

"The Verify route looks the easiest. If I had Verify set up I would choose it as it saves time."
Veronica, 46

"This process cut out a load of time having to fill forms out and obviously, the information is verified."
Fabian,18

"Much easier than the last time I set a bank account up. It's good that this can be done in less than 5 minutes."
Paidraig, 39

Participant expectations

Mostly, participants had experience of having to verify their identity online, this included for:

- Employment background checks
- Registering for an online gambling account
- Conveyancing
- Obtaining a travel visa
- Buying insurance
- Becoming an online seller

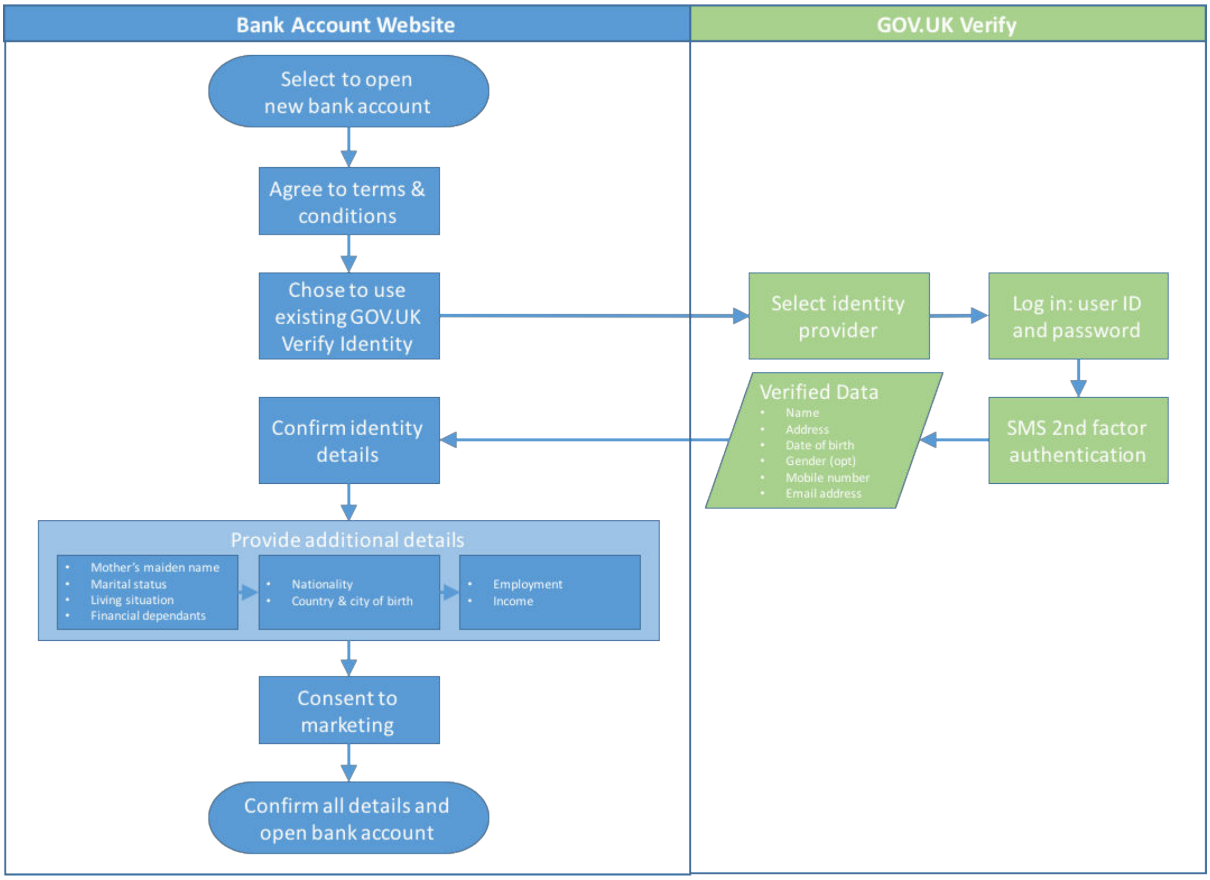
This was seen as a necessary process that participants were mainly fine with undertaking. Some wariness was expressed, particularly when the website was less known and trusted.

Based on previous experience, the majority of participants believed the application for a bank account would take around 20-30 minutes. There was an expectation that as a new customer identity verification was required. Whereas for an already established relationship, the expectation was the bank would have all the information required already. Generally, a benefit of time saving was expected by reusing the GOV.UK Verify identity.

Some participants would expect that if they did not already hold a GOV.UK Verify identity, that by manually completing the bank application they would obtain one at the end of the process.

Research stimulus

A prototype journey for opening a new bank account was used as the stimulus for the user research lab. The prototype journey took the participants through an application process using their existing GOV.UK Verify identity.



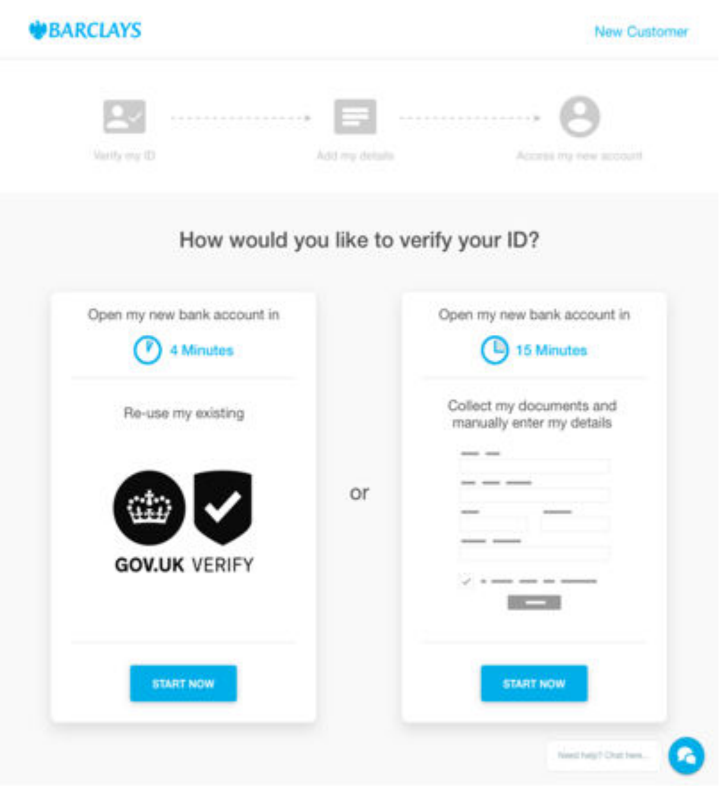
Participant Feedback

The GOV.UK Verify brand was not previously known to the participants. A reasonable level of understanding was reached with most before the reuse task was introduced. The safety and security aspect seemed to be valued, with the Government involvement providing reassurance that it could be trusted. That this was offered at no charge was highlighted as a positive.

There was a degree of confusion in the role of the identity provider. There was also scepticism that the customer's details wouldn't be used for other purposes e.g. marketing. For most participants, a strong brand recognition was important in their choice of identity provider.

There was a low level of recognition that they were transferred into their identity provider's domain, away from the bank application, to sign in to their GOV.UK Verify account. Some participants picked up on the 'cognitive dissonance' of using a provider like Post Office to verify the creation of a financial services product with a competing provider.

Participants generally understood the sharing of verified identity information between their identity provider and the financial service provider. Having to provide additional personal data in order to complete the bank account application proved to be jarring. Many participants expressed a desire to either store additional information with their identity provider, or for their identity provider to derive it from other attribute providers. An example stated was taking their nationality from their passport details or deriving their income from their credit file.



How would you like to verify your ID?

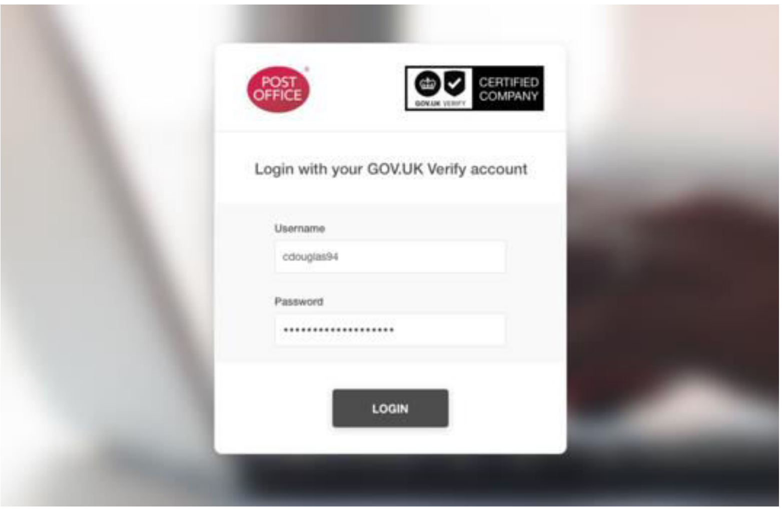
Open my new bank account in 4 Minutes

Re-use my existing

or

Open my new bank account in 15 Minutes

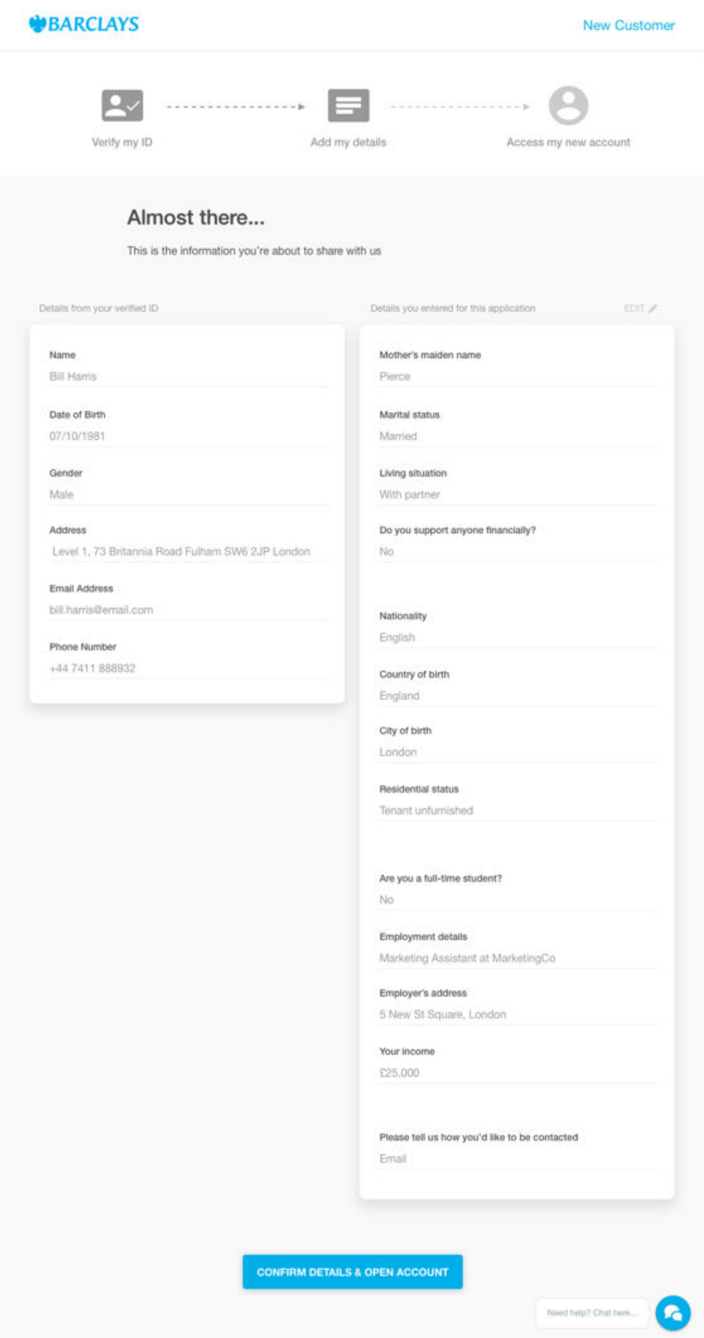
Collect my documents and manually enter my details



Login with your GOV.UK Verify account

Username
cdouglas94

Password
•••••••••••••••••••



Almost there...

This is the information you're about to share with us

Details from your verified ID

Name: Bill Harris
Date of Birth: 07/10/1981
Gender: Male
Address: Level 1, 73 Britannia Road Fulham SW6 2JP London
Email Address: bill.harris@email.com
Phone Number: +44 7411 888932

Details you entered for this application EDIT

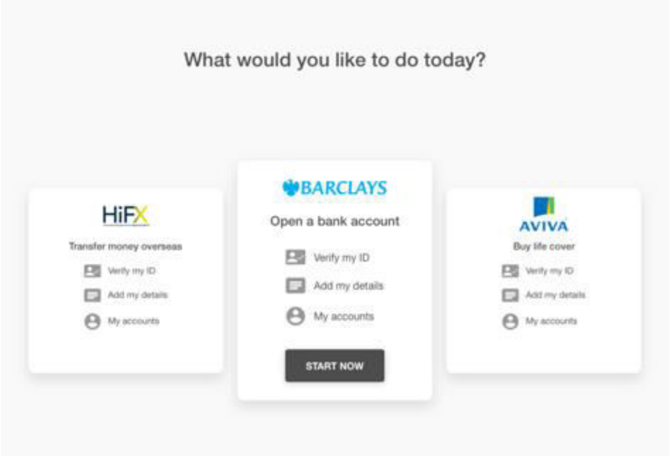
Mother's maiden name: Pierce
Marital status: Married
Living situation: With partner
Do you support anyone financially?: No
Nationality: English
Country of birth: England
City of birth: London
Residential status: Tenant unfurnished
Are you a full-time student?: No
Employment details: Marketing Assistant at MarketingCo
Employer's address: 5 New St Square, London
Your income: £25,000
Please tell us how you'd like to be contacted: Email

When being asked to review their information, it was generally well understood the difference between data received from the identity provider and the additional information they had manually entered. There was limited recognition of their identity data being verified and therefore not editable within the process. This could be a cause of confusion until the GOV.UK Verify identity is more widely used and understood.

It was generally expected that they would be provided with specific bank login credentials for online banking. Though some did think it possible to reuse their GOV.UK Verify identity as a log in to their new bank account. Having the option of both bank issued credentials or reuse of GOV.UK Verify was seen as a viable option by some, though for others this was seen as inappropriate.

Whilst reuse of GOV.UK Verify for online banking log in could be viable in future, it may be seen as a barrier until knowledge and awareness of federated log in is more widely accepted.

Looking specifically at other financial service transactions: for online money transfer there was a general expectation that this was already a quick process (5 minutes) and therefore a benefit of time saving would be difficult to achieve; for a life insurance application this was seen as being a more complex process requiring much more detailed information (such as medical background) and therefore the proportion of effort saved was believed to be less.



Key insights

Overall, there were no significant barriers cited to the concept of reuse of a GOV.UK Verify identity in a financial services transaction. Participants expressed frustration with current financial service on-boarding processes and saw them as a barrier to completing an application. They thought that the use of a digital identity made the process simpler, quicker and more secure.

The majority of participants gave positive feedback and stated they would recommend it to others if it were available. Participants expressed delight in the application journey being frictionless and easy to complete. The time saving upfront was a clear incentive to respondents. They felt using the digital identity could be used to remove complexity. There were some privacy concerns stated however, the fact the digital identity was endorsed by government seemed to mitigate these fears.

Additionally, participants felt the digital identity could be of use in other online transactions.

Other transactions where participants would use a digital identity:

- Financial Services: Insurance, Loans, Mortgages, high value transactions
- Employment: Application and screening
- Property: Buying/selling a house, renting, mortgage transfer
- Age verification: Purchasing age restricted products, gaming and adult sector
- Travel services: Booking, providing passenger details, visas
- Business: Registering a company or charity
- Utilities: Switching suppliers, house moves

Financial Sector Analysis

Hypothesis

Financial service institutions would accept an assured digital identity from a third party provider as part of their product application process if an established trust framework met their regulatory and service requirements.

Research Approach

In order to test this hypothesis a SWOT analysis was performed with the Financial Service providers involved within the project. A future vision was stated where 50% of the UK adult population have a verified digital identity, that is accepted by 50% of UK Financial service institutions as a means of proving their identity when transacting online. The citizen's digital identity wallet is approved by the Government and the UK Regulators to enable them to use on a regular basis in their online lives.

Key Challenges

As we move increasingly to a digital world, customers expect to be able to transact in the channel of their choice with immediate outcomes to their needs. Customers expect to be able to pass identity verification, and they often feel unfairly treated if they're asked to complete additional steps. Account opening processes for non-face-to-face transactions traditionally base their identity verification processes on information available from the customer's credit reference data. This creates a challenge for enabling those with a "thin" credit file, such as younger people, new to country or those with limited recent financial interactions.

An increasingly diverse credit ecosystem is moving a proportion of financial interactions out of the mainstream supply; this results in further fragmentation of data available to verify a customer's identity through traditional means. The lack of available data is often due to limited data sources or a lack of customer consent to use the data that does exist.

With more customer interaction coming through electronic means, the need to keep name and physical address details up to date becomes secondary to maintaining email or mobile contact details. Time spent with a customer face-to-face becomes scarce, and therefore more valuable; neither the financial service provider nor the customer wish to spend this time undertaking administrative tasks.

Macro Trends

Customers are using more products and services than ever before. This creates an increased need for identity verification and strong customer authentication. Customers are also more savvy in regards to how their data is used; demanding greater levels of privacy, control and granular consent. Financial service providers have to respond to these customer expectations, as well as meeting increasingly robust financial and operational risk controls.

Regulatory change brings both threats and opportunities to financial service providers. Being able to deliver innovative customer centric products and services, that leverage the advantages that regulation brings, can create the greatest returns on investment for providers. Frictionless identity verification, improved customer experience, greater fraud control and unlocking additional verified data attributes for risk decision making are current business needs. A trusted digital identity that can meet these business needs and meet the regulatory obligations will create a compelling business case for adoption.

Strengths

For a financial service provider to adopt the reuse of an existing GOV.UK Verify Identity into their product application process there were a number of beneficial reasons identified as part of the SWOT analysis. Many providers already utilise digital means of performing customer due diligence checks. The benefits of allowing the customer to assert their identity using an existing GOV.UK Verify Identity were seen as providing a strong identity that has been verified to the highest standards in comparison to existing methods generally deployed. With these standards being already established, the risk to a financial service provider were lowered as the identity verification methods were proven.

Having an identity that was endorsed, though licenced branding, by the Government was seen as being valuable in establishing trust. This applied for both the providers and their customers. With the abandonment rates for product applications being high, being able to reduce customer friction and mitigate the key reasons for lack of trust with the existing process were seen as strengths for reuse of an existing identity. With consent and control of the personal data being with the customer, a sense of ownership is established. This improves the propensity for sharing data with the financial institution in a trusted manner.

Using a federated identity model was highlighted as a positive due to the interoperability within a cross sector marketplace. The federation provides a shared responsibility to maintain the reputation of the identities asserted by it – delivering benefits of continued evolution of the strength of the assurance provided. Financial service providers would obtain collective specialism from the federation of identity providers, to complement their own expertise. This may be of benefit in the continued battle to remain ahead of cyber criminals and identity fraudsters.

Weaknesses

In order to develop the business case for adoption, the volume of available existing GOV.UK Verify identities would have to deliver sufficient scale. Without scale it may not be viable for financial service providers to change their current application journeys. The reuse of an existing digital identity would likely sit alongside current methods used today. A lack of awareness and understanding by customers of the benefits of a digital identity will be a barrier to adoption that will need to be addressed. The federated digital identity concept is not easily understood by customers. Perceptions of privacy concerns – the Big Brother society – would require investment in marketing and education to raise awareness.

The standards that govern the GOV.UK Verify scheme are not widely understood by financial service providers. The federation has a role to play in raising the level of knowledge within the sector. Identity is only one part of the customer due diligence process; whether a financial service provider:

- can do business with the customer once identified
    - for example, are they sanctioned individual?
- whether they should do business with them

- for example, is the product suitable?

These are distinct processes from establishing the identity itself. Having a reliable and trusted means of establishing the identity gives rise to opportunities for attribute enrichment to satisfy the other requirements of customer due diligence.

A central, commercial, driving force for the adoption of a standards driven digital identity scheme currently does not exist. This may slow the adoption by financial service providers. Having the endorsement of the industry regulator could be the catalyst for such a driving force to be established through industry collaboration on this initiative.

Opportunities

Opportunities exist for financial service providers to reduce their costs by reusing an established digital identity. The percentage of customers who they are unable to verify would be reduced in comparison to their existing processes. Customers who currently abandon the application process can be capitalised upon by removing barriers of privacy, complexity and the need to step out into another channel to complete the process.

A trusted digital identity can underpin the financial service provider's digital strategy. Opportunities to migrate a greater percentage of their customer base online by opening up this channel to more customer segments through a wider range of services. By reducing friction and transaction length, the overall customer experience can be improved. This will drive customer advocacy for their digital services.

The development of a unified, trusted brand, can be a catalyst to a reduction in fraudulent applications and opportunistic identity theft.

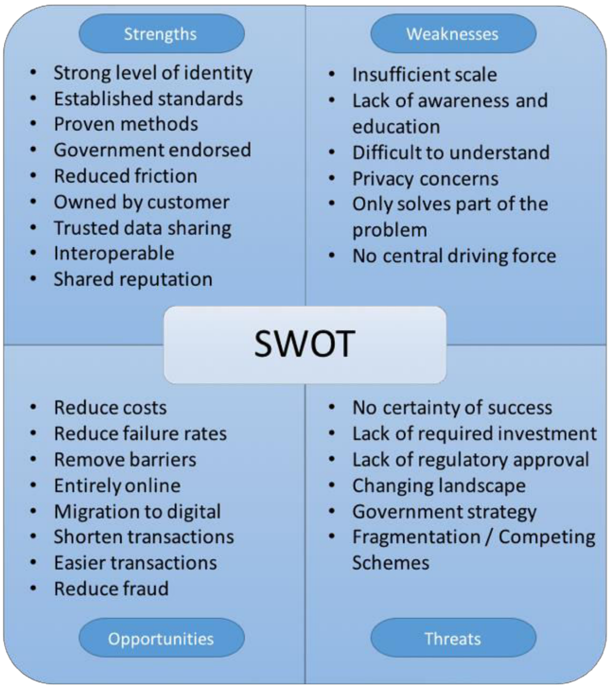
Threats

The certainty of the success of GOV.UK Verify is required to justify the investment required by financial service providers. They would need to remodel their existing customer journeys and system processes to allow for the reuse of a trusted digital identity. The industry regulator needs to provide reassurance that impacts on requirements won't be taken off their current course due to the UK's planned exit from the European Union. Similar concerns around the impact of a change in government, or the ability to deliver the scheme on a commercially attractive basis are also barriers to uptake which need to be mitigated.

Continued fragmentation of the market also poses a threat to the adoption of GOV.UK Verify, particularly if other methods are seen as being more commercially favourable. Google, Apple, Facebook or Amazon have a much greater customer base than GOV.UK Verify could deliver. Should they set a standard acceptable to regulated markets this could have a marked impact on the identity landscape.

Key Insights

The strengths stated of reusing a GOV.UK Verify identity were around providing a strong identity that has been verified to the highest standards. As the standards were already established, this reduced the perceived risk for the financial institutions. Government endorsement being able to reduce customer friction and putting the users in control of their personal data were also seen as strengths. Using a federated identity model was highlighted as a positive due to the interoperability within a cross sector marketplace



SWOT

Strengths

- Strong level of identity
- Established standards
- Proven methods
- Government endorsed
- Reduced friction
- Owned by customer
- Trusted data sharing
- Interoperable
- Shared reputation

Weaknesses

- Insufficient scale
- Lack of awareness and education
- Difficult to understand
- Privacy concerns
- Only solves part of the problem
- No central driving force

Opportunities

- Reduce costs
- Reduce failure rates
- Remove barriers
- Entirely online
- Migration to digital
- Shorten transactions
- Easier transactions
- Reduce fraud

Threats

- No certainty of success
- Lack of required investment
- Lack of regulatory approval
- Changing landscape
- Government strategy
- Fragmentation / Competing Schemes

The providers expressed concerns around the lack of consumer awareness, scale and the fact there didn't appear to be a central commercial driving force for the reuse of GOV.UK Verify. Providers also felt there would be a need for additional identity attribute information to complete some transactions e.g. proof of income, proof of funds etc. There was also a lack of understanding of the standards that have been developed.

> *"There are huge opportunities for the business and customers alike to streamline how we on board and re-verify customers at the point of each interaction."*
> *VP AML Policy, Financial Crime Risk – Barclays*

Opportunities were seen in removing barriers, reducing friction and transaction length, thus improving the customer experience. There was also optimism about the ability of the digital identity to satisfy some of the impending regulations. Fraud reduction and the potential for the reuse of a digital identity to prevent customers falling foul of scams were also stated opportunities.

The lack of regulatory approval and no clear alignment between Cabinet Office and Treasury were felt to be the main threats to the approach. Commercially, providers stated that they would need some certainty around the success and scale of GOV.UK Verify to justify the investment required to remodel their customer journeys to allow reuse.

> *"To make Verify successful we need to change our approach to how we manage fraud and money laundering controls and adopt a more collaborative approach to this. The solution provides lots of opportunities to our business, but also new risks which we need to identify and manage effectively either by ourselves of as part of a community of organisations that want to consume Verify"*
> *VP AML Policy, Financial Crime Risk – Barclays*

Continued fragmentation of the market also poses a threat to the adoption of GOV.UK Verify, particularly if other methods are seen as being more commercially favourable.

A vibrant digital sector can drive economic growth. The financial service sector will play a key role if it can reduce complexity and cost by deriving value from an established digital identity infrastructure

Target Operating Model

Research Approach

The reuse of GOV.UK Verify digital identity creates a role for a commercial hub provider to connect the identity providers to the relying parties (in this case financial service providers). Through a series of workshops within this project, the high level target operating model for such hub providers was explored. The key agreement of this activity was that a hub provider's role was not concentrated on being a technology supplier. Whilst technically connecting the parties is a core requirement, the service layer is the significant role that a hub provider would need to deliver.

Standards

Technical standards have been developed and published by the UK Government for the use of GOV.UK Verify identity providers, hub designers and relying parties. These standards, alongside other technical specifications could be relatively easily adapted to provide an architecture to allow for use in the financial service and other commercial markets. There should be no barriers for technically competent parties to join a commercial hub either as an identity provider or a relying party.

For the service layer, a scheme that identity providers, relying parties, regulators and customers can be confident in needs to exist. For regulated products and services the industry regulator must recognise the scheme in order for providers in that industry sector to adopt it. The scheme must define a common set of standards for identity verification levels of assurance, credential management, authentication, monitoring and service standards.

These standards will need to evolve to meet the various market and sector needs. The evolution should extend, rather than diminish, the needs of government. They must align to globally applicable standards to ensure interoperability within a digital single market. For regulated sectors, the scheme governors should work alongside the appropriate regulatory bodies. They should ensure continued endorsement that meets the particular challenges of the sector.

Governance

On-boarding of new hub providers, identity providers and relying parties should be a standards based mechanism. Certification and governance of the lifecycle for entry, ongoing participation and exit, is required. Commercial freedoms need to exist, governed by the scheme, for introduction of new actors. The scheme requires powers to monitor conformance and behaviours of its members in order to protect its integrity. The scheme's governance also needs authority to remove bad actors.

The governance model for the scheme could be formed of its stakeholders, with self-governance by the members. Alternatively, it could in itself be governed by a regulatory body. Whichever means of governance is adopted the body needs sufficient independence to act in the interests of the whole scheme. It needs to provide an arbitration/ombudsman role to which decisions its members agree to abide.

Scheme integrity

Within a federated scheme a risk of brand, commercial or reputational conflict will undoubtedly arise between the identity providers and relying parties. This could be due to the relying party being an industry competitor of a particular identity provider, the costs of the identity assertion being unappealing to a subset of providers, or ethical concerns in providing a service to certain sectors or providers.

Fragmentation of the scheme is likely to cause confusion to customers and has the potential to undermine the purpose of having a single trusted digital identity scheme. This has the potential to bring the whole scheme down, or lead to separation into competing schemes. A certain level of market maturity is required so that parties would not seek to unreasonably withhold services. The scheme would have to work with all members to broker a satisfactory position.

Commercial Considerations

To make the model commercially viable, there needs to be sufficient reward to introduce new relying parties into the scheme. Similar reward should exist for identity providers to grow the customer base of verified identities. The ability to provide verification to customers as a standalone action, outside of any transaction with a relying party, is likely to become a proposition that identity providers would endorse if the commercial model supported it. There are clear customer benefits in allowing this once the education and awareness of the benefits of reuse become apparent. Customers may choose to switch identity providers who offer services more suitable to their needs.

The hub provider could have a role to play in negotiating pricing between the identity providers and the relying parties. Market forces are likely to dictate the pricing model, with identity providers with the largest volume of customers, higher service levels, or a niche demographic, being able to charge a premium. Relying parties consuming the highest volumes are likely to be offered more attractive rates. The hub provider may aggregate the prices of the identity providers to provide a single rate to relying parties.

Liability

The scheme would have to define a clear liability model in order to be commercially suitable for identity providers and relying parties. This would need to state a clear level of liability in instances where the identity provider has met its obligations and a level of liability for where it has not.

The limit of liability does not have to be a single fixed amount and may be zero. The commercial pricing for identity assertions could vary depending on the level of liability offered. The liability model needs to set out clear obligations for identity providers, hub providers and relying parties.

Particular attention needs to be paid to the level and means of redress offered to customers where either their assured identity is subsequently misused or they become a victim of identity fraud from 3rd party misuse of the scheme. An expectation of suitable identity repair should be given, together with financial redress by the involved parties or the scheme. The ability for the scheme to self-insure should be explored.

Branding

It was felt that the brand identity should be owned by the scheme, with the members taking an interest in the ability to promote and protect it.

Privacy

The GOV.UK Verify scheme operates upon an agreed set of privacy principles[19] and under a contractual model that delivers to the needs of government. As usage within the commercial sector grows, the identity providers may seek to broaden the range of services offered to customers. Whilst it is important to maintain a customer consent centric ethos, the constraints of the existing privacy and contractual model may need to vary to allow such services to be developed. A specific example of this would be to offer the customer an identity statement. This statement could show not only when their identity was asserted, yet also enhance it with details of with whom and for what purpose. Such enrichment of the identity assertion would not currently be allowed.

Role of Government

The role of government in the matured marketplace could be one of policy and standards. There is a precedent for governments to set the standards by which identity is measured in the commercial use of passports (entitlement for crossing a countries border) and driving licences (entitlement to drive) being used as identity assertion instruments. Having a model where government iterate the standards, to maintain quality of the digital identity, provides value in the trust model. Some other elements of the service standard could also be applicable. For example, how the quality provision protects the integrity of the identity. Elements of the requirements of the scheme such as security, records management, data storage and retention could be specified within government issued standards. Other elements of the service standard such as user experience, performance, helpdesk operating hours and commercial models could be set by the market or scheme. In a future model, the Government themselves may buy the services through a commercial hub provider that delivers the right service and price criteria for their needs.

[19] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/361496/PCAG_IDA_Principles_3.1__4_.pdf

Key Insights

Government has a role to play in a future commercial marketplace in setting policy and standards for digital identity. The commercial market demands will drive the service standards based on the needs of the sector.

A governance model is required to oversee all actors within the identity scheme. The risk of bad actors poses a threat of fragmentation and reputational damage to the overall scheme. The scheme governance body would act in the interests of both customers and its scheme members.

A model for reuse of an existing GOV.UK Verify identity can be a catalyst for commercial adoption. In the longer term the need for reverification and the need for growth of volume of assured identities, to drive scale of the market, is likely to mean that identities can also be created in the commercial sector with allowable reuse in a government context.

The Target Operating Model for a commercial identity scheme would consider:

Standards
Proofing
Technical
Operational

Commercials
Visibility
Reward
Volume

Branding
Recognition
Marketing
Government Endorsed

Integrity
Reputation
Protection

Governance
On-boarding
Certification
Arbitration

Liability
Variable limit
Customer redress
Insurance

Role of Government
Policy
Standard
Licensing

Privacy
Consent
Ownership

Conclusions

A widely-adopted, fit-for-purpose, trusted, standards-based digital identity scheme could have significant value for the financial services industry.

For the user it could simplify the initial digital engagement with a provider and subsequent transactions, providing a consistent way to prove “I am who I say I am”.

For the provider, it could deliver a consistent approach to user identification and management and reduce the cost of onboarding and transactional business processes. It could facilitate the delivery of new services such as portfolio management and transform the delivery of existing services, for example, alleviating the need for “step-out” channels when online.

For industry, it could provide the basis for delivering new user centric industry models such as in payments, and create a more competitive, dynamic and engaging marketplace for customers, while answering the demands on impending legislation.

Having government and regulatory approval for a cross sector scheme provides a significant catalyst for adoption. Through the user research, the value of having an identity scheme endorsed by government, was shown. This demonstrated a propensity to use digital channels where they can assert their existing digital identity. It provides confidence for financial service providers to adopt the scheme as a method of customer verification into their online product and service journeys.

There is a real opportunity to develop a shared approach to digital identity in the UK, and GOV.UK Verify does provide a framework that will allow for the next stage of exploring reuse through practical implementation. Market maturity and scale is required for a trusted scheme to be widely adopted, and UK Government need to provide a strategy for how they intend to support this in 2017 and beyond.

To take the proposition forward with purpose the following needs must be addressed:

- Scale of identities within GOV.UK Verify
- Fill the gaps in the model
- Alignment of Cabinet Office and Treasury
- Regulatory approval
- Creation of a cross industry working group
- Commercial model
- Customer awareness and education

Gaps in the proposed design of a functioning UK identity ecosystem need to be filled with a solution and a mechanism for delivery, one key example of this is attribute exchange. With demand in both government and financial service sectors, the potential for other identity schemes or solutions to appear exists. Fragmentation risks, customer confusion, poor experience across sectors, variation of standards and weakness in the ability of the identity market to collectively change as the external cyber and fraud threats evolve.

The hypotheses for customer reuse and financial service provider adoption have been validated through this project.

The issues identified need to be addressed to progress this further.

There are mutual benefits from government and private sector working together to deliver a flexible digital identity scheme. In order to move forward at pace, an agreement on how to deliver a working solution over the coming months, is required.

Next Steps

Government

- Provide a clear plan for scale to 25 million identities by 2020
- State their intended longer term role in the scheme and the support they intend to provide
- Define an acceptable liability model with the private sector for reuse of digital identities
- Provide alignment and regulatory approval between Cabinet Office and Treasury for reuse
- Align UK Money Laundering Regulations to support adoption of GOV.UK Verify digital identity
- Provide technical sandbox environment for the financial services industry to test the proposition and align this with OR connect it with the Financial Conduct Authority sandbox
- Work with the Competition and Markets Authority Implementation Working Group to align an approach to digital identity in the financial services sector
- Provide a technical model for reuse which includes a mechanism for additional attributes to be exchanged
- Help support a commercial proposition for financial services companies to reuse digital identities

Financial Service Providers

- Develop an understanding of the commercial business case for adoption of identity reuse (cost benefits)
- Consider the approach to satisfy impending regulation (e.g. PSD2) and the alternative approach to building API's and addressing it using digital identity
- Confirm the steps needed with fraud and risk teams to allow them to accept the digital identities provided
- Pilot re-use of GOV.UK Verify digital identities through the sandbox environment
- Add reuse on their technical development workstack

Identity Community

- Create a joint government and commercial sector working group
- Work with the British Bankers' Association to develop industry best practice guidelines for reuse
- Develop the commercial model the cross-sector digital identity scheme – who pays, and how much?
- Draft an outline scheme agreement
- Undertake a service, rather than technology, focussed pilot to allow reuse of the Verify identity to obtain a financial service product
- Evaluate other commercial sectors to develop a fully cross-sector scheme
- Develop a strategy to increase customer awareness

Participants

Aviva

Aviva provides around 31 million customers worldwide with insurance, savings and investment products. We are the UK's largest insurer and one of Europe's leading providers of life and general insurance.
www.aviva.co.uk

Barclays

Barclays is a transatlantic consumer, corporate and investment bank offering products and services across personal, corporate and investment banking, credit cards and wealth management, with a strong presence in our two home markets of the UK and the US. Barclays is one of the UK's leading banks, with a long history of innovation. We're proud to be the only bank selected by UK Government as a certified company to provide a safe, secure identity verification service.
www.barclays.co.uk

Experian

Experian has been a trusted provider of data services for many years and has gained a vast array of experience in providing solutions that provide our Clients with confidence that the identity asserted by their customers is as stated. This service expands that service to provide individuals with a mechanism to gain a trusted identity that can be provided to those organisations they wish to do business with, without the inconvenience of offline checks on identity being required.
www.experian.co.uk

HiFX

Collectively, HiFX and Ria (also part of Euronet Worldwide) are now the third largest money transfer business in the world. Your money, wherever it's needed, whatever the reason.
www.hifx.co.uk

Innovate Identity

Innovate Identity is an award winning business with a highly experienced team of digital transformation consultants specialising in online identity, security and privacy. Our team have vertical industry expertise in financial services, payments, technology, telecoms, government, online retail, online gambling as well as breadth of geographical knowledge across multiple global jurisdictions.
www.innovateidentity.com

Meeco

Meeco was created with the purpose to empower people to own and benefit directly from their personal data. Reward is not just about money; it is what matters to you. Meeco is about helping individuals to gain the insight and have the data to negotiable better outcomes for you and your family.
www.meeco.me

Post Office

Post Office are the UK's largest retail network and the largest financial services chain in the UK with more branches than all of the UK's banks and building societies put together. At Post Office, we aspire to be at the very heart of customers' choice by becoming the most trusted provider of essential services to every person in the land. The Post Office is proud to be one the first certified providers of the GOV.UK Verify scheme.
www.postoffice.co.uk

Verizon

Verizon is one of the largest communication technology companies in the world. Every day, we connect millions of people, companies and communities with our powerful technology.
www.verizon.com