connecting the future

Digital Economy Act 2017:
The Identity Verification Services objective

DCMS

February 2023

Response from The Payments Association

Introduction

The Payments Association welcomes the opportunity to contribute to the DCMS online survey on the "Digital Economy Act 2017: The Identity Verification Services objective".

The community's response contained in this paper reflects views expressed by our members and industry experts recommended by them who have been interviewed and who are referenced below. As The Payment Association's membership includes a wide range of companies from across the payments value chain, and diverse viewpoints across all job roles, this response cannot and does not claim to fully represent the views of all members.

We are grateful to the contributors to this response, which has been drafted by Riccardo Tordera, our Head of Policy & Government Relations. We would also like to express our thanks to the DCMS for their continuing openness in these discussions. We hope it advances our collective efforts to ensure that the UK's payments industry continues to be progressive, world-leading and secure, and effective at serving the needs of everyone who pays and gets paid.

With special thanks to:

- Adrian Field, Director of Market Development, OneID
- Aleksander Tsuiman, Head of Regulatory, Veriff
- Andrew Churchill, The Payments Association Ambassador, Project Financial Crime
- Jane Jee, Project Lead, Project Financial Crime
- Peter Ridgway, Digital Industry Adviser, Fujitsu

Tony Craddock
Director General
The Payments Association

Contents

The section numbering below corresponds to the numbering of the 'questions for respondents' in the online form.

1)The first condition for new objectives under section 35 of the Digital Economy Act 2017 is that the data sharing should either:

a) improve or target a public service provided to individuals or households; or
b) provide a benefit (whether financial or otherwise) to individuals or households.

To what extent do you agree that the proposed new objective meets at least one of those parts of the first condition?

Please choose one of the following options:

Agree

Please provide the reason for your response.

We acknowledge that the legislative powers for data sharing as applicable for digital identity are currently being updated under the Economic Crime and Corporate Transparency Bill, the Data Protection and Digital Information Bill, and the Financial Services and Markets Bill.

We appreciate the clear benefit for individuals and households coming from the connection between the individuals' need to prove their identities and transact online, and the availability of data. The benefit is balanced as it should make some aspects simpler, yet it also has the ability to undermine an individual's rights and control.

We believe that the real question is in the direction, control, and extent of data sharing, along with the individual's control of what is shared, when and how.

2) The second condition is that data sharing should improve the well-being of individuals or households.
To what extent do you agree that the proposed new objective meets this second condition?

Please choose one of the following options:

Neither agree nor disagree

Please provide the reason for your response.

Our members observe that the implementation of digital ID measures under consideration could either damage or improve individuals and households.

Whilst the data sharing has the potential to simplify access to services, it also has the negative impact of worry and concern caused by:

1. Ambiguity on how the data will be stored and used
2. What specific information will be shared, and with whom

3. Lack of mention of alternate options for those unable/unwilling to use technology-based services

Nonetheless, individuals and households need to transact online and we welcome the creation of a system that puts trust and inclusivity at its centre where individuals and households are able to access public services as frictionlessly as an increasing number of private services are accessed.

3) The third condition is that the data sharing should support the delivery, administration, monitoring or enforcement of a service provided by a particular public authority (or authorities).
To what extent do you agree that the proposed new objective meets this third condition?

Please choose one of the following options:

Agree

Please provide the reason for your response.

We believe that this condition is fulfilled, as the data sharing is connected to, and directly supports, the delivery of the GOV.UK One Login service.

More generically, it is our view that the more effective sharing of data between public and private bodies is essential in the fight against financial crime. And this view will be evidenced – as highlighted in the FCA PSR ICO APP Scam Tech Sprint and Open Finance Policy Sprint – in forthcoming publication from The Payments Association's Project Financial Crime, "Financial Crime & Data Sharing White Paper", scheduled for March 2023.

4) To what extent do you agree that the following government departments should become a public body eligible to share data for public service delivery objectives (these public bodies are listed in Schedule 4)?

Cabinet Office
Department for Transport
Department for Food, Environment and Rural Affairs
Disclosure and Barring Service

Please choose one of the following options:

Neither agree nor disagree

Please provide the reason for your response and specify which public body you are providing views on.

On this specific question we can only assume that the government has determined the precise need for which departments require data sharing, taking into account all relevant data protection and privacy considerations.

However, concerns were raised among our members regarding the nature of the data to be shared and the services this is intended for. Some members pointed out that not every department requires detailed information on citizens and have expressed scepticism over the desirability of a centralised ID program, preferring a more distributed design to minimize the number of departments that need to store the information. The consideration of

government as a single entity for the purposes of data sharing brings considerable risk and any problems – not to mention penalties for a data breach - could be significant.

Nonetheless, we believe that all government departments should be able to share data to prevent the abuse of government systems e.g. in the prevention of financial crime.

5) To what extent do you agree that the following government departments should be able to share data for the identity verification objective?

Cabinet Office
Department for Transport
Department for Food, Environment and Rural Affairs
Disclosure and Barring Service

Please choose one of the following options:

Neither agree nor disagree

Please provide the reason for your response and specify which public body you are providing views on.

The same logic that we have expressed in Question 4 applies here.

Whilst we understand why the Cabinet Office and the Department for Transport are listed, respectively as Service Provider and for Driving Licenses, it remains unclear why Service users such as DEFRA, DBVS, etc., need to be added to the legislation, and how this impacts other regulations e.g. GDPR. We strongly fear that requiring a legislation update for every change in service user/provider may end up adding the unintended consequence of adding friction and cost to an already strained government process.

6) Are there any other public authorities not proposed in this consultation which you think should be able to share data for the identity verification objective?

Please choose one of the following options:

Yes

Please provide the reason for your response.

Some of our members noticed that Registers of Scotland, and Land & Property Services (LPS) should be included, given that they are the equivalent to HM Land Registry in England. However, it will remain for the government to consider whether opening up data sharing to a larger extent could further improve the inclusivity of the identification services (this would depend on which governmental departments/agencies hold the necessary data).

7) To what extent do you agree that the data items, known as data attributes, as described under this proposed objective are consistent with, and appropriate for, the delivery of the objective?

Please choose one of the following options:

Disagree

Please provide the reason for your response and specify the data item you are referring to.

Most of our members are inclined to disagree for several reasons:

1) Knowledge-based verification is considered to be a weak form of identity check as the data is likely to be available to others, given the frequent hacks and data availability on the dark web.
2) In the consultation text, the sentence "attributes held by government departments necessary for verifying the identity of an individual" is ambiguous, and – without providing examples – undermines trust.
3) Use of ambiguous and open-ended terms relating income for identity checking, or other transactional data, is inconsistent.
4) In the consultation text, the sentence *"Different government services have unique identity verification criteria depending on the level of confidence required in an identity."* indicates that perhaps a standard for identity management should have been developed first.
5) In the consultation text, the paragraph *"The data returned to the government service that initiated the identity verification check on the individual will include the result of the identity check, and a minimum set of attributes required to identify the individual whose identity was checked. For example, this might include the individual's name, date of birth, and any additional data attributes that the government service requested were collected from the individual, such as the individual's address."* suggests that the processing is incorrect. The service user is providing the base set of information that is to be validated as an existing identity. The return should be a 'yes, confirmed', 'no, not confirmed', or 'additional validation required, {specify additional attributes for confirmation}'. Currently the data flow appears incorrect for simple identity verification.

Even our less critical member **–** who tended to agree that the proposed data is consistent with the objective **–** has recommended adding more clarity to the process, such as describing the qualitative differences between different datasets in the process of identity proofing.

8) To what extent do you consider the proposed sharing of data for the identity verification objective will lead to any individual and/or household losing any benefit?

Please choose one of the following options:

Neither agree nor disagree

Please provide the reason for your response.

It is empirical to observe that the push to digital may have caused marginal cases of exclusion, where technology adoption is not possible or where bridging the divide remains inadequate. Thus, we believe that the government should ensure that this outcome does not happen, as the state should counterbalance some consequences of bridging the divide in innovation by promoting solutions that eliminate its potential negative impacts.

9) To what extent do you consider the proposed sharing of data for the identity verification objective will lead to an individual and/or household losing access to a service?

Please choose one of the following options:

Neither agree nor disagree

Please provide the reason for your response.

For the same reasons that we have exposed in Question 8, we believe that the government should bear the responsibility of ensuring that this outcome does not happen.

10) Do you think the proposed data sharing for identity verification services will negatively impact on people who share any of the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

No response.

If yes, please provide the reasons for your response specifying the protected characteristic(s) you think will be impacted.

11) Do you have further comments on this proposed objective?

Yes, we have a few comments to add:

1) From a payments industry perspective, we note that the DMCS GDS lead standard BS8626 explicitly states that the proposed manner of identity verification is not suitable for regulated entities such as those mandated under PSD2 and that British standard PAS499 should be used instead.
2) In addition to the current initiative, we would like to point out that reusability of data is also important from a private-service perspective and that the government should consider opening up registries and databases for use-cases and attribute-checking that are legitimate and support the reusability of public data within the private sector.
3) We highlight the risk that any existing fraudulent or erroneous record becomes the basis for further criminal capability – identity verification is premised in the correct process for granting initial records e.g., birth certificate, driving license etc..
4) Overall, we notice that the language used is ambiguous and suggests that more is intended than it actually is, e.g. "data sharing gateway". The proposal has been written from the perspective of the government and not the individual e.g., benefit: "the infrastructure to unlock hundreds of millions of pounds of savings across departments through avoided costs and duplicate digital identity systems;" could have been written to highlight the decrease in cost to the individual (lower taxation), or an increase in spend in other areas i.e., the actual outcome and not the intermediary outcome. The section, "What other options have been considered?" highlights other legislation in place at present, yet there is no mention of what these are, or the removal of such.
5) We believe that simplification is required, with a clear distinction between:
   - What is the objective?
   - What is wrong with current methods?
   - What is the proposal?
   - Why is this better?
6) Some of our members question the need for a centralised government ID service, that replicates services already available in the private sector market, e.g. GDS are building a DBS service (criminal records service) when there are already several available in the market, and think that GDS should better align with the DCMS framework for identity. They highlight that there are two legal gateways being proposed for data sharing, one within the Data Protection Bill and one from this consultation and that it would be better and simpler to have a single framework

where citizens could consent to share data from and to any destination across public and private sector.

12) Please indicate whether you are happy for the relevant points and comments you have made to be published in the consultation summary report:

We are happy for my responses to be published alongside my organisation.

About The Payments Association

The Payments Association (TPA) helps 200 companies from across the payments ecosystem to navigate a complex regulatory environment and facilitate profitable business partnerships.

Our purpose is to empower the most influential community in payments, where the connections, collaboration and learning shape an industry that works for all.

We operate as an independent representative for the industry and its interests, and drive collaboration within the payments sector in order to bring about meaningful change and innovation. We work closely with industry stakeholders such as the Bank of England, the FCA, HM Treasury, the Payment Systems Regulator, Pay.UK, DCMS, HMRC, UK Finance and Innovate Finance.

Through our comprehensive programme of activities for members and with guidance from an independent Advisory Board of leading payments CEOs, we facilitate the connections and build the bridges that join the ecosystem together and make it stronger.

These activities include a programme of monthly digital and face-to-face events including our annual PAY360 conference and PAY360 Awards dinner, CEO round tables and training activities.

TPA runs seven stakeholder working groups: Inclusion, Regulator, Financial Crime, Cross Border, Digital Currencies, ESG and Open Banking. The 150 volunteers within these Project Teams represent the collective view of The Payments Association members at industry-critical moments and work together to drive innovation in these areas.

We also conduct exclusive industry research which is made available to our members through our Insights knowledge base. These include monthly whitepapers, insightful interviews and tips from the industry's most successful CEOs.

See www.thepaymentsassociation.org for more information.

Contact malik.smith@thepaymentsassociation.org for assistance.