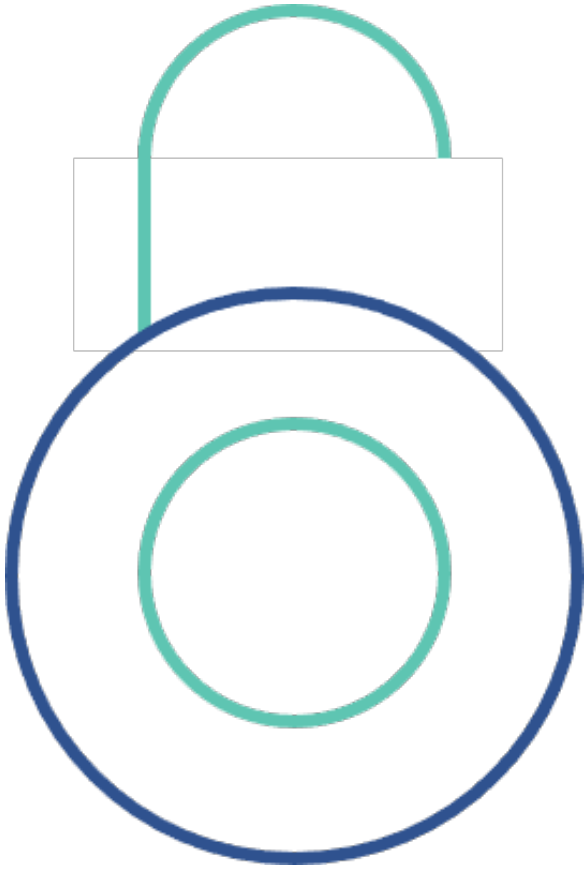
July 2022

UNLOCKING BANK ASSURED IDENTITY FOR THE FINANCE AND LEASING SECTOR



oneid®

EXPERT CONTRIBUTORS

CONTENTS

FOREWORD

This research project grew out of the current nervousness many lenders have in relation to using Digital ID in a way that fully complies with the Money Laundering Regulations (MLRs/Regulations). The MLRs currently exclude key wording which wasn't transposed over in January 2020, and which would have provided a safer 'regulatory harbour' in the digital/electronic identity space.

The Money Laundering Regulations (MLRs) were updated in January 2020 to say that identity may be verified '*by means of an electronic identification process, including by using electronic identification means or by using a trust service… and that process is secure from fraud and misuse and capable of providing assurance that the person claiming a particular identity is in fact the person with that identity, to a degree that is necessary for effectively managing and mitigating any risks of money laundering and terrorist financing'.*

The original text within the Fifth Money Laundering Directive (5AMLD), on which the MLRs are based, also included '*or any other secure, remote or electronic identification process* ***regulated, recognised, approved or accepted by the relevant national authorities.****'* This was not transposed into the UK regulations because neither the strategy nor authority had been articulated or developed at the time. As a result of this omission, the JMLSG has not felt able to front-run the Regulations to recommend the use of Digital Identities.

This environment is now changing, however, with the Government developing its Digital Identity and Attributes Trust Framework (DIATF), including a Governing Body, and its Good Practice Guide (GPG 45) as a methodology for verifying 'good' digital identities. There are also likely to be future changes to the Regulations to include the original 5AMLD text referenced above. As new legislation will be required to enable the DIATF, it will take some time to be operational, but the certification process has commenced for Digital ID providers .

Bank Assured ID (BAI) uses key data and information held by the banks, shared through Open Banking rails with customer consent, which has already been verified and AML checked. This project looks at the feasibility of financial services firms using bank-verified data for their own KYC purposes, and whether additional data could be provided. If feasible, this could potentially provide one solution for driving forward the Digital ID revolution in a fully AML compliant way without having to wait for Government and regulatory developments. This is in no way downplaying the excellent work by Government and other stakeholders to date. It's purely a timing issue.

Richard Bostock, Senior Policy Manager, FLA

As sponsors of this project, we would particularly like to thank Ewan Willars from Upstream Insight (the author and key researcher) and Rob Laurence from Torwood Consulting, and BMW Financial Services, JCB Finance, NewDay and United Trust Bank, all of whom provided invaluable input into these research findings.

Keith Mabbitt, Chief Customer Officer, OneID

EXECUTIVE SUMMARY

In recent times, as more of us choose to bank online via our phones and apps and to transact online, and particularly since the pandemic, customers expect to be able to open new products and services through digital channels.

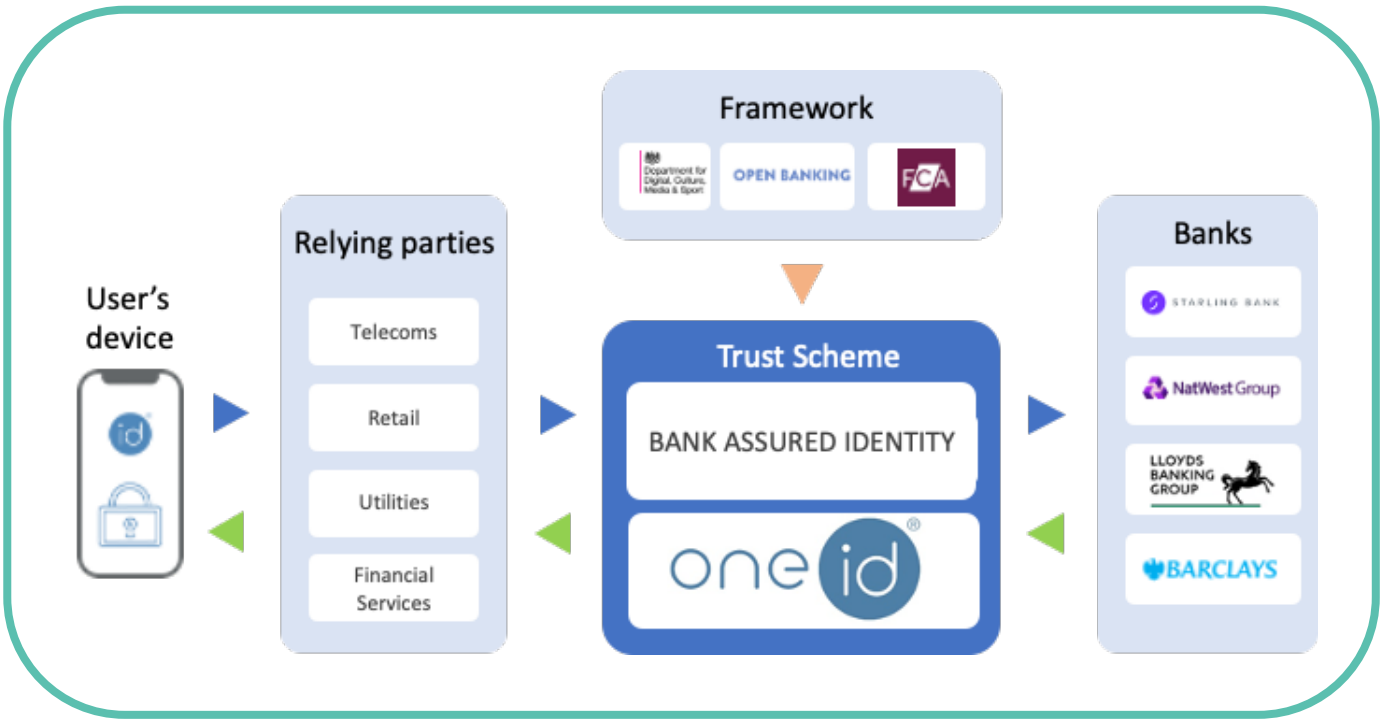
But increasing online identity fraud and a complex regulatory environment have presented both challenges and opportunities for financial service firms seeking to offer simpler and more secure customer onboarding.

THE IDENTITY CHALLENGE

The most recent revisions to the Money Laundering Regulations did include changes aimed at enabling electronic or digital identity to be used more widely for Customer Due Diligence (CDD). Despite those changes, uptake of digital identity by regulated industries such as the finance and leasing sector has been limited, and the development of the Government's own Digital Identity Trust Framework has been slow, while industry may need a more immediate solution. Not only to improve regulated CDD, but also to improve customer experience, increase efficiency and to reduce fraud. Step forward Bank Assured Identity.

WHAT IS BANK ASSURED IDENTITY?

Bank Assured Identity (BAI) is a new identity model. It enables customers to consent to share verified identity information banks hold about them with third parties. It uses the Open Banking infrastructure and internet banking authentication methods to allow a quick, secure and customer friendly exchange of customer information from a bank to a relying party, via the BAI service provider, on a transaction-by-transaction basis.



To begin to test the potential value of BAI, the project team and OneID held a series of workshops (hosted by the FLA), structured interviews, and a survey with four members of the FLA: BMW Financial Services, JCB Finance, NewDay and United Trust Bank.

The research enabled the project team to assess the market fit – identifying the core and potential extensions to the information that could be shared by banks and their customers under the model, against the data that these organisations collect when onboarding their customers. The products in scope included a range of both B2B and B2C onboarding journeys.

WHAT WE FOUND

The research uncovered a range of primary and secondary use cases that Bank Assured Identity could provide. The primary use cases were universal, and applicable to all the participating firms, while a number of secondary use cases were more valuable to some firms based on their business model and products.

PRIMARY USE CASES
- **Providing identity data and removing friction**
- **Anti-impersonation checks**
- **Setting up verified repeat payments**
- **Authenticating customers accessing an account**

SECONDARY USE CASES
- **Setting up customer accounts**
- **Proving identity evidence**
- **Verifying source of income**

It is possible that each of the primary use cases could provide sufficient value as standalone options. The ability to gather verified identity information in a relatively friction-free way both improves the customer experience and removes a first-party fraud vector. This use case has wide coverage, with the core identity data in principle able to be provided by all banks.

Other fraud-reducing use cases came to the fore during the research, particularly as an option to provide an anti-impersonation check in line with Strong Customer Authentication protocols, and to set up repeat payments such as direct debits without fear of fraud or inaccuracy.

The true value of Bank Assured Identity model overall may lie in the wide range of benefits and the value that can flow from an ensemble product – using the single process to both gather customer data, improving the journey for customers and reducing friction, while being leveraged to provide additional services and value at the same time.

Additional use cases that may open up over time were also recorded, such as providing a full end-to-end KYC solution for individuals and extending the model to cover business data. There are additional factors required to unlock the full potential of Bank Assured Identity, centred on aligning to standards and extending the data able to be shared.

It was clear from the research that there is significant potential value to be unlocked by Bank Assured Identity for the finance and leasing sector. The next steps will be to test the model in practice, enabling the full value of the BAI model to be assessed.

INTRODUCTION

A major focus for the financial services industry in recent years has been the potential to make use of digital identity solutions to strengthen fraud protection and improve customer experience. There have been several iterations of digital identity in the last decade, and more recently the Government has been developing its own Digital Identity Trust Framework, with certifications for services such as Right to Rent, Right to Work and DBS checks underway. However, the use of digital identity by FLA members has to date been limited.

As the UK identity market continues to emerge, financial services firms are interested in understanding how Bank Assured Identity and other identity architectures might work to the benefit of their customers.

HOW DIGITAL IDENTITY MIGHT HELP

There are many issues that digital identity can help to address:

- In recent years, and particularly since the start of the pandemic, all firms and their customers have had to rely more upon digital sales and onboarding. Even in the motor industry, sales processes have shifted away from face-to-face contact. Ensuring that customers can be identified and verified in line with AML rules remotely and digitally is not easy, and assured digital identity is one possible solution.

- Customers must supply a range of data about themselves via whatever sales journey they are on, whether face-to-face or remotely. This can cause:
    - unnecessary friction and a negative impact on the customer experience,
    - abandonment of the sale,
    - data entry mistakes, which can subsequently cause poor matching rates against bureau data, and require manual intervention by the credit provider to ensure data is accurate,
    - it is a potential first-party fraud vector allowing bad actors to claim fraudulent identities.

Digital identity has the potential to provide customer data in a more accurate, customer friendly and pre-verified way.

LEVERAGING BANK ASSURED IDENTITY

There are significant advantages to sharing the customer data already held and checked by banks. For example, matching rates against third party registers and credit bureau records could be improved by ensuring better alignment of identity data held across the financial system. Repeat payments can be set up (and if necessary re-established) in a purely digital and automated way using accurate bank account details known to belong to the customer in question.

By leveraging Strong Customer Authentication (SCA) checks carried out by banks to authenticate customers as part of the data transfer process, other issues may be addressed:

- negating the need for password management by the credit provider, allowing secure access to customer accounts or portals,
- enabling anti-impersonation checks to be carried out prior to credit being provided.

OBJECTIVES

To test these assumptions, the research was designed to meet the following objectives:

- Clarify specific use cases for which Bank Assured Identity could potentially address challenges experienced by relying parties and their customers:
  - customer frustration due to unnecessary friction, data entry requirements or lengthy onboarding processes,
  - inefficiency, such as requiring manual intervention, extensive customer data verification or delays in processing transactions,
  - inaccurate customer information and data quality issues,
  - customer abandonment and failure to complete online processes,
  - challenges in creating, or enabling access to online customer accounts,
  - difficulties concerning the requirement to undertake liveness / anti-impersonation checks.

- Assess the requirements of different relying parties for specific use cases, including the data required, the level of assurance (for example due to AML obligations), and the technical method of delivering the information.

- Identify what additional data/attributes might be required that could be delivered through the Open Banking infrastructure or from an attribute provider.

- Recommend specific and actionable steps that could help to integrate the new model into the work of FLA members and ensure the greatest value for customers and relying parties.

METHOD

A research programme was designed to gather primary evidence from AML experts working within four organisations, each specialising in a different area of finance and leasing. These were BMW Financial Services, JCB Finance, NewDay and United Trust Bank.

The questions the firms were keen to explore in this research included:

- How would BAI integrate with existing consumer journeys?
- What are the potential use cases?
- Are there benefits to leveraging the authentication model used by banks, and utilised by the BAI model?
- Would it be a 'waterfall' solution and add another option for consumers, or could it replace some existing processes entirely?

The project team undertook a series of structured interviews with the participants, as well as conducting a detailed survey to capture information concerning the products, the key features of the customer journeys, and most importantly, the range of information collected during the onboarding process. This included data about the customer, how that information is gathered, and what checks are undertaken to ensure the information is valid and verified.

PROJECT SCOPE

The project aimed to examine a mix of eight use cases, involving both B2B and B2C products, with both sole traders and limited companies included in the scope.

Commercial considerations and assessing economic value were out of scope of the project, to retain competitive neutrality and ensure compliance with anti-trust rules.

PROJECT GOVERNANCE

To protect the identity of the providers of information gathered during the research, the project team ensure that the information was anonymised and aggregated before being shared amongst the participants, and for the final project report.

To ensure good project governance, a special purpose Working Group was convened, involving the four participating firms, the project team, and a BAI provider OneID.

The Working Group operated under specific terms of reference, and ensured the project was delivered in an appropriate and independent manner throughout the research, the review of the findings, and the creation of the project report. The project was funded by OneID.

The research and analysis were undertaken by an independent project team, consisting of Ewan Willars from Upstream Insight and Rob Laurence from Torwood Consulting.

INTRODUCING BANK ASSURED IDENTITY

Bank Assured Identity is a new way to transfer information held about a customer by their bank, digitally and securely, to a relying party with which the customer is transacting.

The model is built on the foundations provided by Open Banking. The Open Banking ecosystem was developed by UK banks in response to an order by the Competition and Markets Authority. It is a system regulated by the Financial Conduct Authority (FCA) which enables customers to consent to two separate services. To facilitate these services, third party providers connect to UK banks using agreed 'Application Programming Interfaces' (APIs), an established and relatively simple way to transfer predetermined information between organisations.

There are two regulated service types. Account Information Service Providers (AISPs) provide services based on the sharing of information concerning a customer's banking transactions – such as financial management tools, and affordability checking processes.

Payment Initiation Service Providers (PISPs) provide services based on payments made from bank accounts held by the customer, avoiding the need for cards to be used and avoiding charges relating to payments such as interchange fees. This enables services such as digital wallets.

A NEW FORM OF DIGITAL IDENTITY BASED ON OPEN BANKING

While the exchange of identity information is not part of the scope of the CMA's order, the same infrastructure, processes, and user guidelines have now been harnessed to allow the transfer of information held by a bank about a customer's identity via a Commercial API. This includes information such as their forename and surname, date of birth and address. This is data that the bank has collected from the customer, has previously validated and verified, and kept up to date. The information is also provided only once the customer has provided consent and been authenticated by the bank's processes in line with Strong Customer Authentication.

Over time, the range of data able to be transferred under this model might be expanded, to include other data commonly held by a customer's bank, and even to include information held by banks about companies.

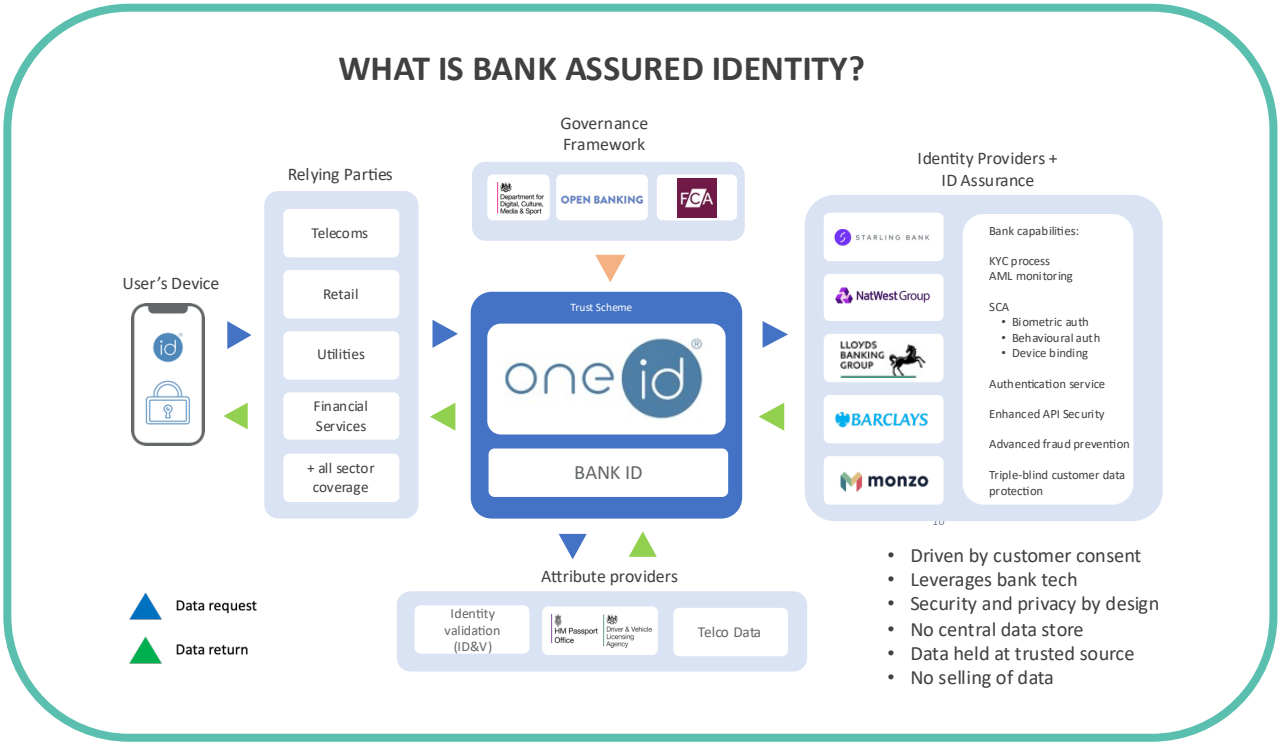
The customer providing their explicit consent to the bank to share their identity information is a key component of the journey. The customer remains in control of exactly what information is shared as part of each transaction.

The BAI service provider that orchestrates the exchange of data does not typically persist or in any way store any of the customer's identity information. It is shared in real time, and strictly on a transaction-by-transaction basis. This limits any exposure the customer or the other parties involved may have to risks of data being compromised, and other security and privacy concerns.

THE BANK ASSURED IDENTITY ARCHITECTURE

The model uses the same infrastructure and processes that underpin the Open Banking ecosystem, and therefore reflects a very similar flow of data. Banks act as the source of identity data, the Bank Assured Identity provider sits in the centre to orchestrate the transfer of information via API, and the relying party is the recipient of the customer's identity data.

The model also allows for information to be gathered simultaneously from other sources. These can include government databases, other organisations with whom the customer has a relationship, credit bureaus or other trusted sources.



The identity information can be combined with other Open Banking services from an appropriately licensed provider, whether the BAI provider themselves or a third party. This could allow an affordability or source of funds check via an AISP, or to make a one-off payment via a PISP.

The authentication check that forms part of the process could be leveraged as a separate service. This authenticates the customer using the combination of their smart device's capabilities, and the checks banks have created to enable access to the customer's banking app or online account.

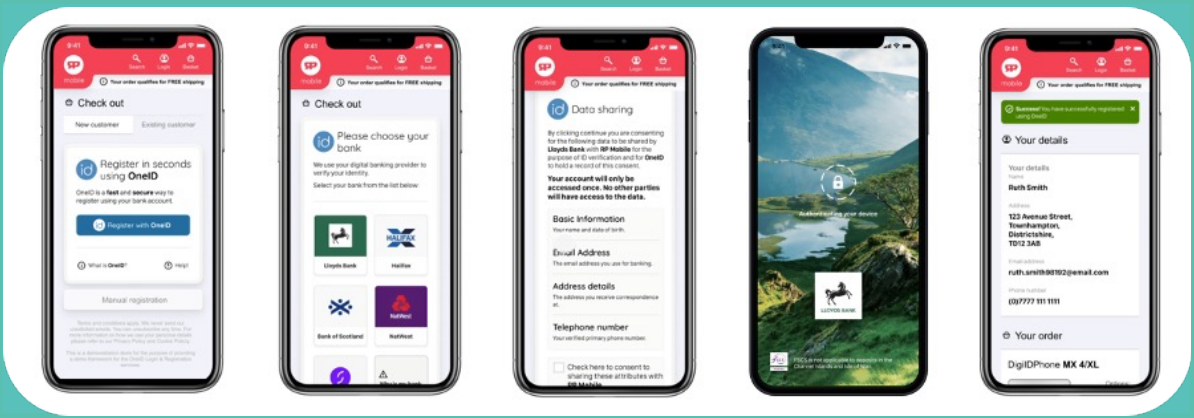
A Strong Customer Authentication compliant authentication check utilising existing infrastructure could provide a range of practical and valuable use cases.

Potential use cases are explored in detail later in this report.

USER EXPERIENCE

The Open Banking user journey provides a low friction and quick user experience, with zero form-filling, building in customer control and requiring their consent to share data. The same applies to Bank Assured Identity.

THE BANK ASSURED IDENTITY CUSTOMER JOURNEY



1. The customer, while making a transaction that requires them to pass on their identity information, can register with the provider via a BAI service.

2. The customer chooses a bank who they have an account with from a selection.

3. They are then asked to provide their consent for the information they are being asked to transfer.

4. Once their consent is provided, the customer is authenticated by their bank to access their banking app via methods compliant with Strong Customer Authentication. This includes two-factor authentication using their smart device, typically involving a biometric factor such as their facial image or fingerprint.

5. The bank is then able to transfer the required information from their systems using APIs and an open standard format, routed by the BAI provider to the relying party.

Confidence in the BAI scheme is enhanced by the trusted relationship customers have with their bank, and by the extensive regulations and controls that exist around the sharing of personal data and the banking system.

While no bank can claim that all customer data is 100% accurate at any given time, there are requirements for banks to keep customer records up to date, particularly identity data. The regulations require extensive checks by banks as part of their own customer due diligence and AML obligations throughout the relationship with a customer. This helps to ensure that the data shared with relying parties is correct, and likely to match the data held by Credit Bureaus and other trusted third-party sources.

RECORDING TRANSACTIONS

The audit trail available to the regulator on request, or to help to manage a complaint or investigation involving a Bank Assured Identity transaction is an important factor for relying parties to consider, given the rules around reliance set out in the regulations.

Reliance

39 (2) "When a relevant person relies on the third party to apply customer due diligence measures under paragraph (1) … (b) they must enter into arrangements with the third party which … enable the relevant person to obtain from the third party immediately on request copies of any identification and verification data and any other relevant documentation on the identity of the customer, customer's beneficial owner, or any person acting on behalf of the customer;"

Money Laundering Regulations 2019

The BAI service provider stores a limited set of information, which when combined with the more detailed records held by the customer's bank can provide full details of the transaction.

For BAI users, the provider records the customer consent, the bank the customer connected to, the relying party, a customer identifier, what data they shared (an attribute list, not the actual data) and associated timestamps.

The customer's bank holds details of the actual shared data, timestamps, customer confirmation, device data and authentication record. The data privacy model has been designed so that the customer is the only party who sees all of the data.

When combined, these can provide a full description of the customer, the transaction and transfer of data, and ensure compliance with the relevant regulations.

SURVEY FINDINGS

The four participating organisations each completed a survey to identify the information they collect from customers, whether personal or business customers.

Personal customers (B2C), sole traders and significant individuals within businesses (B2C)

ATTRIBUTES COLLECTED / PROCESSES	B2C	B2B (ltd)	B2B (Sole)	B2B	B2B	B2C	B2C	B2C	REQUIRED FROM CUSTOMER	VERIFIED
Account is created	Y	Y	Y	Y	Y	Y	Y	Y	8	8
Position in business (B2B only)		Y	Y	O	Y				3	4
Title	Y	Y	Y	O	Y	Y	Y	Y	7	8
First name	Y	Y	Y	O	Y	Y	Y	Y	7	8
Middle name/s	O	Y	Y	O	Y		Y		4	6
Last name	Y	Y	Y	O	Y	Y	Y	Y	7	8
Other names	O	Y	Y	O			O		2	5
Gender	O	Y	Y	O		Y		Y	4	6
DOB	Y	Y	Y	O	Y	Y	Y	Y	7	8
Address	Y	Y	Y	O		Y	Y	Y	6	7
Address History	Y	Y	Y	O			Y		4	5
Telephone number	Y	Y	Y	O	Y	Y	Y	Y	7	3
Email address	Y	Y	Y	O	Y	Y	Y	Y	7	2
Correspondence address		Y	Y		Y		Y		4	3
Communications preference	Y	Y	Y	Y		Y	Y	Y	7	2
Domicile address		Y	Y		Y				3	2
Nationality		Y	Y		Y		Y		4	2
Dual nationality		Y	Y						2	2
Citizenship in other countries		Y	Y						2	0
Country/city of birth		Y	Y				Y		3	0
Marital status	Y	Y	Y	Y			Y		5	2
Residential status	Y	Y	Y	Y			Y		5	4
Mother's maiden name									0	0
Bank name	Y	Y	Y	Y		O	Y	O	5	5
Bank acc number	Y	Y	Y	Y		O	Y	O	5	5
Bank acc sort code	Y	Y	Y	Y		O	Y	O	5	5
Name on bank account		Y	Y			O	Y	O	3	1
Employment status	Y	Y		Y			Y		4	2
Employer name	Y	Y		Y			Y		4	3
Employer address	Y	Y		Y			Y		4	2
Occupation	Y	Y	Y	Y			Y		5	2
Sector	Y	Y	Y	Y					4	2
Employment start date		Y	Y				Y		3	0
Source of income		Y	Y				Y		3	1
Salary		Y		Y			Y		3	2
Frequency of pay		Y					Y		2	1
Total income		Y							1	0
Tax residency status		y	y						2	0
National Insurance number									0	0
PEP status		y	y		Y	Y	Y	Y	6	4
Sanctions status		y	y		Y	Y	Y	Y	6	4
Anti-impersonation check	Y	Y	Y	Y	Y	Y	Y	Y	8	
Repeat payment set up	Y	Y	Y	Y	Y	Y	Y	Y	8	

KEY	
	Core BAI data
	Potential extensions to BAI data
	AISP data
	Other potential BAI services
Y	Mandatory data from customer
O	Optional data from customer

The survey focused on the data currently collected directly from customers. The information in these tables is anonymised, with each product example identified as being B2B or B2C, and where appropriate dividing between sole trader and limited company customers.

The table on the previous page expresses the data collected about individuals. The table below shows data collected about corporate entities.

Business data collected from limited companies and sole traders

ATTRIBUTES COLLECTED / PROCESSES	B2C	B2B (ltd)	B2B (Sole)	B2B	B2B	B2C	B2C	B2C	REQUIRED	VERIFIED
Business Name		Y	Y	Y	Y				4	4
Trading Name (if different)		Y	Y	Y	Y				4	3
Company Type		Y	Y	Y	Y				4	4
Registered address		Y	Y	Y	Y				4	4
Correspondence address		Y	Y	Y	Y				4	4
Email		Y	Y	Y	O				3	3
Communications preference		Y	Y	Y					3	3
Website address		Y	Y		Y				3	3
Business registration number (Companies House)		Y	Y	Y	Y				4	4
Registered VAT number					Y				1	3
When did the business start trading?		Y	Y		Y				3	4
In which country is the Parent company, headquarters or beneficial owner located?		Y	Y		Y				3	4
Country of tax residency		Y	Y		Y				3	3

THE FINDINGS

Data requirements vs availability

The survey returns show a wide variety of data collected direct from customers, and of verifications and other checks undertaken. The high degree of variance is predominantly due to the variety of product types tested, and participants' own risk appetites, onboarding journeys and technical capabilities.

Some clear patterns are apparent, and they reflect positively on the potential for BAI to provide a solution relevant to the principal data needs of financial services firms.

A similar range of core identity data is required by all the participants, and which is used to comply with regulatory requirements for customer due diligence. This information includes the customer's name, date of birth and address. Along with the customer's contact details,

and the customer's bank and account details, this is mirrored by the core information provided by Bank Assured Identity.

Other personal data is typically sought from customers on a less consistent basis, varying more significantly between different firms and products. This wider spread of data may be used by relying parties to manage risk, or to better service the individual, and is not currently part of the core offering of the BAI model.

However, there is no reason in principle why the data couldn't be shared by banks in the same manner as the core identity attributes *if* the bank holds it within their systems.

Verification checks
The data that is then checked against trusted third-party registries varies between different participants, as well as the method used. The methods include checking with commercial registries, credit bureaus, and organisations such as CIFAS and others.

Although the data provided by the BAI model has been checked by banks at the time it is gathered, and kept up to date in line with regulation, none of the participants felt that this would negate the need to carry out additional verification. This is likely to continue to be the case until BAI providers become certified under the DCMS Trust Framework and are formally recognised by regulators or in JMLSG guidance.

Other processes
There are additional processes undertaken by the participants that have the potential to be augmented or replaced by BAI, based on the attributes provided by BAI, or the authentication checks undertaken as part of the process:

- **Anti-impersonation checks** are carried out to authenticate the customer and ensure that credit is only provided to the correct customer, to prevent fraud and ensure compliance with the regulations and JMLSG Guidance Notes. Participants currently utilise one or more of a variety of methods including knowledge-based authentication. The Strong Customer Authentication check carried out by banks as part of BAI could fulfil the same goal. Under the wording of JMLSG Guidance Note 5.3.90 (bullet 5) a an SCA check would be considered compliant, as it relies on authentication factors already verified by the customer's bank.

- The creation of **repeat payment instructions** in a digital and automated manner, based on bank account information that has been demonstrated to belong to the customer in question via the authentication process.

- The participants vary in terms of the **identity evidence** they require from customers, dependent on the product type and inherent risk, the extent of the customer's credit file and the accuracy of matching of their details against trusted third-party registries, such as information held by Credit Bureaus. For credit products involving thin-filed customers or in a near-prime category, or those working in certain industries, collecting standard identity evidence can be an issue. Bank Assured Identity may be able to help by providing an alternative source of identity evidence.

- **Setting up a customer account or portal** is something that all the participating organisations do at some stage of their onboarding journey. The information provided by BAI is, in principle, sufficient to set up an account. The authentication check encompassed by the BAI process could be used to enable SCA-compliant access to the customer's account on an ongoing basis. This would be without the provider persisting password data or needing to re-establish customer access if a password is forgotten or compromised. If the customer's contact details have changed, BAI could also provide a means to keep the information updated based on the bank's records.

- The fact that BAI runs on the infrastructure created for Open Banking means that the BAI service can be **combined with an AISP or PISP service**. These could include identifying source of funds, assessing affordability, or making a payment (such as a settlement payment to pay off a loan or mortgage).

Business data

The data collected during B2B use cases varied significantly from that asked of personal customers. Data is collected across two categories - firstly concerning the significant individual or individuals from within the organisation, and secondly data concerning the business itself.

A further difference was regarding sole traders – in some instances they are treated as personal customers, with a very similar data requirement. In other cases, it was a hybrid approach, with more details collected about the individual than for representatives of limited companies. Data is also collected about the business where available from Companies House.

At present the Bank Assured Identity model is focused on the sharing of personal customers' details held by their bank, however the Open Banking implementation also applies to SMEs. There is no reason in principle why a wider range of data that a bank holds about its business customers might also be shared. Such attributes go significantly beyond what is required to be shared under regulation for Open Banking's current implementation, or by the Second Payment Services Directive (PSD2) which has similar requirements.

BANK ASSURED IDENTITY MARKET FIT

The alignment between the core BAI identity attributes and bank account information provided therefore matches well with the standard identity data required to be collected about individuals for credit products. This demonstrates the potential for a range of immediate use cases to be derived from this dataset, regardless of whether it can be extended to cover additional customer attributes, or business data in future.

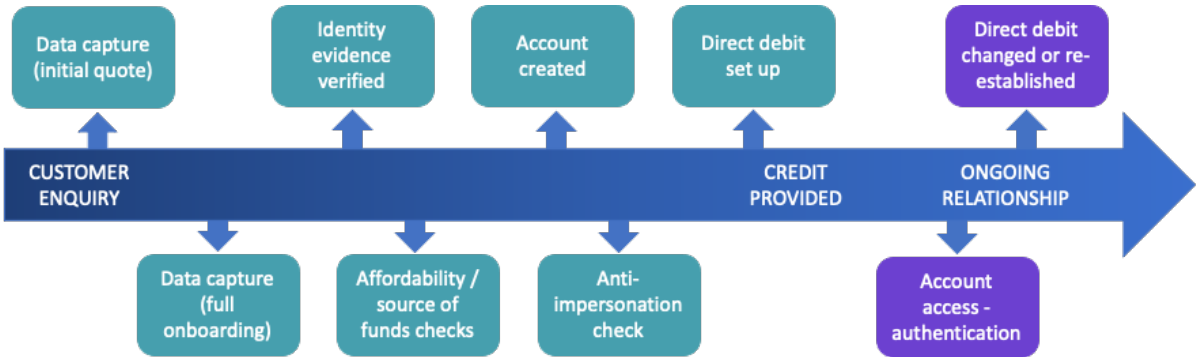
The inclusion of a Strong Customer Authentication-compliant check and the option to build in additional Open Banking services has the potential to further widen the use cases, explored in the following section.

The assessment, based on this research, is that Bank Assured Identity has significant potential value for the finance and leasing sector.

MAPPING AGAINST USER JOURNEYS

From amongst the organisations that took part in the research there were a range of customer journeys identified. These ranged from one-stage online onboarding to face-to-face initial meetings with either sales representatives, franchisees or nominated brokers before 'full' onboarding by the firm.

Despite the differences, a series of generic steps and processes were identified, and the potential for Bank Assured Identity to be used at each step was assessed.



How to value and assess the business case for BAI at each stage is considered on page 23.

It was clear that BAI has potential use cases at every stage of a customer's onboarding journey. These range from the initial data collection and identification of the customer, to affordability checks and the setting up of a customer account and repeat payments, identifying that they are the customer in question before credit is extended, and then to enable ongoing secure access to their account.

However, there were some potential issues raised that may require further thought, although none appear to be insurmountable.

BAI is designed to share a customer's attribute data, under consent, from the customer's bank, via the BAI service provider to a (single) relying party. This becomes more complex where there is an intermediary that is responsible for collecting customer data on behalf of the organisation at the outset, such as a broker or franchise/sales team.

For organisations with near-prime products, to ensure good value it may also be beneficial to only carry out certain processes such as anti-impersonation checks once the customer's suitability and affordability have already been established.

For each product and each potential BAI user firm, the exact pattern and value of deployment will differ based on their business and product range.

USE CASES

When undertaking the interviews and exploring the survey data provided by participants, a series of potential use cases emerged.

They varied in terms of their potential coverage and value across the participants. It has been possible, based on these two variables, to identify a number of use case categories:

- **Primary use cases** – of interest and applicable to products across all participants, and without further adaptation of the BAI model.
- **Secondary use cases** – of greater interest to the majority or a sub-set of participants, and where the overall value of the use cases may be more limited.
- **Future use cases** – the use cases that are not possible under the current BAI model, or where additional regulatory clarity may be required.

PRIMARY USE CASES

Providing assured identity data: This could include core identity data such as name, date of birth and address as well as bank account information, and communications information relating to personal customers. Information could also relate to sole traders and significant individuals within a corporate entity.

It would prevent the need for customers to provide data and evidence, reducing friction for customers, and removing a first-party fraud vector. It would ensure data is more accurate, and better able to be matched to third-party registries such as credit bureaus.

The implication for the flow of data within an intermediated customer onboarding journey is one area that needs further consideration, particularly for independent brokers.

Anti-impersonation checks: All the participants carry out one or more methods of checking the applicant via an anti-impersonation check prior to the credit being provided.

The BAI method with its intrinsic use of a SCA-compliant two-factor customer authentication (one of which is typically based on a biometric factor) could potentially replace or enhance existing methods. Participants considered that BAI may be a candidate to possibly replace existing methods in some cases, in others to add to a 'waterfall' of alternatives that could be offered.

Although adherence to the SCA standard helps to assess the level of assurance this method provides, and the need for anti-impersonation and liveness checks are based on the assessed level of risk, clearer guidance from the JMLSG would assist firms in deciding to use this as a standalone process.

Setting up direct debits and other repeat payments: Direct debits and other repeat payment methods could be set up using the authenticated bank account and identity information provided by BAI. This would ensure accuracy and eliminate a potential fraud vector. It could

be undertaken in an automated and fully digital way, with the potential to use digital signature techniques alongside BAI.

All participants use direct debits, and a proportion of direct debits require some degree of checking or amending for accuracy during the set-up process. Re-establishing direct debit mandates that have been cancelled by the customer or based on closed accounts are also able to be serviced by BAI, negating the need for costly and inefficient manual intervention.

Using BAI authentication to provide access to customer accounts or portals: All of the participants create a customer account and provide a portal of some sort to enable the customer to gain access to documents or to engage them over the course of the relationship. As most of the products provided by FLA members typically require limited customer interaction post-onboarding, customers frequently forget account passwords. These then require updating, and the credit provider must store and maintain records of passwords which in turn increases their risk.

This is a use case that few had considered prior to the interviews, but most of the firms were interested in the potential that replacing customer passwords using BAI authentication could have. This would replace their need to maintain passwords. It would in all cases match (and in many cases strengthen) the existing authentication methods.

SECONDARY USE CASES

Setting up customer accounts: All participants open customer accounts based on the data they receive direct from the customer as part of their customer due diligence. The data required to set up the account is also included amongst the core BAI dataset exchanged with relying parties. The method could therefore provide an efficient, accurate and automated way to establish customer accounts without requiring additional input direct from customers. It would also enable customer contact details to be kept up to date, reducing account management costs for firms.

Providing identity evidence: The participants in the project varied significantly in how they identify customers, the evidence they seek, and the checks they then carry out. All firms are compliant with the regulations in this regard, and in line with existing JMLSG Guidance.

In some cases, customers may have problems due to a lack of primary evidence types (for example a passport or driving licence). BAI could provide an additional or alternative means to identify hard-to-verify customers or those without standard forms of identity evidence. It is unlikely that firms would rely on BAI as a sole form of evidence, and particularly without regulatory recognition of the method. But used as a secondary form of evidence, it could reduce the need for physical visits to customers and help to onboard thin-file individuals.

Combining Open Banking AISP to verify income: Verifying a customer's income can be an inefficient process when evidence is gathered from the customer – this can include sending or scanning PDF copies of bank accounts, payslips and tax forms. The same verification could be carried out using an AISP service to immediately assess the frequency and value of income into a customer's account and the source of the income at the start of an onboarding.

FUTURE USE CASES

Future use cases are those for which, at least at present, insufficient data is available through BAI, or the lack of regulatory recognition or clarity would make its use challenging.

Using BAI as a standalone KYC solution: While BAI can legitimately be used as a source of secondary identity evidence and can provide a range of identity attributes, the data provided would still need to undergo checks to verify it against trusted third-party sources by all relying parties. There is neither sufficient regulatory or standards-based clarity or recognition by the relevant authorities – in this case the FCA – to allow its use without additional checks.

Given the potential to expand the information provided via APIs to other data held by banks, and to augment this with information from other sources, the data package could encompass the full requirements for financial services firms to onboard a customer from start to finish.

If the level of assurance provided by the method could also be established and recognised, for example by the FCA or within the Government's Trust Framework, the model could provide a standalone solution for the data it provides. This would provide significant value for relying parties by removing the need for additional verifications. OneID is working with industry, Government and regulators towards this goal.

BAI for businesses: The information required to be collected from businesses provides an obvious extension to the current model. This may be particularly true for sole traders and SMEs, who may have fewer records available from Companies House, and for whom any efficiencies in the process of gaining access to credit might have comparatively greater value.

There is no reason in principle that BAI for businesses could not become a valuable use case if the model is extended to encompass the sharing of company information by banks.

ALIGNING TO STANDARDS

There are other countries that have implemented similar systems of digital identity based on the sharing of information banks hold about their customers. Perhaps the most well-known of these being the BankID examples developed in Nordic counties in the early 2000s, and now used ubiquitously in these countries for a wide range of use cases.

Such schemes differ in terms of their architecture, the persistence of the identity, or the extent to which they are centralised or federated. However, one common factor they have, and which has increased the range of use cases and provided confidence to both consumers and relying parties alike, is their recognition in regulation, and that there are standards to which they align.

While many of the use cases explored in the previous section do not explicitly require alignment to standards or recognition by the FCA or JMLSG Guidance, standards are likely to be fundamental to unlocking the full value of digital identity in the UK in general, and for BAI specifically.

BAI is being developed to align with the Government's Trust Framework and the existing Digital Identity Good Practice Guides (GPGs). Certification against the DCMS requirements will expand the regulated use cases BAI can service. It will build market confidence and allow formal reliance on BAI as a stand-alone process.

STRONG CUSTOMER AUTHENTICATION

One standard of the authentication process that the BAI model already aligns with is the Strong Customer Authentication standard set out in PSD2. The SCA method used by banks to authenticate their customers, based on two-factor authentication and a biometric option in many cases, is a strong and secure method. This should build confidence for the relying parties and widen the use cases that might flow from its application. These include anti-impersonation checks, allowing customers to access their accounts, or assuring that the customer is the rightful owner of the identity or bank account information being shared.

GPG45

Good Practice Guide (GPG) 45 is as close to a digital identity standard that exists in the UK regulatory framework at present. It also forms a core part of the Government's Trust Framework. BAI can be assessed against GPG45 scoring and levels of assurance for customers whose bank accounts have been created using standard onboarding practices and maintained in line with the UK Money Laundering Regulations.

The alignment of BAI with GPG45 is being progressed via the DCMS certification process. The current assessment is that the model would align to at least a Medium Level of Assurance.

There is also the potential opportunity for banks or the BAI service provider to 'step up' the level of assurance the model provides, for example by undertaking additional verifications.

Adding a fraud check, for example via a CIFAS API call, and bank account activity history should enable a High Level of Assurance to be achieved.

JMLSG GUIDANCE NOTES

The Joint Money Laundering Steering Group Guidance Notes are the definitive guide to compliance with Money Laundering Regulations for the UK Financial Services industry, including FLA members.

The Guidance Notes are kept in line with changing regulations as they are amended over time, and often provide specific examples of generic types of processes or methods that can be compliant with given elements of the regulations. This is important, as many requirements placed on financial service organisations are risk-based, rather than purely standards-based. Methods and processes that are given as examples in JMLSG Guidance are more likely to be considered compliant, and adherence to the guidance carries weight in any future assessment of an organisation's compliance.

It is therefore a significant factor for financial services firms when considering the composition of their due diligence processes.

A number of the participants felt that JMLSG Guidance is (in parts) outdated and needs to be updated to reflect current but relatively new methods and technologies. The use of digital identity in general is an example, and this certainly extends to BAI.

A salient example is the guidance given around anti-impersonation checks. These are covered in JMLSG Guidance Notes Part 1, paragraphs 5.3.85 to 5.3.91.

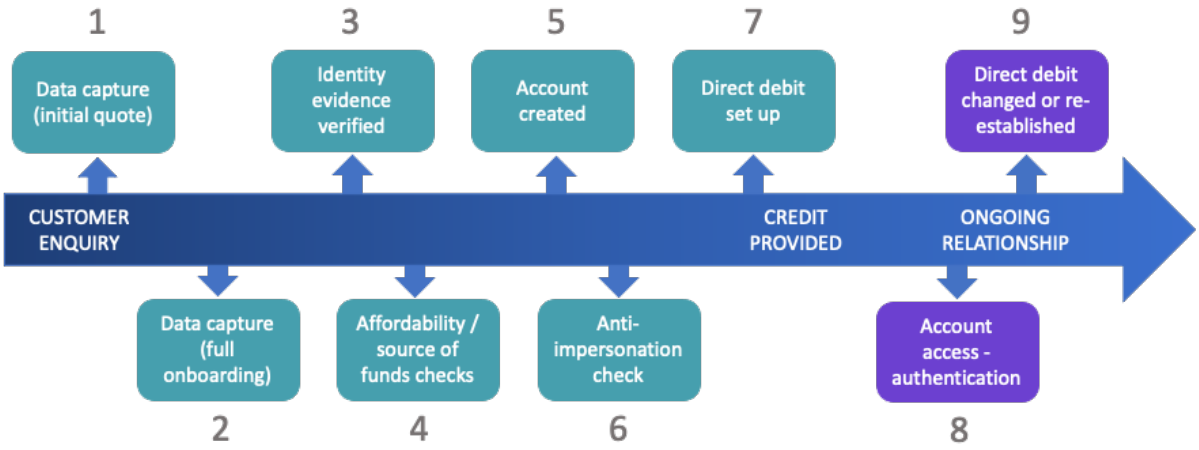
The guidance sets out the need to carry out additional verification steps when a customer is onboarded remotely and digitally. The examples given in the guidance include:

- the use of biometric data,
- using knowledge-based authentication based on PINs or secret codes,
- requiring first payments to be made from a UK-based bank account,
- verifying additional aspects of a customer's identity,
- contacting the customer on a previously verified channel such as a landline.

There is nothing in the guidance that precludes the use of new methods, or specifically BAI. However, relying parties in financial services are likely to have greater confidence if it is more explicitly included in the examples given in the JMLSG Guidance.

ASSESSING THE VALUE

Assessing the value of digital identity has often proved problematic for potential adopters. This may be due to some of the factors being somewhat intangible (the benefits of better customer experience, for example) while other factors are more straightforward, such as the degree of fraud that might be prevented.



The true value will be particular to each firm in question. What considerations might a firm have in trying to assess the value of Bank Assured Identity at each stage of their journey – whether in terms of financial value, time savings, or improved customer experience?

USE CASE	VALUE FACTORS TO CONSIDER
1	Can reducing customer friction reduce abandonment rates?
2	Will pre-verified data allow a firm to reduce the checks they undertake? Can firms quantify the costs associated with correcting data inaccuracy, or the potential first-party fraud costs that might be avoided?
3	What are the costs of identifying customers without standard ID evidence?
4	How manual or inefficient are current affordability checks? What are the costs of capturing evidence of the customer's source of income?
5	Are there potential savings by automating the creation of customer accounts?
6	Would using a bank's Strong Customer Authentication as an anti-impersonation check reduce fraud? Would this be a 'waterfall' option or replace a more costly current method of checking the customer?
7	Are there savings to be made by reducing fraud or errors in the setting up of repeat payments, or by fully digitising the process?
8	What costs are associated with running authentication systems to allow customers access to their account? Would leveraging banks' authentication methods reduce risk of data being compromised, or GDPR compliance costs?
9	When direct debits need to be re-established or changed, is this a current fraud vector? Could there be value in automating the process?

THE VALUE OF BAI TO BANKS

This report has primarily focused on the value that Bank Assured Identity could have for FLA members as relying parties, and for their customers.

Banks are a critical part of the BAI model, as providers of the customers' data, and in generating confidence in the data being shared. It is therefore vital to consider the value that BAI may have for banks, and why they would want to participate in delivering identity information on behalf of their customers.

The first point to note is that the UK lags behind many other countries in developing a bank-led identity solution. For example, banks are providers of identity information in all the highly successful and universally used identity schemes that form part of daily life in the Nordic countries. In the US too, a very similar scheme to the Bank Assured Identity model explored in this report has recently been launched by a range of major US-based banks.

By providing bank assured identity, banks can directly and indirectly benefit in many ways:

- Increasing the services available for their customers using existing data and infrastructure, helping to avoid disintermediation, and providing additional relevance to consumers.
- Fulfilling an important social and economic role.
- Helping banks to off-set the rapidly rising costs associated with keeping customers' data secure and up to date, through the value generated by BAI transactions under a revenue sharing model.
- Helping their customers to retain control of their identity data, and to utilise it in a safe, trusted, and user-friendly way.
- Strengthening the UK's defence against fraudsters, money launderers and terrorists, protecting individuals and helping to reduce data touch points.
- Specifically help to tackle the growing issue of Authorised Push Payment (APP) scams.

MAXIMISING THE VALUE OF BAI

Extending the BAI model to add further value for relying parties and customers rests on three factors: extending the data available, providing greater regulatory clarity or recognition, and building confidence in the approach.

Extending the personal attributes shared

The data is currently focused on the core identity attributes for personal customers. Banks collect a far wider range of personal data. Extending BAI to cover more of this range of data would be an obvious and potentially valuable step.

Extending to business accounts

In addition to extending the range of personal data shared, banks also hold verified data concerning their business account holders. The research has demonstrated a significant potential demand to receive these attributes via the BAI model. Banks should consider the potential to extend data to include business accounts, and the value this would provide to their customers, their relying parties, and the banks themselves.

Augment with additional data sources

The core and potentially extensible data provided by BAI has significant value to financial services firms. This could be further enhanced by pulling in data from additional trusted sources, such as credit bureaus, CIFAS, government registries, the Passport Office, and other Open Data sources.

Mapping to standards

Alignment to standards, certification of that fact, and recognition of techniques in industry guidance can unlock regulated use cases and provide greater confidence for relying parties. The research has demonstrated the significant and immediate value that BAI may have for relying parties, but alignment to standards could expand the use cases, and the value to relying parties (and therefore customers).

Applying OIDC attribute metadata

OpenID Connect (OIDC) has defined a range of standardised 'claims' – customer attributes such as name, date of birth and address. New protocols are in development that would extend this framework to include information regarding the provenance and verification of the claims being shared (e.g. what, how and when a check was undertaken, according to what rules, and using what evidence).

Applying the metadata to information shared via BAI was identified in the group discussions as potentially providing significant value to relying parties.

Relying parties as assured identity providers

There is a growing discourse to extend the principals of Open Banking data sharing to other regulated sectors – what is described as 'Open Data'. In addition, financial service firms have long been involved in agreements concerning the reciprocity of data sharing, such as their arrangements with credit bureaus.

There may be an exciting opportunity to extend the range of information provided by BAI to include data from organisations other than financial service providers. This might include other organisations with a wide customer base, and operating within other highly regulated sectors, such as telecoms.

Reciprocal sharing of identity data

It may be possible to explore how customers, when presented with the information shared by their bank under the BAI model, might have a chance to check the accuracy of the data being shared. If it requires updating, there may be a valuable opportunity to introduce a feedback mechanism to help the bank to update incorrect customer data. This would also help to ensure that relying parties receive only the most up-to-date information.

CONCLUSIONS

Bank Assured Identity has significant unlocked potential for the finance and leasing sector.

The research findings demonstrated that there is significant potential value to be extracted from the Bank Assured Identity model. This is true for any firms operating in regulated sectors requiring customer due diligence and anti-money laundering and fraud checks to be made.

There are a number of factors that could widen the use cases and maximise value, and these are reflected in the recommendations on the following page. The model also has significant valuable in the immediate term.

Uniquely for a digital identity solution, the focus is much broader than simply verifying the identity of the consumer or providing their identity attributes. The Bank Assured Identity model also benefits from its leveraging of two other well-developed and highly regulated processes – the open banking infrastructure, and banks' own Strong Customer Authentication methods.

PRIMARY USE CASES
- **Gathering identity data and removing friction**
- **Anti-impersonation checks**
- **Setting up verified repeat payments**
- **Authenticating customers accessing an account**

SECONDARY USE CASES
- **Setting up customer accounts**
- **Proving identity evidence**
- **Verifying source of income**

As a result, Bank Assured Identity has a wide range of linked use cases. Any one of the primary use cases might have sufficient value alone. But when considered along with other linked and (potentially simultaneous) use cases, the value equation is significantly enhanced.

Tangible value such as the ability to reduce fraud risk, to automate otherwise manual processes and to reduce data inaccuracy is combined with the benefits of reducing onboarding friction, improving the customer experience, and cutting abandonment rates.

Further research is certainly required in practice – the theoretical use cases and value assumptions need to be tested, and ultimately the full value will only truly be understood on a firm-by firm basis. There is also a need to engage, firstly with the banks that lie at the other end of the process, to encourage them to widen the data they might provide, and to include business data, for which there are evident use cases. Also, to engage with the JMLSG and regulators to build awareness and confidence in the model.

The research has clearly demonstrated that the Bank Assured Identity model has a variety of benefits to financial services firms. It aligns with a wide range of pertinent use cases that can be addressed now, and that could be further enhanced in the future.

RECOMMENDATIONS

RECOMMENDATION 1: FIRMS TO ASSESS THE FULL VALUE OF BANK ASSURED IDENTITY
Each of the participants identified overlapping use cases, each of which could augment or improve their own existing processes. Each use case has a value – explained in principle on **page 23.** It will be for each organisation to determine the value of BAI, based on their own level of fraud, their focus on customer experience, and their existing processes.

RECOMMENDATION 2: TEST IN PRACTICE
The primary research carried out for this report has uncovered a series of potentially valuable use cases, as well as ways to extend the BAI model to add further value. Testing of the BAI model by financial services firms in practice will provide the technical and commercial evidence required. Trust scheme providers should also explore the potential to utilise the FCA Regulatory Sandbox to undergo live testing.

RECOMMENDATION 3: SURVEY FINANCIAL SERVICES FIRMS
The participants involved in the research were open and honest in providing insights into the attributes they collect from customers, their onboarding journeys and existing pain points. This reflects only a small sample, and a wider gathering of evidence would provide additional insight. This evidence could help to persuade banks to extend the BAI model to additional data categories and explore the widest possible range of use cases.

RECOMMENDATION 4: EXTEND THE DATA SHARED BY BANKS
For bank assured identity providers and their stakeholders to engage with banks to raise the possibility of extending the model to capture additional data points for personal customers, and the value of extending the model to include the business data they hold.

RECOMMENDATION 5: ALIGN TO STANDARDS
For stakeholders in BAI, including BAI providers and their banking partners, to seek greater clarity on the alignment of the model with existing standards such as GPG44 and GPG45, and the government's trust framework as it develops, and to seek certification against those standards where appropriate.

RECOMMENDATION 6: SEEK REGULATORY RECOGNITION
To seek recognition of the BAI model by the competent authority as a formally recognised means of providing data with appropriate level of assurance.

RECOMMENDATION 7: UPDATE JMLSG GUIDANCE NOTES
Work constructively with the JMLSG, in line with the current regulations, to update the Guidance Notes in a timely manner, to ensure that they reflect the range of techniques and processes available to firms. This should include Bank Assured Identity, and any future developments concerning the development of the Government's Digital Identity Trust Framework and recognition by competent authorities.