OPEN IDENTITY EXCHANGE

THE USE OF BANK DATA FOR IDENTITY VERIFICATION

White Paper

August 2015

Contributors

OIX UK is the UK arm of a global organisation and works closely with the Cabinet Office on the Identity Assurance Programme. Its goal is to enable the expansion of online identity services and adoption of new online identity products. It works as a broker between industries, designing, testing and developing pilot projects to test real use cases.

Table of Contents

Objectives of the White Paper

To articulate the benefits of consented reuse of bank data through an industry wide open standard, to improve the efficacy of identity verification of individuals in the UK.

Who should read this white paper?

- Senior stakeholders in the banks that are interested in a future digital identity market;
- Banks that are seeking to engage further in the Identity space and are actively exploring value proposition that could be created by their customer identity information;
- Identity Providers;
- Data aggregators and other stakeholders in the market.

1. Executive Summary

The growth of digitised service delivery across private and Government sectors in the UK is putting traditional customer identification and Know Your Customer (KYC) processes under increasing pressure. The cost to the UK economy of the current inefficiencies of customer identification and onboarding is estimated at over £3.3 billion per year[1], with organisations trying to balance their regulatory obligations with the need to on-board customers at lowest cost and least friction.

The cost and time of identifying consumers slows down digitisation and the development of innovative financial services, and it also holds back the other industries that rely upon the existence of verified bank identities. Government needs a higher level of identity assurance for its own service digitisation.

An effective digital identity marketplace solves many of these problems, and the GOV.UK Verify service is an important investment that seeks to kick-start this market. Meanwhile, there are strong arguments for banks to invest in the identity market to enable digital propositions for their new and existing customers.

The current market for identity assurance identity services is not able to serve 100% of the population. The main opportunities to increase the demographic coverage of identity assurance services relate to how many people are covered by the data and methods available to providers to achieve the required levels of assurance in 5 elements of identity proofing and verification[2]. This paper explains the current landscape of the market of data services that supports identity verification and the opportunity this creates for the banking sector.

The banks have an important role to play in the development of the digital identity market. Banks are obliged to meet high standards for identity verification when opening accounts for customers, usually derived from a face-to-face inspection of the customer's identity documents (e.g. passport, driving licence). Online digital identity services do not have this face-to-face option, and instead currently rely upon corroboration of digital evidence from trustworthy sources such as bank or credit card account as a part of the process when verifying a person's identity.

However, the bank data used today is derived from secondary sources and not provided by the banks specifically for identity purposes. Key challenges of commercial viability, strategic value, data quality, liability, privacy and user consent[3] need to be addressed for bank transaction data or credit card evidence to support digital identity verification effectively.

This discovery project has hypothesised a model by which bank data could be shared more directly and efficiently to GOV.UK Verify certified companies and others in the identity services market. The project has approached the challenge with the assumption that such a service must be beneficial for all parties, and in particular, commercially viable for the banks. There must be clear value to citizens, and a clearly defined privacy approach that is acceptable to the stakeholders.

Regulations currently in development in the EU and UK will affect the ways in which some data is shared by the banks. Therefore, the project has also considered the regulatory landscape and future regulatory challenges for the

[1] The Economics of Identity Ctrl-Shift, 2014
[2] https://identityassurance.blog.gov.uk/2015/06/16/how-gov-uk-verify-works-a-film/
[3] See Appendix A for more detail on privacy and consent.

banks. Based on the findings of this discovery project, an 'alpha' project is proposed to develop a more detailed design, and then transition into a proof of concept, to show how bank information can enable a wider demographic to create a trustworthy digital identity. This should be done as an Open Identity Exchange (OIX) project.

The aim of this paper is to report on the findings of a project that explored the consented use of bank data through an industry open standard, to improve the efficacy of identity verification of individuals in the UK. It then argues that there will be commercial and strategic benefits for all stakeholders to engage and support an alpha project.

GOV.UK Verify is a Cabinet Office initiative under the Government Digital Services (GDS) programme.

It enables people to access public services digitally by establishing a digital identity through a private sector identity service that meets a high standard of assurance described further in Appendix B and defined in the Cabinet Office Good Practice Guide 45 (GPG 45).

In time this will significantly reduce the cost of delivery of public services as well as providing a convenient digital channel for users. Digital identities created to this standard are sufficient to meet Anti Money Laundering (AML) and Know Your Customer (KYC) requirements for identity verification[4]. Benefits from this initiative are described in the Benefits to Stakeholders section in this paper.

At this time of publication of this paper the GOV.UK Verify service is a beta service. It has set a number of objectives[5] to achieve before becoming a fully live service and reports publicly on its progress against these objectives.[6]

In this early market the supply chain of data sources to support the creation of digital identity has not yet evolved to support the GOV.UK Verify initiative. The Digital Data Deficit section below describes how many users assertions of identity cannot be digitally verified and the challenges that users face as a result.

[4] Regulation 17 of the Money Laundering Regulations 2007 allows reliance on third parties to apply any customer due diligence measures.
[5] https://identityassurance.blog.gov.uk/2015/03/26/gov-uk-verify-objectives-for-live/
[6] https://www.gov.uk/performance/govuk-verify

2. Regulatory Dynamics in the Banking Sector

Over the next two years two significant regulatory events will occur that will potentially require banks to make a significant portion of their customer data available (upon consented request) to a new category of third parties, and banks will need to address the risks associated with this new regulatory context.

The Revised Payment Services Directive[7]

The Revised Payment Services Directive (PSD 2) is a European Directive that at time of writing is entering the final stage of the legislative process and is expected to be published in autumn 2015. It amends the current regulatory environment for banks in a number of ways but the most significant is the introduction of new regulated services. They are split broadly into three categories, but the two most pertinent are Account Information Services (AIS), e.g. account aggregation, and Payment Initiation Services (PIS), which enable payments to be initiated on behalf of customers straight from their bank account to a payee. These services can be offered by payment services providers (e.g. banks) or by 'third party providers', who will therefore need to have access to customers' account information on a consented basis.

The conclusion is that after full implementation of PSD2 there will be an environment where consumers can more easily allow current and new services providers to manage their personal finances, aggregate their data and initiate payments on their behalf.

Data Sharing and Open APIs in Banking[8]

In the March 2015 Budget, HMT committed to deliver an Open API (Application Programming Interface) standard in banking. They believe that allowing customers to have easier and more open access to their data will lead to benefits and encourage innovation. They believe the development of an API standard that meets the requirements around data protection and security, with reasonable cost, could be feasible in 1 to 2 years.

There is clearly an overlap between the HMT proposals and what will emerge as a result of PSD2. However, there are also some differences between the two proposals, particularly around scope. At the time of writing the industry is still awaiting formal confirmation of how HMT will take the API proposals forward.

The implications of PSD2 and the direction created by HMT's Open API proposals are potentially very significant. Customers are likely to become accustomed to consenting to have their bank data used in order to access new services, which may include digital identity services. Complying with the legislation will be a major investment for the banks, and therefore it is likely that many will be keen to explore what opportunities can be created.

[7] Legislation titles in full: Proposal {..} on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC (COD/2013/0264)
[8] HM Treasury: Data Sharing and Open APIs in Banking. Consultation opened 18 March 2015.

3. The potential value of consented banking data for identity assurance services

GOV.UK Verify is a different approach to allow citizens to operate on-line to the current Government Gateway. GOV.UK Verify is an early example of a federated approach to digital identity, which is based on establishing many Identity Providers that leverage various data sources, and allow consumers a single registration and login mechanism to access multiple services.

The government has developed standards that the Identity Providers must meet which are designed to make the creation and maintenance of fraudulent identities increasingly difficult with each defined 'Level of Assurance'. An overview of how Identity Providers meet the government's standards is found in Appendix B. They require data from different sources to be validated, checked and / or corroborated against one another. For the purposes of validating identity evidence, these data sources are categorised under the headings 'Citizen', 'Money' and 'Living'. The corroborated data sources must be under at least 2 different categories. Providers are also required to establish that an identity has been active over time. Banking data could help providers meet the required standards in both of these elements, for people whose identity cannot currently be verified using the available data sources.

Identity Providers can validate user-entered data by corroborating it against authoritative sources. There is currently no agreement to access bank data directly. As a result, some people who don't have credit accounts (such as a loan, mortgage or credit card) are not able to assert financial evidence by entering in the details of a bank account. In addition, lack of direct access to or interrogation of consented banking data means that providers are not able to refer to bank account data to establish that an identity has been active over time.

The Cabinet Office programme has therefore been working with the controllers of large customer data sets that use data that have been shared by banks for other purposes, primarily credit risk management. However, directly provided data could meet a wider range of needs, particularly in respect of activity history.

The following section describes the challenges with the derived bank data currently available[9].

4. Current use of bank data for identity assurance

This section discusses how banking data is currently used for identity verification in the context of GOV.UK Verify. It is set out in terms of the government standards[10].

[9] The data currently used includes data from banks and also from non-bank financial institutions, particularly credit providers.

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

The 'Money' Category

The unbanked population of the UK is relatively low, so operation of a bank account or credit card is a very valuable attribute that links much of the target population. These attributes can be categorised in the 'money' category, which, when fulfilled, allows the evidence present to be classed as 'moderate strength' under Good Practice Guide 45 (see Element A) if:

- The Issuing Source of the Identity Evidence confirmed the applicant's identity in a manner that complies with the identity checking requirements of The Money Laundering Regulations 2007.
- The issuing process for the Identity Evidence ensured that it was delivered into possession of the person to whom it relates.
- The issued Identity Evidence contains at least one reference number that uniquely identifies itself or the person to whom it relates.

The use of some authoritative sources in the money category, where the source was not originally intended as a source of data for identity services, is resulting in variable results for users and problems can occur when users attempt to validate money evidence:

- Some bank account and credit card details are not present in the authoritative source data sets due to a lack of user consent; this is typically for accounts that pre-dated the current Data Protection Act, and so the account holder did not agree to any data sharing. An Identity Provider cannot always pre-determine the outcome before asking a user to enter details of a bank account; therefore sometimes users enter valid bank details and have them rejected as invalid.
- There is sometimes a mismatch between the identifiers known to users and those held by the authoritative source. This is common with some credit and debit card numbers where the authoritative source holds an internal identifier from the issuing source.

Privacy, Consent and Data Protection

This project has been mindful of the challenges and risks surrounding privacy, consent and data protection:

User Perception: *Service users may assume that the identity provider has access to their bank funds or may use their records for other purposes.*

Liability: *In the event of fraud or service failure, the stakeholders may dispute liability for any damage or costs associated with rectifying poor quality data. although if the Treasury open API approach is adopted it is likely the banks will not take liability for the data once it has left their estate*

Dispute: *The service will need a common supervisor/ombudsman to resolve disputes between the various stakeholders.*

For further information – see Appendix A.

Identity Providers require a service through which they can validate the bank account or credit card number asserted by a user to meet the requirements of Elements A and B of the Good Practice Guide 45.

Knowledge Based Verification

Identity Providers need to be able to link the person to the identity to meet Element C of the Good Practice Guide 45. Some Identity Providers achieve this by generating questions. Banking data could help to generate questions for users who don't have sufficient material in their credit records to generate the required strength and range of question.

Knowledge based verification must be based on data held within an authoritative source, which is used to generate questions that only the user is likely to know the answer to. There are a number of common issues relating to this data when it is not derived directly from banking sources:

- The data is not current; balance information maybe a month or more out of date or accounts may have been closed in intervening period.
- The service provider's name prompted in the questions may not be familiar to the user; for instance a trading vs. commercial name or a change due to a merger or acquisition.
- A user's credit or debit card number may differ from the question due to the authoritative source holding an internal identifier from the issuing source.

Activity History

Identity Providers need to be able to establish that users have been active over time. Banks could provide confirmation that a user has been active over time, in line with the Good Practice Guide 45 Element E. This would help Identity Providers to verify those users' identities that cannot currently be verified because there is insufficient evidence of activity history in currently available data sources.

The 'activity history' of the claimed identity should be based upon real world activity by the person. This is sometimes difficult to determine from the authoritative sources commonly used by Identity Providers because:

- These sources do not always contain sufficient transactional data; they may denote payment history through an automated payment on a credit facility.
- The balance data for bank accounts only reports the balance of an overdraft facility, if one is in place - it does not report a positive balance (because that is not a credit facility so is not relevant for credit history purposes).
- The frequency of updates on loans and mortgages does not always allow for granular analysis to derive sufficient evidence of activity history.
- Customers do not always have continuous / repeated activity history on their credit cards, so credit data is insufficient to demonstrate activity history to the required thresholds.

5. Proposition

The discovery project team considered the different data sources available in retail banks, and number of structural approaches, all of which needed to be viewed from a customer experience and data privacy perspective. Other considerations included the need to include all UK banks, irrespective of size and reach, to ensure the widest possible reach of the population, and where the solution could support customer segments currently under represented in derived data, such as students moving into working life, and older citizens.

The conclusion was that a service to allow interrogation of more granular, directly provided current account information than currently available from the derived data was a possible solution. For example, this might include transaction records as well as other types of bank data. This could be provided on a similar basis to the GOV.UK Verify document checking service[11], which allows providers to 'ask' a data source to validate a specific set of user-entered data, or check that a user's activity history meets the required thresholds, based on the user's consent (rather than the providers having general access to more data than they actually need to complete the required elements).

The discovery project team considered two ways that an alpha project could explore how to deliver such a service:

- A service that uses bank data held by a single data processor, such a payments settlement system. In this instance, individual banks, as data controllers, would permit the use of the data but would not be required to operate the service.
- An open standards-based service in which each bank developed data queries to a common design and service standard. Under this design a common interface might be stood up to route the service queries to the appropriate bank.

6. Benefits to Stakeholders

This section describes the benefits that would accrue to stakeholders if the banks chose to address the challenges described in section 4 above.

Citizens

The digital identity services market is in the early stages of development. Assuming the market continues to develop, citizens will benefit from a standardised, secure way to access multiple on-line services that protects their personal data and removes the need for multiple user IDs and passwords. As the market develops, having a digital identity will enable people to access an increasing range of digital public and commercial services. For example, buying a financial services product would be simpler when a digital identity is used, as it would remove the need for banks to request paper identity documents.

The ability to assert bank data would make it possible for more people to have their identity verified according to the government's standard when they set up a digital identity account. It would allow Identity Providers to validate bank account details provided by users, and check whether a user has been active through a bank account, based on the user's consent for the Identity Provider to access or interrogate the bank's data for that purpose. This will allow more citizens to access digital public services, and in future other services that require high assurance of identity.

[11] https://identityassurance.blog.gov.uk/2014/10/10/introducing-the-document-checking-service/

UK Retail Banks

The UK banks are currently split between those that have made specific investments in digital identity, and the bulk of banks that have not[12]. There are many views in the market as to why banks need to invest, and three main arguments are most commonly discussed.

Firstly, digital identity will create a new market of secure, verified, digitised attributes for the UK adult population. In future, the banks will be able to leverage this market to support their own customer onboarding, KYC obligations, remediation of customer information, fraud and sanction checking. Having access to digitised attribute information could be a major cost saving and enable genuine digitisation of banking, for example by enabling banks to allow people to open a new account without having to go into the branch.

Secondly, the identity information held by banks has commercial value, and GOV.UK Verify is an opportunity to begin to realise that value. Identity Providers will generate a revenue stream for banks derived from their requirements to verify users' identity details and maintain their currency through regular refreshing of the evidence. As the GOV.UK Verify model includes multiple Identity Providers, it is a competitive, commercial market. Banks will be able to compete and invest in the quality of the data that they provide to the market.

Finally, digital identity services delivered by non-bank Identity Providers could erode the relationship between banks and their retail customers, making the new market model that PSD2 will create even more challenging for banks. Participating in digital identity can become a strategy to maintain customer relationships.

Identity Providers

The primary benefit for Identity Providers is the availability of an additional source of data to validate user-entered data (element B), establish a link between the identity and the person (element C) and establish activity history (element E), which would help them achieve the required standards against the 5 elements of identity assurance at level of assurance 2. This would enable the providers to give people a wider range of ways to prove their identity, and increase their success rates in verifying people's identities. This means the customer experience will be better and rates of successful verification of identities will increase.

Government, and other IDPs

Delivery of bank data as a commercial service to Identity Providers would provide the growing market with the ability to make use of the largest amount of high quality, detailed customer identity information in the UK, using a clear customer consent journey and according to clear privacy principles and security standards.

[12] Payments UK engages with its members through the Identity Assurance Forum (IDAF). IDAF enables a more coherent and engaged discussion on the role of identity assurance and digital identities in the collaborative payments space.

7. Conclusions and Next Steps

Banks invest large amounts each year to protect their customers from fraud and meet regulatory obligations. As the use of digital channels increases the costs and complexities of this task are increasing. Establishment of trustworthy digital identities for citizens will be a significant economic benefit for all organisations and enable new and more efficient service propositions to be developed.

However, the complexities of this subject are significant and all stakeholders must consider how they can realise benefits from the proposed model. Successful solutions would need to be developed using iterative, agile discovery processes, and use open standards, rather than imposing proprietary industry designs. Agreement of the privacy and consent principles for the design will be a key consideration. The banks must decide where this opportunity fits into their own strategic roadmaps.

How bank data is used in the emerging digital identity systems will be of critical importance. A number of regulations are in development and banks must understand how they can achieve the policy objectives set out in legislation in a manner that is commercially viable and provides them with greatest opportunity.

The current market has need for more data sources to accurately verify identities across a wide demographic. Bank data as a service presents an opportunity to address current issues for the benefit of all parties. Considering the legislative drivers, the paper has outlined the benefits to stakeholders, including the banks, based on the prospect that the service will be commercially viable. It has articulated the benefits of consented interrogation of bank data through an industry wide open standard, to improve efficacy of identity verification of individuals in the UK.

Therefore, this paper proposes that an alpha project is initiated to prove that access to consented bank data can help provide high quality useful data as a service on the basis of consent and in compliance with identity assurance principles. The authors would encourage stakeholders with an interest in the 'alpha' to become involved in shaping this alpha project through the OIX forums.

Appendix A: Privacy and Consent

Privacy and consent are major considerations in the design of a service for validation of bank data. This section has been developed following conversations during the discovery phase. It was agreed that this level of detail should be reserved for an Alpha project. However, it has been included here to outline some of the key issues that have been considered and will be considered further at any later stage.

Attaining the user's consent to the processing of his / her personal data through the service will be a major consideration in the service design. To deliver the proposed service the bank and Identity Provider must have a contract in place to govern the data controller / data controller relationship and ensure that both parties are subject to common obligations for the proper handling of personal data. This would most likely take the form of a trust scheme so that multiple Identity Providers and banks can participate.

The Identity Provider must obtain evidence (to a sufficient level of assurance) of the service user's claimed identity, with checks to ensure that the verification is not part of a potential account takeover or other fraud. This evidence of identity would need to be derived from authoritative sources such as citizen documentation (e.g. passport, driving licence) and/or other appropriate sources that suffice to permit the verification.

Since the Identity Provider does not know what consent was provided by the service user to the bank when the service user/bank relationship was established, the Identity Provider must obtain fresh consent for:

- the repurposing of existing activity data for identity verification;
- the release of that data (or derived data) to a third party for assertion of identity;
- the potential intervention of other organisations for the purposes of audit, prevention or investigation of fraud, user support, or other governance activities.

The service must ensure that contractual liabilities in the event of a loss (or alleged loss) of user credentials or data are taken into account. If a financial institution refuses to compensate a customer for the loss of funds arising from misuse of credentials because the customer granted access for an Identity Provider, then broader consumer confidence in the scheme will be undermined by adverse publicity.

Prior to verifying the bank data, the Identity Provider should offer a fresh consent notice to the user, which describes in simple, easy-to-understand terms, the key uses of the data including:

- the identity of the data controller (the identity provider) and associated contact details
- purpose of access and how the data will be used
- sources and types of data to be accessed
- with whom the data may be shared and for what purposes
- for how long the data might be retained and why
- what controls are in place to protect the data
- where the data will be stored and processed

The Identity Provider should also make it clear that no more data will be accessed/obtained than is strictly needed to complete the verification. The Identity Provider must then obtain evidence of consent from the user to a level of confidence that can be proven to relying parties, e.g. by using the service user's credentials to digitally sign the consent notice.

The service will also need to consider revocation of consent (i.e. what steps are required if a user withdraws consent for processing), and subject accessibility (i.e. notifying the user upon request of all information held by the Identity Provider or released by the financial institution).

Consent interoperability

The identity provider submits the consent message to the bank, together with the service user's matching data set (name, address, date of birth and other details needed to singulate the service user) and the associated request for information. This data package will need to be formatted in a way that is understood by all parties (i.e. open standard) and signed by the identity provider.

Release of verification data

The bank releases the requested data to the Identity Provider. This should ideally comprise a hashed verification of data rather than primary transaction data, and should be signed with the bank's details and acknowledgement of the consent notice provided by the Identity Provider.

Outcome

The Identity Provider has obtained assurance of the service user's identity to the required level of assurance based upon bank transaction records, with an associated record of consent from the service user.

Appendix B: What makes a good data source or method?

GOV.UK Verify (Verify) is based upon a set of Identity Proofing and Verification (IPV) processes set out in GPG 45 IPV [13]. This establishes a common framework for establishing the requirement for the IPV of the identity of an individual. The guidance defines a process for assuring an identity at Level of Assurance (LOA) 2[14] and above:

- **Claimed Identity:** the Applicant shall be required to declare the name, date of birth and address that they wish to be known as so that there is no ambiguity about the identity that is going to be used. -
- **Identity Evidence Package:** the Applicant shall be required to provide evidence that the Claimed Identity exists. This may be provided electronically or physically depending on the level of assurance required and the capabilities of the organisation that is going to proof the Applicant.
- **Validation:** the evidence provided shall be checked in order to determine whether it is Genuine and/or Valid.
- **Verification:** the Applicant shall be compared to the provided evidence and/or knowledge about the Claimed Identity to determine whether it relates to them.
- **Activity History:** the Claimed Identity shall be subjected to checks to determine whether it has had an existence in the real world over a period of time
- **Counter-Fraud Checks:** the Claimed Identity shall be checked with various counter-fraud services to ensure that it is not a known fraudulent identity and to help protect individuals who have been victims of identity theft.

In order to accomplish the above, the IPV process has been defined as consisting of 5 Elements:

- IPV Element A – Strength of Identity Evidence from Citizen, Money and Living categories
- IPV Element B – Outcome of the Validation of Identity Evidence
- IPV Element C – Outcome of Identity Verification
- IPV Element D – Outcome of Counter-Fraud Checks
- IPV Element E – Activity History of the Claimed Identity

Details on pertinent aspects of these Elements are illustrated below.

Evidence required to fulfil IPV Element A must:

- Have been issued through a process that confirmed the applicant's identity through an identity checking process;
- Have been issued through a process that delivered the evidence into the possession of the person to whom it related;
- Have at least one unique reference number or image/photo/biometric of the person to whom it relates;
- Be held at an authoritative or issuing source that can be referenced during the IPV process in order for the evidence to be proved valid;

[13] For more details: https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

[14] A Level 2 Identity is a Claimed Identity with evidence that supports the real world existence and activity of that identity. The steps taken to determine that the identity relates to a real person and that the Applicant is owner of that identity might be offered in support of civil proceedings.

- Optionally, have features that can be checked during the IPV process in order for the evidence to be proved genuine;
- Allow the cross referencing against asserted Identity attributes (name, DOB, Address).
- Have Unique reference numbers that are known to the individual and not widely known or accessible.

Example of Evidence to fulfil the 'money' category of IPV Element A include:

- Bank account and sort code checked against name and address.
- Credit/Debit card numbers & CCV checked against name & address.
- Loans, Mortgages, insurance and other financial products checked against name & address.

Methods used to check that evidence is valid or genuine include:

- Checks against issuing or authoritative sources to determine if evidence is valid.
- Transactions carried out against financial products (for instance zero balance. payments) to determine if evidence valid (if combined with a feedback loop for a reference number then it proves access to a genuine account).
- Checks of cryptographic features on the evidence to determine if evidence genuine (e.g. Chip and PIN).

Element C determines that the entity asserting the Identity is the owner of the claimed identity; verification can be undertaken using a number of different methods:

- Static based verification - Verification of an individual through the issuance of a token through an out of band channel.
- Dynamic Knowledge Based Verification - Gathering information from the individual to prove they have sufficient knowledge about the claimed identity.
- Physical Comparison - Verifying the individual by a visual confirmation that they appear to be the person to whom the Identity Evidence was issued.
- Biometric Comparison - Verifying the individual by a biometric confirmation that they appear to be the person to whom the Identity Evidence was issued.

Methods used to verify an individual might include:

- An Identity proofing organisation makes a small payment into an individual's bank account (that has already been validated) with a unique reference number. The individual logs into the online banking provider and plays back the reference number to the Identity proofing organisation to complete the process.
- The individual is asked questions relating to attributes and transactions from a financial product, for instance:
    - Balance of account on a specific date;
    - Overdraft amounts;
    - Specific amounts paid/received;
    - Dates of specific transactions;
    - Locations of recent cashpoint withdrawals;
    - Details of direct debits to specific organisations (dates set-up, amounts etc.).

- Confirm the user knows the PIN for a chip and pin card through the use of a chip and pin device and cryptographic token previously issued to the known identity.

Element E Activity History of the Claimed Identity

This determines that there is proof of continuous existence of the claimed identity over a period of time backwards from the point of assessment. To qualify, the Activity Event shall relate to an interaction between the Claimed Identity and a source of Activity Events. This can be in either direction, e.g. the Claimed Identity using the services of the source or the source initiating an interaction with the Claimed Identity including issuing something to the Claimed Identity.

Examples of activity history relating to the Money category include:

- Setting up a direct debit (**not** the payment of a direct debit).
- A cashpoint withdrawal.
- Issuance of a cheque from the account.
- An Internet payment from the individual's account.
- The authentication of the individual in a specific channel (Online, Telephony, Face to Face).
- The authorisation of a payment using a mobile device linked to the individual.
- A face-to-face check of the individual and identity documents in accordance with Money Laundering regulations.