OPEN IDENTITY EXCHANGE

White Paper

How Digital Identities which meet Government Standards could be used as part of UK Banks' Customer On-boarding and KYC Requirements

Jan 2017

Contributors

pwc

bba

The voice of banking

Cabinet Office
Government Digital Service

OIX OPEN IDENTITY EXCHANGE

This report has been prepared with the assistance of PricewaterhouseCoopers LLP ("PwC"). PwC accept no liability (including for negligence) to anyone in connection with this report.

Foreword

Chris Ferguson, Director, Digital Group, Government Digital Service

Public and private sector services in the UK are being transformed by the culture, practices and technology of the digital age. In the UK Government we are designing services to be simpler, cheaper and more convenient for users. If end-to-end digital transformation of services is to be successful, people must have confidence in how their personal data is used and stored as criminals have become adept at stealing identities and personal data through new and innovative forms of fraud. Users of services need to know that they are protected from the increasingly sophisticated threat of fraud and identity theft.

Launched by the Government Digital Service in May 2016, GOV.UK Verify is a fundamental building block in the transformation of UK public services. A safer, more secure way of proving who you are online, it helps fight the growing problem of online identity theft. GOV.UK Verify will expand to enable those who choose to access online public services to prove their identity to high government standards.

The Government Digital Service has created a new market of identity services built around user needs and delivered by private sector companies. This market, created in response to the aggregated demand of digital public sector services, is expected to grow and evolve in response to changing needs, new technologies and new threats.

In a global digital economy, users need to be able to prove who they are online, not just in the country where they live, but in other countries as well. People need a secure way to prove who they are that works beyond national borders. We developed GOV.UK Verify in collaboration with international governments so that identity infrastructures are interoperable and assertions of identity from other countries can meet the UK government's published standards. Projects planned to begin in 2017 will begin to test interoperability between UK and other national digital identity systems.

The UK Government is working with the private sector to explore how people might use a GOV.UK Verify identity account to assert their trusted identity online to access a wider range of services across a number of industry sectors. This report provides an analysis of how digital identity could be used to improve the process of opening a bank account. It describes how the approach differs to the current banking practices which have built up through years of regulatory and business change.

We're creating the GOV.UK Verify 'sandbox' environment so that private organisations will be able to test how GOV.UK Verify works for services within their sector. This will provide a space to engage in dialogue with government on the operation and governance of GOV.UK Verify beyond the public sector.

Fraud and identity theft are common problems with a high cost for both government and industry. Criminals can expose an individual's personal and financial data and cause significant damage to the reputation of organisations that they hack. Fines imposed by regulators add to already high costs of reparation. This new collaborative approach is needed between the public and the private sector to protect people and businesses.

It is our expectation that, alongside the UK Government, private sector organisations will invest in developing this new market of identity services and use it to help secure their digital services. Doing so will help to protect our users and our services from identity theft or fraud activity and keep people's information private and secure.

Table of contents

1. Executive Summary

View from the British Bankers Association

In a digital age, and as more of our banking is carried out online, via apps and mobile phones, customers expect to be able to open new products and services with financial institutions through digital channels. But increasing internet identity fraud and a rapidly changing regulatory environment make it difficult for banks to be able to offer a simple and secure identity verification process for their new customers.

The UK Government has created GOV.UK Verify as a new way to safely and securely prove who you are online. Originally deployed as a means for an individual to identify themselves when seeking to access a range of government services, the financial services industry is now beginning to look very seriously at the possibilities of customers being able to utilise digital identities in establishing relationships with banks, building societies and other financial service providers.

To help to better understand the potential benefits and challenges in using a GOV.UK Verify identity as part of an non face-to-face on-boarding process, PwC were commissioned by the BBA to undertake objective research in two parts: firstly to survey a range of banks on the methods they currently use for the identity verification of their customers, and secondly to compare their existing requirements against an assertion of a digital identity that meets the currently implemented government standard, Level of Assurance ("LOA") 2.

Summary of main findings

- The research uncovered significant variety in the identity verification approaches used across different sizes and types of banks and financial institutions, and even in the language used to describe that process. The report distinguishes identity verification from the other processes that banks conduct to test a customer's eligibility for a product or service.
- At a basic level, there is a broad correlation between the size of the bank and the level of data sought from the customer, with larger banks seeking the most data, mid-tier banks seeking substantially less (perhaps more targeted) information, and some new banks seeking significantly less – in one case just a photo of a passport and a thumbprint.
- However, such a correlation cannot be taken at face value alone. In fact new and smaller banks seek less data direct from applicants but seek more substantial information via background technology-driven processes.
- The variance is also likely to be explained in part by the greater need amongst banks with larger customer bases to remove or identify 'false positives' amongst their customers.
- The report finds that the government LOA 2 standard for identity verification under GOV.UK Verify is equal to or exceeds the level of assurance currently achieved by the majority of banks in a non face-to-face on-boarding environment.
- However it was also clear that a significant proportion of the banks interviewed are looking to achieve even higher levels of assurance in the future, with a number working towards LOA3.

- While GOV.UK Verify-derived identities match the data requirements for the identification and verification of a customer, and the necessary level of authentication, financial institutions utilising such a solution would still require additional data and checks in order to meet their obligations under AML legislation, JMLSG guidance, and to undertake credit risk assessment.

Conclusions

Considering the 'fit' of GOV.UK Verify IDs against the banking industry's current on-boarding identity and verification requirements, there are a number of potential benefits that might be derived from its adoption by the retail financial sector.

Tackling fraud is an issue of vital importance to the banking industry, and the use of an ID that has been derived via a federated system, such as GOV.UK Verify, has significant advantages in maintaining better identification of fraudulent IDs in the on-boarding stage, and later through the potential use of digital identities alongside payments and other transactional processes, and in the use of products utilising new Application Program Interfaces ("APIs"). This could be a significant benefit which requires further exploration, and will be an interesting point of discussion to pursue further, alongside initiatives such as the Payment Strategy Forum's new Payment Strategy. Fraud can only be addressed effectively through collaboration and GOV.UK Verify could represent a credible vehicle through which to start that process.

While there were questions raised in the interviews with regard to how digital identity use will mesh with banks own on-boarding processes and online environments, which need to be addressed, for customers to be able to utilise a single secure ID to undertake a range of actions carries enormous potential. This might initially include opening a bank account, to establishing new products and services across a range of industries in time, and with enhanced levels of security. Improving customer experience, whilst at the same time reducing fraud and impersonation risk, if it can be realised, is likely to be of significant interest to banks and their customers alike.

Given the alignment of GOV.UK Verify to the EU's eIDAS standards, and the development of similar digital identity schemes in a range of countries across the EU, there may also be the possibility to utilise digital IDs for those applying for products or services across border, for instance to support the requirements of the Payment Accounts Directive.

However the report clearly identifies some significant challenges that need to be further explored, and if possible addressed:

- Firstly, a standards-based approach to establishing identity and its verification is a departure from current 'business as usual'. Banks will need to be better informed of the standards that underpin the provision of digital identities, and to have confidence in the information they receive. Using digital identities requires banks to rely on third party data in a way that they do not currently. It would also reduce their ability to compete in the way that they identify their applicants, which some banks consider to be an important part of their offering.
- At present the use of digital identities is not well described in the JMLSG guidance, which guides banks' on-boarding requirements. However this may change as part of the upcoming JMLSG review. Similarly efforts are ongoing in the Commission to ensure that the revisions to 4th EU Money Laundering Directive ("4AMLD") currently being discussed reflect the opportunity to utilise digital identities, which has been supported by BBA and the European Banking Federation.
- While there is an established liability model for use of GOV.UK Verify identities for accessing public services, there is currently no such regime in place for use of digital IDs by the financial services sector. This will need to be addressed before any form of adoption will be possible.
- There is also no current commercial model for the reuse of GOV.UK Verify identities. The cost of adoption, at a time of significant change for banks, is absolutely critical, and must be considered fully and be attractive to the industry for adoption to take place.

Looking further into the future, additional questions will need to be addressed. A number of banks reported that they are actively looking at how to achieve higher levels of authentication, towards LOA3, perhaps by the use of biometrics, or via behaviometrics or the use of API-derived data, for example. Whether GOV.UK Verify-derived identities could be developed towards this higher level of authentication ought to be considered.

And finally, GOV.UK Verify IDs may currently satisfy banks' identity and verification requirements, however that is only part of the data required to on-board a customer. Consideration could be given as to the potential to collate a wider range of data, derived from GOV.UK Verify and other established sources to generate a more holistic Know Your Customer ("KYC") utility.

2. Introduction

The purpose of this project was to explore the extent to which digital identities which meet Government standards (GOV.UK Verify) could be used as part of banks' current on-boarding and KYC practices for non face-to-face retail customer on-boarding.

The project ran between July 2016 and November 2016. The British Bankers Association ("BBA"), the Cabinet Office and PwC contributed to this project.

The independent research which underpins this report was carried out by PwC, and consisted of a number of interviews with participating banks to understand their on-boarding requirements (Appendix A). This paper summarises the findings from the interviews and compares these to the digital identity standards which underpin GOV.UK Verify.

The scope of this project was to:

- Understand in detail existing on-boarding practices adopted by a range of UK retail banks. A sample of 11 banks from across the industry were interviewed; and
- Consider the similarities and differences between the existing on-boarding practices, including industry and regulatory expectations, and the digital identity standards which underpin GOV.UK Verify.

3. Background and Context

Electronic Identification and Authentication Services ("eIDAS") Regulation

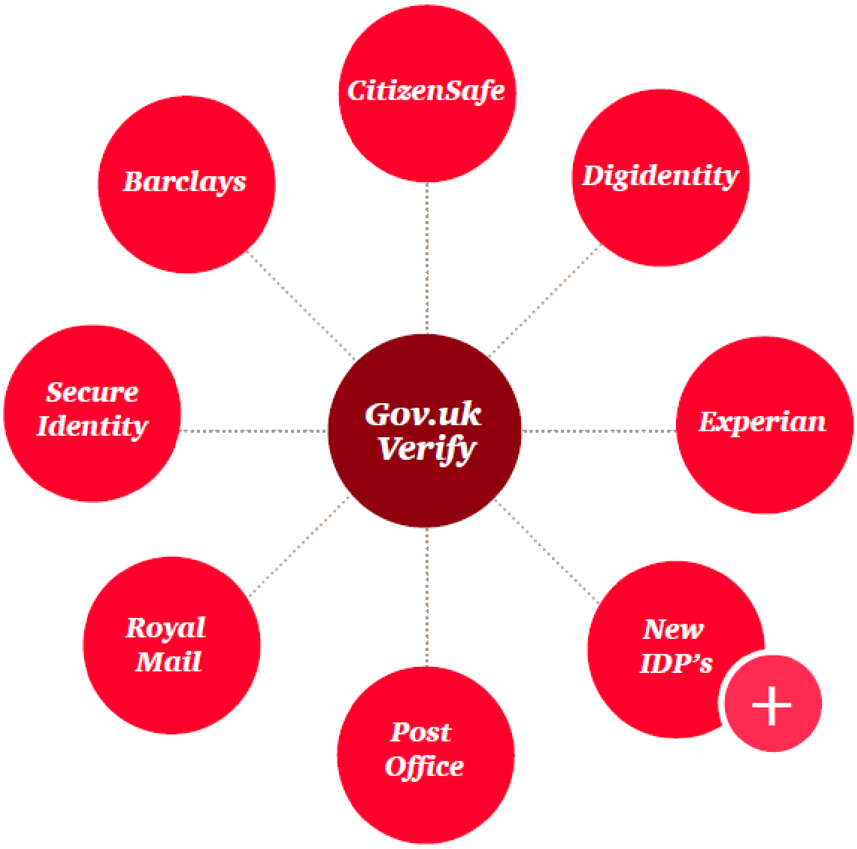
Regulation EU No. 910/2014, commonly known as eIDAS, is an EU regulation on electronic identification and trust services for electronic transactions in the European internal market. It seeks to establish a single legal framework for recognising electronic signatures and identities throughout the EU.

This is part of a wider programme by the European Commission to create a single digital market in which identity is important, as some services can only be offered digitally in circumstances where the provider can reliably identify the user.

GOV.UK Verify

An identity scheme has been developed in the UK based on standards which can be mapped to the eIDAS levels of assurance. The UK Government has created GOV.UK Verify, a new way for individuals to safely and securely prove their identity online when accessing digital public services provided by central Government.

GOV.UK Verify is decentralised and currently uses seven certified identity providers ("IDPs") to conduct verification checks according to agreed standards. The user is able to choose from any of the seven certified IDPs to establish a digital identity.



GOV.UK Verify has been built to enable everyone in the UK to be able to create a digital ID which can currently be used to access an increasing number of central Government services.

High level comparison of eIDAS to GOV.UK Verify

GOV.UK Verify aligns with eIDAS (the "Regulation") in delivering a digital identity which allows the user to access public services. It is intended that individuals in the UK will be able to take advantage of the scheme for online public services in the UK and in other EU member countries due to the alignment of standards between the UK and EU. Pilots are currently underway to explore the application of GOV.UK Verify in the private sector.

Under the eIDAS standards EU Member States are obliged to accept digital identities of "Notified" schemes and only for accessing public services. Currently, whilst in line with eIDAS standards, GOV.UK Verify is not yet a Notified scheme. This is a political decision and is not mandated in the Regulation, should Her Majesty's Government wish to notify GOV.UK Verify under the Regulation it would then be mandatory for other Member States to accept assertions of identity from GOV.UK Verify Identity Providers.

Understanding of the GOV.UK Verify service

GPG 45 requirements and interpretation

The basis of the identity proofing process performed by IDPs on the GOV.UK Verify service is the Good Practice Guide 45 ("GPG 45"). This document is issued jointly by Communications-Electronics Security Group ("CESG"), the UK's National Technical Authority on Information Assurance and the Cabinet Office, Government Digital Service.

GPG45 provides an "as-is" example of how the specific requirements can be met. Within the UK there is no statutory attribute or set of attributes that are used to uniquely identify individuals. GPG45 sets out four levels of identity proofing:

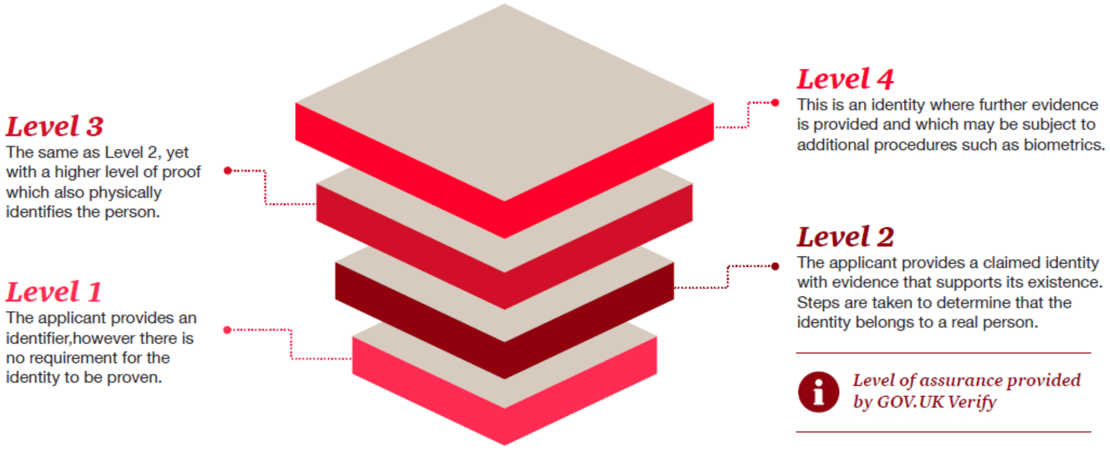

Level 3
The same as Level 2, yet with a higher level of proof which also physically identifies the person.
Level 1
The applicant provides an identifier,however there is no requirement for the identity to be proven.
Level 4
This is an identity where further evidence is provided and which may be subject to additional procedures such as biometrics.
Level 2
The applicant provides a claimed identity with evidence that supports its existence. Steps are taken to determine that the identity belongs to a real person.
Level of assurance provided by GOV.UK Verify

Figure 1: Levels of identity proofing assurance[1]

GOV.UK Verify currently provides LOA2. LOA3 assurance could be achieved through use of a biometric (for example) as the biometric ties an individual to their true identity.

[1] *Source: Good Practice Guide no.45 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/370033/GPG_45_identity_proofing_v2_3_July_2014.pdf*

Identity Proofing and Verification of an Individual

The identity proofing process typically follows the process set out below to the determined level of assurance:

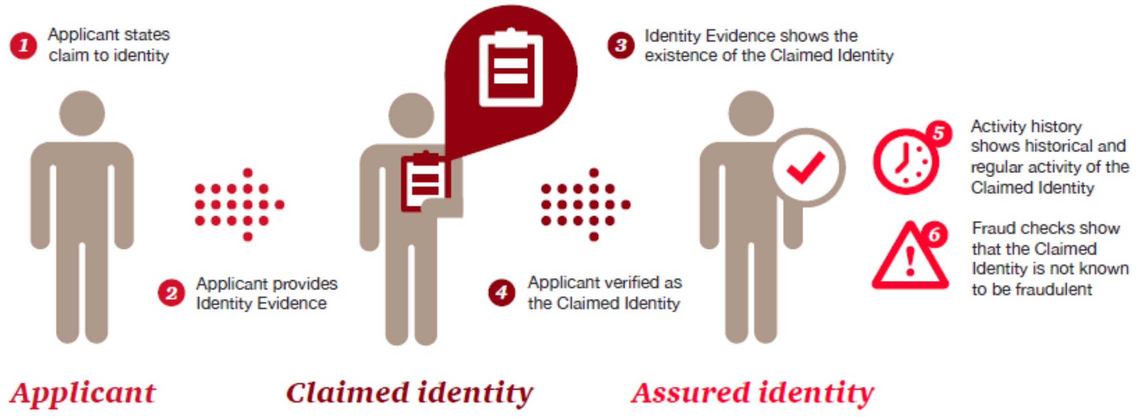

1 Applicant states claim to identity
2 Applicant provides Identity Evidence
3 Identity Evidence shows the existence of the Claimed Identity
4 Applicant verified as the Claimed Identity
5 Activity history shows historical and regular activity of the Claimed Identity
6 Fraud checks show that the Claimed Identity is not known to be fraudulent
Applicant
Claimed identity
Assured identity

Figure 2: Overview of identity proofing and verification process for Level 2 Assurance[2]

[2] *Source: Good Practice Guide no.45 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/370033/GPG_45_identity_proofing_v2_3_July_2014.pdf*

4. Identification and verification in the Retail Banking sector

The Money Laundering Regulations ("MLR") 2007

The MLR require banks (and other financial institutions) to apply risk-based customer due diligence ("CDD") measures and take steps to prevent services from being used for money laundering and terrorist financing.

Regulation 5 sets out the meaning of CDD measures:

a) "identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

b) identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the relevant person is satisfied that he knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement; and

c) obtaining information on the purpose and intended nature of the business relationship."

Non face to face on-boarding can present a higher risk for a bank or other institution. The MLR Regulation 14(2) states that where a customer has not been present for identification purposes, a relevant person must take specific and adequate measures (often referred to as Enhanced Due Diligence or EDD) to compensate for the higher risk. One or more of the following measures should be applied:

> "ensuring that the customer's identity is established by additional documents, data or information;
>
> supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution which is subject to the money laundering directive;
>
> ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution."

In the UK, the Joint Money Laundering Steering Group ("JMLSG") has produced guidance to help banks and other institutions meet these obligations.

JMLSG Guidance

Identification requirements for private individuals are contained within Section 5.3 Part I of the JMLSG guidance.

Firms should obtain the following basic information about their private individual customers:

- Full Name
- Date of Birth
- Residential Address

Verification of the identity obtained must be based on "*reliable and independent sources*".

Non face-to-face Identification and Verification

Where a customer is not physically present for identification purposes, the JMLSG Guidance recommends specific and adequate measures to compensate for the higher risk based on MLR Regulation 14(2). It also suggests that the *"extent of verification in respect of non face-to-face customers will depend on the nature and characteristics of the product or service requested and the assessed money laundering risk presented by the customer"*.

Non face-to-face identification and verification carries an inherent risk of impersonation fraud. JMLSG recommends that firms undertake additional anti-fraud checks.

JMLSG Guidance suggests that a firm should carry out non face-to-face verification either electronically or by reference to documents. For the purposes of this project the focus is on electronic verification as set out in JMLSG Guidance Part 1 Section 5.3.79 – 5.3.81 The standard level of confirmation is one match on an individual's full name and current address and either a second match on an individual's full name and either his/her current address or his/her date of birth.

<u>Electronic Verification</u>

Where identity is verified electronically, the JMLSG Guidance recommends that this should be performed by the firm on-boarding the client either directly or using a reliable supplier. The standard level of confirmation consists of:

- One match on an individual's full name and current address, and;
- A second match on their full name and either his current address or his date of birth

As part of the 4AMLD changes are being proposed[3] to the current e-identification requirements which could be reflected in JMLSG Guidance in the future. Please refer to section 8.

[3] http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf

5. Purpose of this research

This research has been undertaken to assess the extent to which the eIDAS-compliant digital identities which underpin GOV.UK Verify could be used by retail banks as part of their customer on-boarding processes.

The research seeks to establish whether there could be benefits for banks and their customers in using a digital ID service which meets regulatory requirements. These benefits could include improving the customer experience, mitigating identity fraud and easing the compliance burden.

Our approach to the research

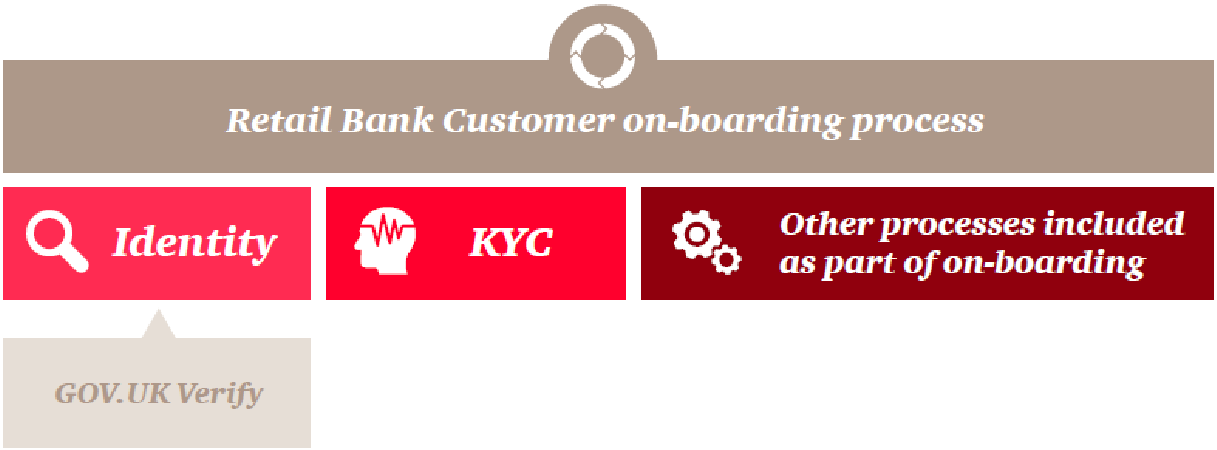
The BBA commissioned PwC to undertake the analysis required for this research.

PwC conducted interviews with a sample of 11 UK retail banks. To get a good understanding across the industry, the sample included a wide range of banks - from the smaller, challenger banks to the larger, global banks. The sample is set out as Appendix A.

The purpose of the interviews was to understand current non face-to-face on-boarding practices performed by UK retail banks, and in particular, understand how they execute the identity assurance element of the on-boarding process for private individuals.

KYC is often used as a synonym for customer due diligence checks. The FCA's Financial Crime Handbook states that KYC can also refer to suitability checks related to the sale of regulated financial products. The elements of KYC are not prescribed in the same way across the industry.

For the purpose of this research, PwC has distinguished between identity related data, KYC related data and on-boarding related data as follows:

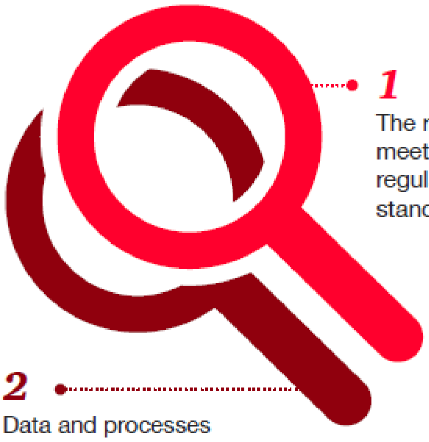

Retail Bank Customer on-boarding process
Identity
KYC
Other processes included as part of on-boarding
GOV.UK Verify

Identity Attributes	Core identity attributes required for a private individual by legislation
KYC Attributes	The scope of KYC includes the core identity attributes required for a private individual by legislation. It also includes other information which is collected either for anti-money laundering ("AML") purposes, other Financial Crime purposes (for example fraud), or suitability purposes.
On-boarding Attributes	This includes attributes which are not AML or Financial Crime related but are required to fulfil an individual bank's end-to-end on-boarding process. This includes information on a customer's communication preferences or information collected for product targeting.

In addition to the collection of attributes, there are a series of processes which are undertaken by banks as part of the on-boarding journey. These are covered in Section 6.7.

PwC compared current UK retail non face-to-face on-boarding practices for non face-to-face banking with the requirements of GOV.UK Verify, and specifically the standards detailed in GPG 45, GPG 44 and the GOV.UK Verify IPV Operations Manual.

The analysis has been undertaken our analysis through 2 lenses:



1 The requirements to meet the minimum regulatory and legal standards; and

2 Data and processes required to successfully complete on-boarding journey

For the purposes of this research, PwC has referred to private individuals who are new to the bank, or applying for a digital ID for the first time as "applicants".

PwC has set out the commonalities and differences between the processes currently adopted in UK retail banks with that of GOV.UK Verify.

6. Findings

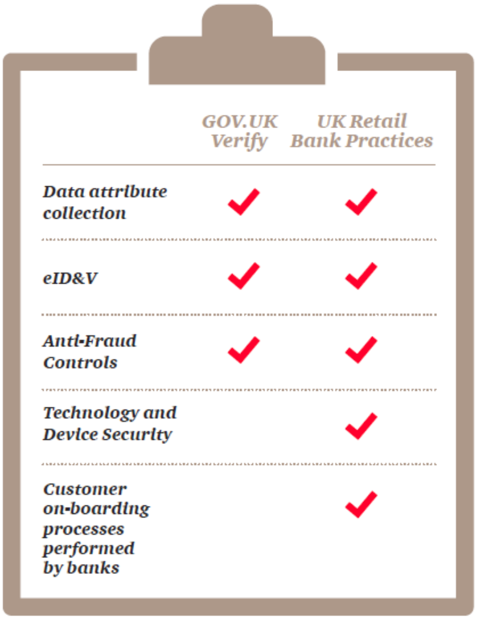
Categorisation of comparison

In order to draw a comparison between UK retail non face-to-face on-boarding practices and GOV.UK Verify, the analysis has been broken down into high level categories. Not all categories are applicable to both and there are some differences in the application of these.[4]

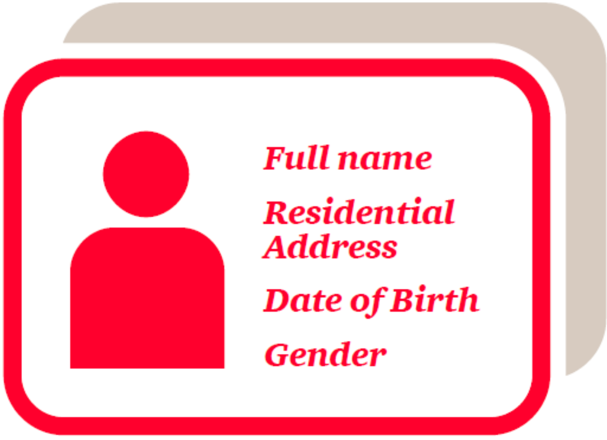
Eligibility

Under GOV.UK Verify, it is possible for individuals under 18 and non-UK residents to have their identity verified with the current set of IDPs. Verification can however be more difficult under these circumstances.

Six of the banks interviewed required applicants to be 18 or over to open a current account, the remainder would allow applications from other ages, but would usually assign them a different product such as a student account. Age was often used as a way to mitigate product risk, for example, products involving loans and overdrafts were often restricted to over 18's only.



	GOV.UK Verify	UK Retail Bank Practices
Data attribute collection	✓	✓
eID&V	✓	✓
Anti-Fraud Controls	✓	✓
Technology and Device Security		✓
Customer on-boarding processes performed by banks		✓



GOV.UK Verify verifies the minimum amount of data required by JMLSG

At the time of conducting the fieldwork for this project, six banks allowed applications from non-UK residents, although it was noted that there are often problems with conducting non face-to-face on-boarding of these applicants. Via their non face-to-face channel, four banks would only accept UK residents and one would only accept British nationals. Since completing our fieldwork, under the Payment Account Regulations, effective from 18 September 2016, firms are legally obligated at a minimum to be able to receive and consider applications for payment accounts from legal residents elsewhere in the EU.

[4] The Financial Crime checks which are performed by banks differ from the checks performed by GOV.UK Verify. In relation to technology and device security this refers to the specific steps banks take in relation to the use of device controls for authentication purposes. These differences have been drawn out in the comparisons made.

Data Attribute Collection

Data Attributes collected under GOV.UK Verify

Once an applicant has been successfully validated by GOV.UK Verify (see Figure 2), the following data attributes are considered verified ("assured identity"):

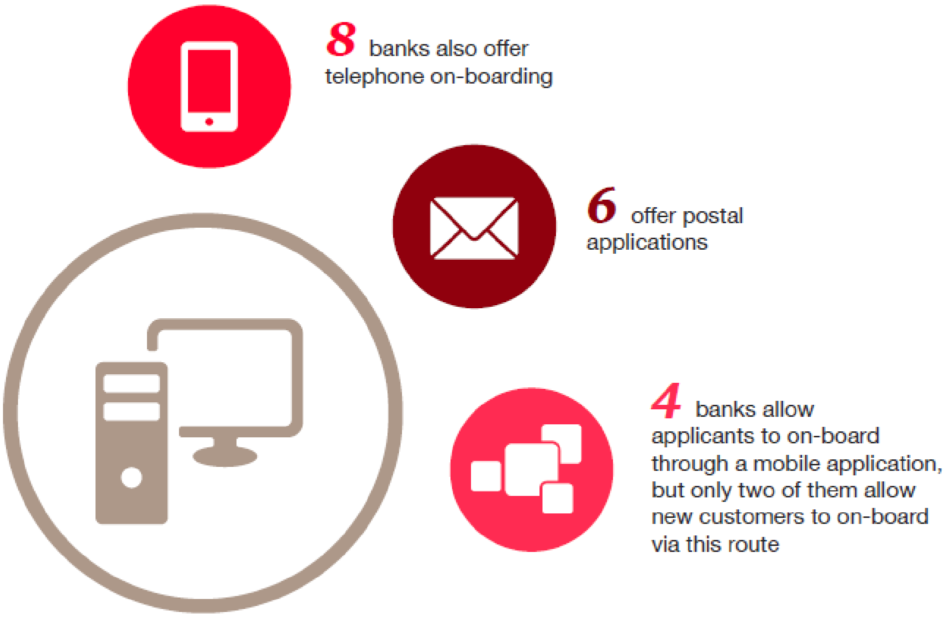
> *"GOV.UK Verify verifies the minimum data required by the JMLSG."*

Where an applicant has historical values for name, address and date of birth, three years of historical data is available.

Data Attributes collected by banks

Methods of collection

For non face-to-face on-boarding, most banks interviewed collect data attributes through the use of an online webpage. Eight banks also offer telephone on-boarding and six offer postal applications. Four banks allow existing customers to activate a new product through a mobile application, but only two of them allow new customers to on-board via this route.


8 banks also offer telephone on-boarding
6 offer postal applications
4 banks allow applicants to on-board through a mobile application, but only two of them allow new customers to on-board via this route

Most Banks collect this information through the use of an online webpage

One bank interviewed can collect the required set of data through photographic capture of a government issued identity document or through access to an applicant's Apple Pay account using their thumbprint.

Identity – Core Attributes

All banks surveyed collected the identity data set out in the JMLSG guidance. These principal identity attributes are also available as verified output of GOV.UK Verify.

A number of variations were observed in core identity attribute collection between banks:

Identity Attributes

Name

8
banks required collection of First Name, Middle Name and Last Name

3
banks did not collect Middle Name

1
bank could collect up to 5 previous names, where required

Address

8
banks collected a 3 year address history for applicants

3
banks collected a 12 month address history if the applicant had been at their address less than 3 or 6 months

5
banks provided an option to provide multiple addresses. These include primary, residential and correspondence addresses. In some instances this information was verified.

Date of Birth

All banks collected an applicant's date of birth

Gender

Only **1** bank surveyed did not collect an applicant's gender. However we noted as part of our discussions that many Banks were moving away from this.

KYC and On-boarding – Data Attributes

In addition to the core identity attributes collected by all banks surveyed, for most banks, a wider set of data attributes was also required to be collected. For the purposes of this project, these data attributes have been split into "KYC Data Attributes", which are collected for regulatory or legal requirements, and "On-boarding Attributes" which are collected to fulfil bank specific on-boarding requirements:

KYC

Information for tax residency requirements

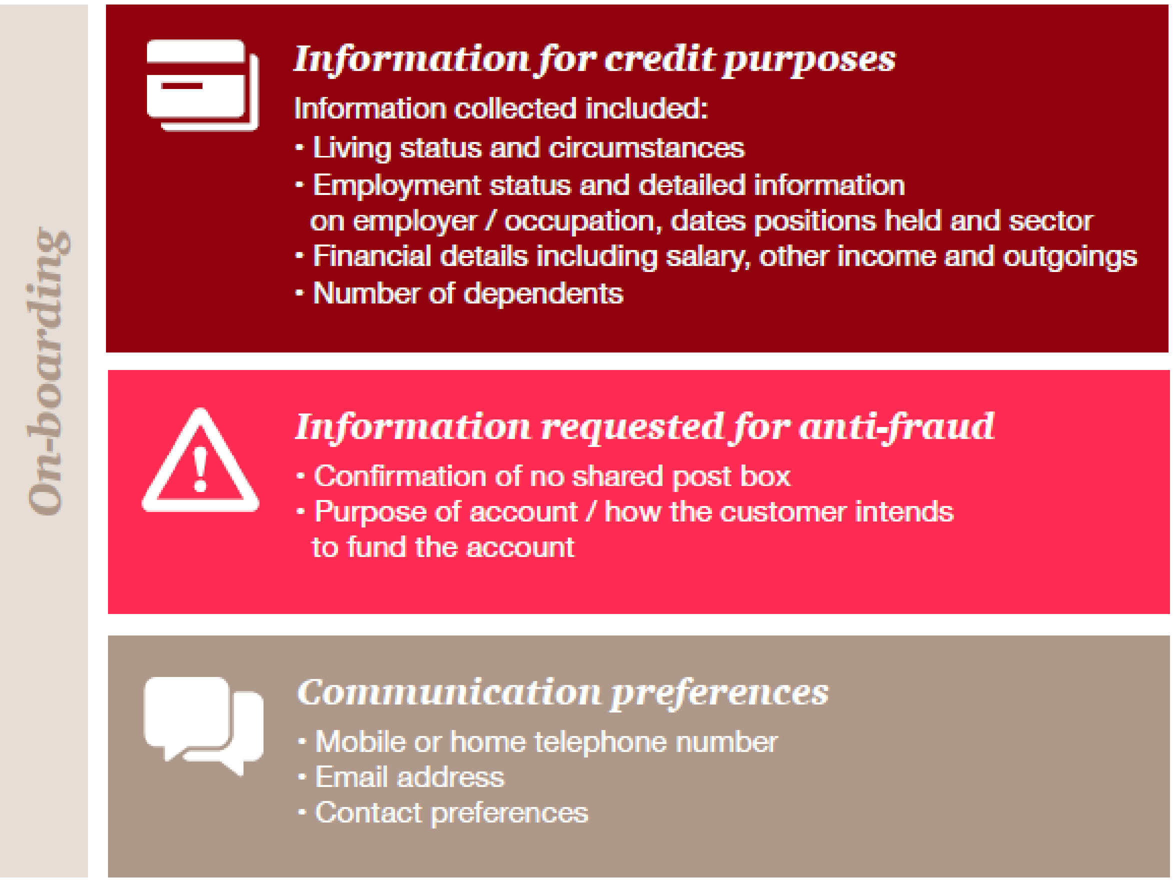
Ten banks surveyed either collected an applicant's tax residency status or as part of the eligibility for an account would ask an applicant to confirm they were UK resident for tax purposes.

In most cases this information is requested during the account opening stage. However one bank in our sample requested this information post account opening.

Information requested for customer profiling and risk rating

Information collected included:

- Nationality / country or city of birth
- Marital status
- Other names / alias
- Other addresses



On-boarding

Information for credit purposes

Information collected included:

- Living status and circumstances
- Employment status and detailed information on employer / occupation, dates positions held and sector
- Financial details including salary, other income and outgoings
- Number of dependents

Information requested for anti-fraud

- Confirmation of no shared post box
- Purpose of account / how the customer intends to fund the account

Communication preferences

- Mobile or home telephone number
- Email address
- Contact preferences

Full data requirements are set out in Appendix B.

Where this information is not specifically requested from a customer, it may be available to the bank through other means. For example, some of the challenger banks did not require an applicant to directly enter information but were able to extract it using technology.

Much of the on-boarding data which is collected by banks is done so as industry practice. For example it is not a regulatory requirement to collect information on a customer's nationality or marital status, but this can help with risk rating or product targeting, for example. For the larger banks this can be helpful to identify false positives when screening hits occur.

Some banks also collected further information for anti-fraud controls or to help them contact customers.

Comparison to GOV.UK Verify

The data attributes collected under GOV.UK Verify are sufficient to fulfil the identity part of the interviewed banks' non face-to-face customer on-boarding processes.

However, in order to complete the customer on-boarding process, all banks interviewed required additional information. This was required to fulfil KYC requirements and also other on-boarding requirements. This varied by category of bank interviewed:

> *"The data attributes provided by GOV.UK Verify would be sufficient to meet JMLSG guidance on the standard evidence required to identify a private individual."*

		Outputs	Collected attributes		
		GOV.UK Verify Output	Challenger	Mid-tier Retail	Large Retail
Identity	Core Identity Attributes (KYC) *Minimum regulatory requirement*	✓	✓	✓	✓
KYC	Information collected on Tax Residency		✓	✓	✓
	Information collected /requested customer profiling and risk rating		✓*	✓	✓
On-boarding	Information collected /requested for credit purposes		✓*	✓	✓
	Information collected /requested for anti-fraud[5]		✓*	✓	✓
	Communication preferences			✓	✓

*Although the challenger banks interviewed did not require the applicant to enter this information similar information was obtained through the use of technology.

GOV.UK Verify has been designed to provide a means of digital identity. Whilst this digital identity may be used for a variety of purposes, it was originally designed for the provision of access to Government services. The establishment of a digital ID does not by itself mean that an individual will be eligible for a particular service.

In addition to identity attributes, the banks collect significant additional data attributes not provided by GOV.UK Verify. These are collected both for wider KYC and on-boarding purposes, and to meet other obligations e.g. tax residency obligations.

A more detailed version of this table is included as Appendix B.

[5] This refers to information collected from applicants for the purpose of anti-fraud checks. The anti-fraud checks for identity purposes performed by GOV.UK Verify are covered in section 6.5

Electronic Identification and Verification ("eID&V")

Verification performed under GOV.UK Verify

The Identity Proofing and Verification Manual ("IPV Manual") sets out the steps required by IDPs in order to validate the Claimed Identity:

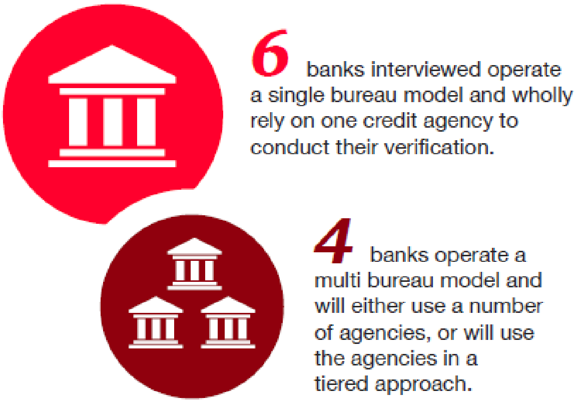
1. Ensuring the Claimed Identity provided is the same identified by the Identity Evidence;
2. Validation of the Identity Evidence to ensure it is authentic. This could involve physical inspection, reading embedded chips in documents, or electronically validating an electronic signature. To test that the evidence is valid, checks are performed against the Issuing Source (e.g. DVLA or Passport Office in the UK);
3. Verification is performed through knowledge based verification, physical comparison (either face-to-face or through a video streaming link) or through a biometric. Depending on the method used, a higher level of assurance can be provided. Currently GOV.UK Verify provides LOA2;
4. A counter-fraud check is performed (see section 6.5); and
5. Activity history is assessed to ensure the Claimed Identity has been in existence over time.

The additional verification check to mitigate against the risk of anti-impersonation is in line meet the JMLSG Guidance recommendations on electronic verification.

Current Bank industry practice

Ten banks surveyed use credit reference agencies to electronically validate information provided in the application stage. The credit reference agencies used included Experian, Equifax and Callcredit.

One bank does not allow non face to face on-boarding and all applications are conducted in branch. Six banks interviewed operate a single bureau model and wholly rely on one credit agency to conduct their validation. Four banks operate a multi bureau model and will either use a number of agencies, or will use the agencies in a tiered approach. A successful check usually requires a balance of positive indicators and lack of negative indicators.



6 banks interviewed operate a single bureau model and wholly rely on one credit agency to conduct their verification.

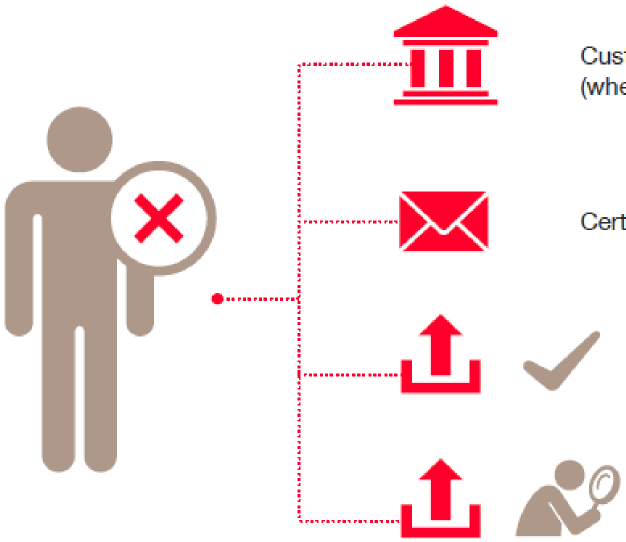
4 banks operate a multi bureau model and will either use a number of agencies, or will use the agencies in a tiered approach.

Failure of eID&V checks

When an applicant fails an eID&V check it is not always possible for them to continue their journey to on-board in a non face-to-face context. There are a number of different routes:

Failure of eID&V checks

When an applicant fails an eID&V check it is not always possible for them to continue their journey to on-board in a non face-to-face context. There are a number of different routes:



Customer is required to come into a branch (where applicable) and present identity documents;

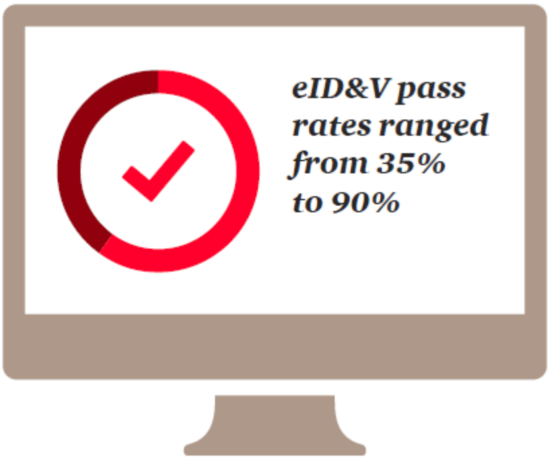
Certified identity documents can be provided via post;

Scanned copies of the identity documents can be uploaded and are checked using electronic documentation checking technology;

Scanned copies of the identity documents can be uploaded and are physically inspected.

For one bank, the customer journey ends where the eID&V check is failed. For six banks, the non face-t0-face customer journey can continue with documents provided via an electronic document checking service or by post. Three banks would end the non face-to-face journey here and request the applicant visits a branch to complete their application.

In addition to eID&V, two banks also used knowledge based verification questions as an additional measure to verify an applicant. Knowledge based verification involves using knowledge of private information on an individual to verify that the person providing the identity information is the owner of the identity.



eID&V pass rates ranged from 35% to 90%

<u>Comparison to eID&V carried out by GOV.UK Verify</u>

GOV.UK Verify is able to validate identity evidence by checking asserted details with the issuing source. Banks currently rely on information held by credit reference agencies who use a combination of publicly available information, such as electoral rolls, and credit history information which is shared by lenders, to verify their customers non face-to-face.

Banks do not currently undertake checks on an applicant’s activity history or tenure, as conducted by GOV.UK Verify.

For the majority of banks in the sample, the customer journey does not end if the applicant fails eID&V checks. All banks offer alternative on-boarding processes. Under the GOV.UK Verify process, an applicant would have the option of trying another provider where the verification process fails.

Anti-fraud controls

Anti-fraud measures in GOV.UK Verify

GOV.UK Verify runs a significant number of anti-fraud checks around identity. The IPV Manual issued by the Cabinet Office sets out the anti-fraud checks performed by GOV.UK Verify in relation to identity. The IDP is required to have the following counter-fraud checking capabilities:

- Whether the Claimed Identity has been subject to identity theft, regardless of whether it was successful or not;
- That the Claimed Identity is known to reliable and independent sources (i.e. not a zero footprint identity);
- Whether the address is associated with identity fraud;
- Whether the Claimed Identity is deceased; or
- Whether the address history of the Claimed Identity is consistent with the declaration by the Customer.

All identity providers use a range of independent sources for identity fraud checks.

The IPV Manual sets an extensive list of "contra-indicators". These can be defined as information that either contradicts statements from an applicant or raises some doubt over whether the applicant is legitimate. These can be discovered during the identity proofing process or during the lifetime of an account. The discovery of a contra-indicator will usually require investigation. To successfully verify an applicant's identity there can be no confirmed contra-indicators.

Anti-fraud measures adopted by banks

All banks interviewed conducted anti-fraud checks on applicants. Eight banks conducted these prior to account opening and three conducted them after the account was opened. A range of third party providers were used by banks to conduct these checks. The fraud checks also included checking for re-direction of mail or whether the identity belongs to a deceased person.

In addition to fraud checks, all banks interviewed conducted anti-impersonation checks. These included the following:

- Sending a letter to the applicant's asserted and verified address for them to sign and return;
- Sending the card to the applicant's asserted and verified address for them to activate; and
- Sending welcome letters to the applicant's asserted and verified address.

Two banks required confirmation that the applicant did not have a shared post box.

Comparison to GOV.UK Verify

As part of the customer on-boarding process, GOV.UK Verify and banks both conduct thorough anti-impersonation fraud checks. Anti-impersonation fraud checks undertaken by GOV.UK Verify rely on electronic means. Most banks undertook additional anti-impersonation fraud checks such as direct mailing to postal addresses as recommended by JMLSG[6]. Whilst redundant from a risk mitigation perspective, these additional anti-impersonation fraud checks could continue to be used alongside a digital ID.

[6] JMLSG Guidance Part 1, Mitigation of impersonation risk, 5.3.82

Technology & Device Security

A variety of location and device security checks are performed by some banks. These include the following:

- IP address checks to ensure it is not blocked and is in line with address information supplied; and
- Where a customer is on-boarding through an app, two banks use a mobile phones' geolocation feature to check where a customer is located.

In addition, one bank uses a biometric as part of its on-boarding process. This bank operated processes to electronically check the validity of identity documents and could un-lock and read e-chips where present. Five banks surveyed are actively looking into introducing biometrics as part of the customer on-boarding process.

Some banks only allow operation of the account with a registered device. Whilst GOV.UK Verify operates a variety of identity and device security features, it is device agnostic. The seven IDPs currently contracted under GOV.UK Verify are also investigating the use of biometrics and other developing technologies. Each Identity Provider agrees a pipeline of enhancements to their service with the Government Digital Service.

Customer On-Boarding Processes performed by banks

In addition to the data attribute collection described in Section 6.3, a number of processes are performed before on-boarding can be completed. These processes are not conducted under GOV.UK Verify.

The scope of the end to end customer on-boarding process also includes the following:

- Credit checks
- Screening
- Additional due diligence for high risk clients
- Risk rating

Ten banks surveyed conduct screening for Politically Exposed Persons ("PEPs") and Sanctions purposes. One bank did not perform any automated screening. A variety of third party and in-house systems are used. In addition, five banks conduct negative news screening on applicants.

Five banks use employment information to establish source of wealth and source of funds. One bank asks how the customer intends to fund the account at the on-boarding stage. Three banks only collect information on source of wealth and source of funds as part of EDD where the applicant is considered to be high risk.

Six banks risk rate their customers using a combination of the attributes collected at the account opening stage. These include product type, country of residence, channel through which the application has been performed, and geographic location. Two banks risk rate customers based on their transaction history.

For all banks the on-boarding process for customers who pass eID&V checks or screening checks is an automated process with no manual sign off.

7. Comparison of GOV.UK Verify to customer on-boarding practices

The data attributes provided by GOV.UK Verify would be sufficient to meet JMLSG guidance on the standard evidence required to identify a private individual.

The JMLSG Guidance is prescriptive as to the method of electronic verification which is required. Different standards for electronic verification are applied by GOV.UK Verify.

The level of identity assurance provided by GOV.UK Verify is Level 2. Of the bank's interviewed, the levels of identity assurance ranged between Level 1 and Level 2. Therefore, in some cases the identity assurance provided by GOV.UK Verify is higher than the banks currently believe their systems are achieving.

> ***"The level of identity assurance provided by GOV.UK Verify is Level 2… in some cases the assurance provided by GOV.UK Verify is higher than banks believe their systems are currently achieving."***

At present the on-boarding and verification processes are owned by the banks which undertake them. If a different model such as GOV.UK Verify for identity verification were to be adopted, the banks all queried the level to which they could rely on GOV.UK Verify and the extent to which the bank would assume liability. The question of liability was a critical issue raised by all the respondent banks.

A challenger bank saw its on-boarding and verification processes, using a variety of innovative technologies, as a source of competitive advantage over their larger and more established rivals.

> ***Some banks see their on-boarding process as a "source of competitive advantage"***

The scope of customer on-boarding also includes processes which are wider than identification and verification of an individual, for example credit checks and fraud checks including additional anti-impersonation and screening. The verified data attributes provided by GOV.UK Verify are limited by design and additional data related to an individual might be shared in instances where information is required for example for discounting or a fraud investigation.

Challenges in adopting GOV.UK Verify

During interviews with the participating banks, a number of challenges in adopting GOV.UK Verify were discussed. A consistent theme was a concern about the cost of adopting and using GOV.UK Verify. Participating banks were keen to stress that the cost of using GOV.UK Verify would have to be commercially viable for them to adopt it.

> ***"Participating banks were keen to stress that the cost of using GOV.UK Verify would have to be commercially viable for them to adopt it"***

The banks interviewed wanted to understand how much reliance they could place on the assured identity output of GOV.UK Verify. In order to place reliance on this, a number of banks said they would need to understand more about the processes which underpin the authenticated ID performed by the IDPs.

The customer experience is very important to banks and they were interested to understand how GOV.UK Verify could be integrated with their current on-boarding journeys. There was concern about the extent to which GOV.UK Verify could contribute to a more holistic on-boarding experience and how it could be integrated with processes required to collect the additional data points required to meet specific KYC and on-boarding requirements.

In addition, there are processes which are included as part of the on-boarding journey which are not part of the scope of GOV.UK Verify. Credit checks would still be required by a number of banks and in all instances these are provided as part of the output of eID&V.

Most banks interviewed noted that they are constantly looking for new ways to enhance and innovate their current on-boarding process. One bank had already integrated a biometric and a number spoke about future plans to use biometrics. Further clarification on how this may work alongside a digital ID would be required.

Banks also raised the question as to whether there would be a choice of identity providers. Some noted that they may be uncomfortable with a market competitor undertaking identity checks and the brand confusion this may cause to the end customer.

8. Future developments

Payments Services Directive II

The UK Payments Services Directive II ("PSD2") came into force in January 2016. PSD2 requires that all EU Member States implement these rules as national law by January 2018. This will require Payment Service Providers ("PSPs") to enhance their security requirements through the use of strong customer authentication. Of the banks interviewed, one is already using a biometric and five have future plans to introduce a biometric as part of the customer on-boarding process.

> ***"Of the banks interviewed, one bank is already using a biometric and five have future plans in place as part of the customer on-boarding process."***

Payments Account Directive

The Payments Account Directive ("PAD") was adopted in July 2014 and implemented in banks in 2016. It seeks to improve switching of accounts and access to basic bank accounts to ensure all consumers legally resident in the EU have access to basic banking services.

Amendments to the 4th EU Money Laundering Directive

The European Banking Federation ("EBF") has suggested a number of amendments to the proposal amending the AMLD4 around e-identification. A proposal has been made to widen the e-identification schemes to include those not notified as eIDAS services but those which are fully compliant with the technical and security requirements arising from eIDAS.

9. Glossary of terms and abbreviations

Eligibility – The criteria by which an individuals' attributes are considered for access to products and services

Identity – Identification of a customer in accordance with UK Regulatory Guidance

Identity Assurance – The process that determines the level of confidence that an applicant's identity is their real identity

IDP – Identity Provider

IPV – Identity Proofing and Verification

JMLSG – Joint Money Laundering Steering Group

Know Your Customer (KYC) – Includes identification of a customer and also understanding your customer more broadly. The scope of KYC for this exercise includes tax residency information and additional information over and above identity on a customer.

On-boarding – Refers to the end-to-end process of on-boarding a client. This includes KYC and also the additional processes undertaken by an institution to on-board a client.

Verification – The process performed to determine whether an applicant owns an identity

Appendices

Appendix A

The BBA invited banks to contribute towards this exercise.

In order to obtain as broad an understanding of the UK retail banking KYC requirements as possible, the BBA ensured the final sample spanned the full spectrum of the retail banking industry including a credit union and a mutual. Collectively these have been referred to as "banks" throughout this document.

For the purposes of presenting the findings of these interviews and to provide an element of comparability, participating banks have been divided into three categories:

Large Retail	**Mid-Tier Retail**	**Challenger**
Barclays	Co-operative Bank	Starling Bank
HSBC	South Yorkshire Credit Union	U Account
Royal Bank of Scotland	Nationwide	
Lloyds Banking Group	Tesco Bank	
Santander		

Appendix B

Consolidated table of findings

Attribute	Bank A	Bank B	Bank C	Bank D	Bank E	Bank F	Bank G	Bank H	Bank I	Bank J	Bank K
Title	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
First Name	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Middle Name	✓			✓	✓	✓		✓	✓	✓	✓
Last Name	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Other names						✓			✓	✓	✓
Gender	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Date of Birth	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Address	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Address History	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Correspondence Address				✓		✓			✓	✓	
Domicile Address	✓										
Nationality	✓	✓		✓		✓		✓	✓	✓	✓
Dual Nationality										✓	
Citizenship in other countries									✓		
Country/City of Birth	✓					✓		✓	✓	✓	
Marital Status	✓	✓				✓		✓	✓	✓	✓

Attribute	Bank A	Bank B	Bank C	Bank D	Bank E	Bank F	Bank G	Bank H	Bank I	Bank J	Bank K
Living Status/Residential status	✓							✓	✓	✓	✓
Mother's maiden name	✓	✓									
Employment status	✓					✓		✓	✓	✓	✓
Employer Name	✓	✓			✓	✓		✓	✓	✓	✓
Employer Address	✓				✓	✓		✓	✓		
Occupation	✓	✓		✓		✓		✓	✓	✓	✓
Sector										✓	
Employment start date	✓							✓	✓	✓	✓
Source of income	✓					✓		✓	✓	✓	
Salary		✓				✓		✓	✓	✓	
Income before tax	✓	✓				✓		✓	✓	✓	✓
Annual income	✓	✓				✓		✓	✓	✓	✓
Frequency of overtime or bonus	✓					✓		✓			
Frequency of pay									✓		
Total income	✓	✓				✓			✓	✓	✓

Attribute	Bank A	Bank B	Bank C	Bank D	Bank E	Bank F	Bank G	Bank H	Bank I	Bank J	Bank K
Savings and assets									✓		
Other income								✓	✓	✓	
Tax residency status	✓	✓		✓		✓		✓	✓	✓	✓
Number of dependents								✓	✓	✓	✓
National insurance number					✓					✓	
Initial deposit amount					✓						
Shared letterbox								✓		✓	
Purpose of accounts				✓					✓	✓	
Source of funds to account	✓			✓				✓	✓	✓	✓
Childcare/maintenance costs									✓		
Rent/mortgage costs									✓		
Other credit cards									✓		
Declared bankruptcy									✓		
Monthly council									✓		✓

Attribute	Bank A	Bank B	Bank C	Bank D	Bank E	Bank F	Bank G	Bank H	Bank I	Bank J	Bank K
tax											
Owner of other properties									✓		
Email address	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Telephone number	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓