

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:



Contributors:



Author: Bryn Robinson-Morgan

Published: December 2016

Executive Summary

Contents

5	Background
7	Scope
8	Customer Research
9	Financial Sector Analysis
11	Target Operating Model
12	Conclusions
13	Next Steps

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 Association¹

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 breaches², misuse of personal information³, identity theft, fraud⁴, 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 fragmented⁷. 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 Chancellor⁸

In May 2016, the UK government formally launched their new digital identity program, GOV.UK Verify⁹. 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. 4MLD¹⁰, PSD2¹¹, PAD¹², GDPR¹³ and the Open Data Standard).

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>

¹³ <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/>

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 Operating Model Considerations

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

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.

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 areas 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

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 customer¹⁴ 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

¹⁴ <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 Verify¹⁵ 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 assurance¹⁶. 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 inclusion¹⁷, this aligns with UK government strategy.

¹⁵ <https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify>

¹⁶ http://oixuk.org/?page_id=2111

¹⁷ <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, such as 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 hypotheses 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

Customer Research

Context

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.

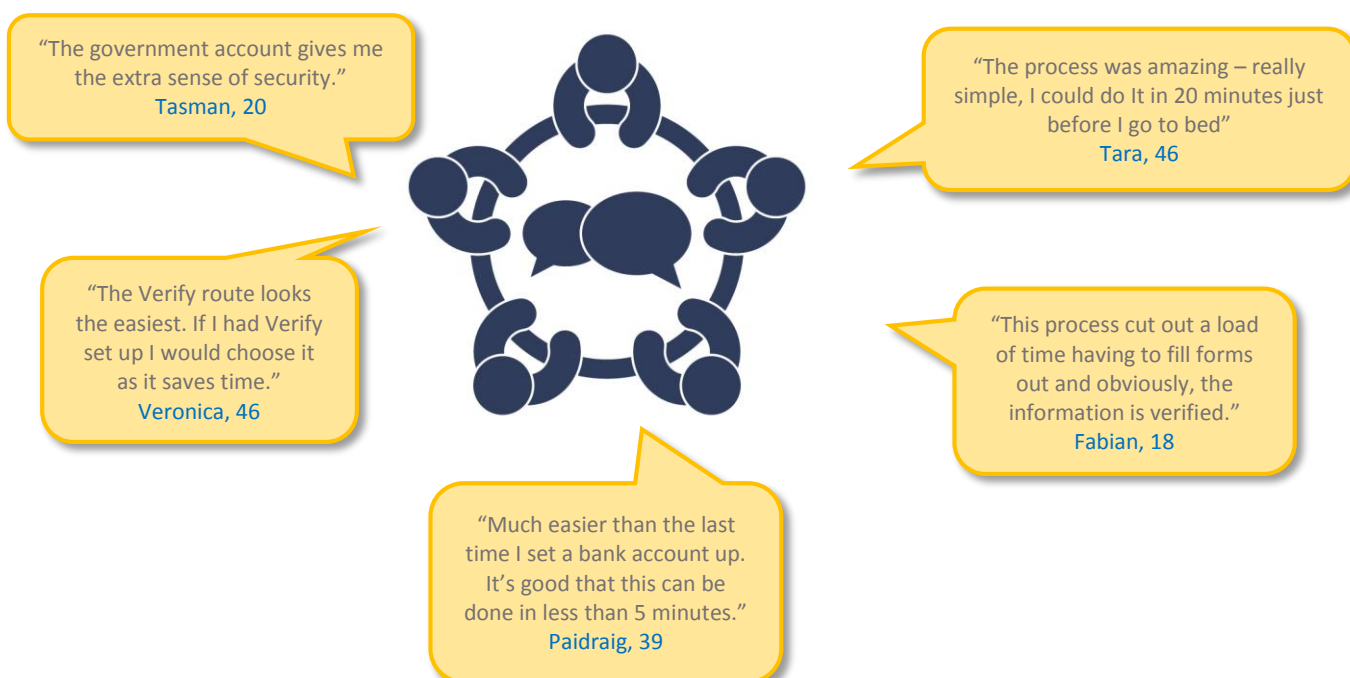
It is important to note that asserting identity is one part of financial service product application. The user testing did not validate whether the application would actually be successful.

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

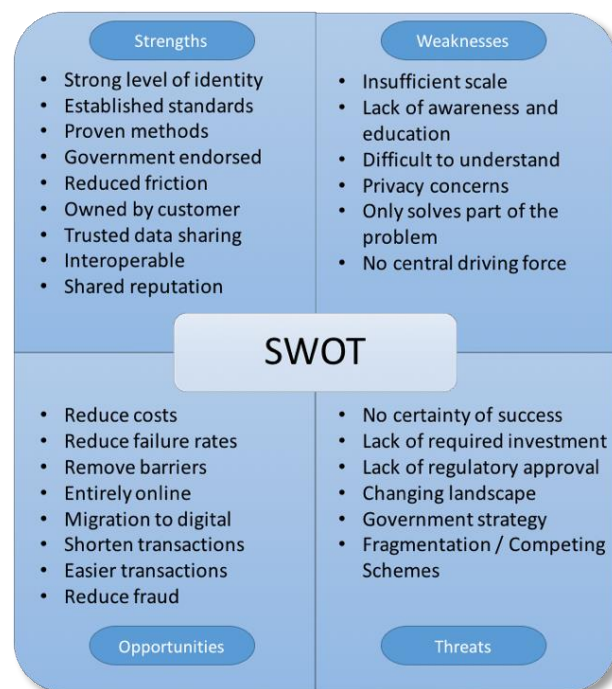
Context

In order to test this hypothesis a SWOT analysis was performed with four financial service providers involved within the project. A baseline assumption was made that 50% of the UK adult population would have a GOV.UK Verify digital identity in the next 3 years, that would be accepted by 50% of UK financial service providers as a means of proving their identity when transacting online.

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

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.



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.

“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

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 or 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.

Target Operating Model

Context

The reuse of the 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.

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