DCMS CP: Digital Identity and Attributes Consultation
Barclays Response

About Barclays

Barclays is a British universal bank. We are diversified by business, by different types of customer and client, and geography. Our businesses include consumer banking and payments operations around the world, as well as a top-tier, full service, global corporate and investment bank, all of which are supported by our service company which provides technology, operations and functional services across the Group. For further information about Barclays, please visit our website home.barclays.

Consultation Questions

Section 1 – Creating a Digital Identity Governance Framework

1. **Do you agree an existing regulator is best placed to house digital identity governance, or should a new body be created?**

Reusable digital identities have the potential to streamline and improve a wide range of services across the digital economy, supporting a number of sectors, and improving online services for customers. However, if not done properly, they could introduce significant risk to individuals and the economy, for example through identity theft and fraud: fraudsters may create false identities, or steal the identities of others, and immediately reuse these for nefarious purposes such as applying for physical ID documentation (such as passports), taking out loans, or setting up a fake business. It is critical, therefore, that the governing body overseeing the digital identity framework has clarity of oversight and remit, strong enforcement capabilities, and an ability to act quickly if it identifies bad actors and/or weaknesses in the system.

Barclays is agnostic as to whether this governing body is a new, purpose built regulator, or whether a new division is set up within an existing regulator, so long as the body is effective and has sufficient powers to perform its role. Government, however, should not take this decision on a cost basis, given the cost of getting this wrong (and allowing fraud to infiltrate the economy) would far outweigh the cost of setting up a new regulator. At this early stage in the development of the market, it should be possible to create a relatively small, efficient and nimble organisation, that could be further built out as the market matures.

Barclays agrees that it would be important to leverage the experience of existing regulatory bodies when establishing this new regulator/division. This could be done through appropriate secondments from existing regulators, into this new body. Furthermore, the governing body should ensure strong collaboration and cooperation with other relevant regulators, for example, if digital identity is to be used in the financial services sector, it should work closely with the FCA, the BoE, and the relevant entities overseeing the money laundering regulations in the UK.

We agree with the proposal that all of the governance functions outlined should be undertaken by a single regulator, in order to avoid a complex regulatory landscape.

We would also encourage government to consider whether the governing body should oversee all firms that create and provide *reusable* digital identities, i.e. whether membership of the trust

framework should be made mandatory for all these firms. This could help ensure that personal identity information is appropriately protected, and would prevent a blurred regulatory perimeter, whereby some firms involved in digital identity could fall outside of oversight from the governing body, by simply not joining the trust framework. This would help to prevent consumer harm and confusion where customers do not realise that a digital identity provider they are using is not part of the framework and therefore does not fall under the remit of the regulator (noting that consumers wouldn't necessarily know to check a register or look for a trustmark).

2. Which regulator do you think should house digital identity governance?

As above, Barclays would be supportive of government creating a new regulator, if that is deemed to be the best way to ensure effective oversight.

However, if it is deemed that an existing regulator should house a new division to oversee the digital identity market, then we do not believe there is a clear choice as to which regulator. Given the cross-sectoral nature of a digital identity market, it is important that the regulator is able to operate across the economy with entities in many different sectors. As a result, we do not believe any of the existing sectoral regulators would be appropriate to be the governing body. The regulator should also have strong expertise in the latest technologies relevant to a digital identity market, including biometrics, AI, cryptography and distributed ledger technology. Furthermore, the focus of this regulator needs to be clear and defined from the outset towards establishing and overseeing an effective digital identity market. We believe the ICO is likely the best candidate, given its focus on information, data and privacy.

3. What is your opinion on the governance functions we have identified as being required: is anything missed or not needed, in your view?

We consider that the governance functions identified are the right ones.

We would suggest explicitly including reference to enforcement capabilities within this list, including the ability to revoke (and temporarily freeze, whilst under investigation) a firm's ability to create / verify digital identities, to enable the governing body to act swiftly if a bad actor is identified (as outlined in section 2.6.4).

Trust framework, standards and rules management

4. What is your opinion on the governing body owning the trust framework as outlined, and does the identity of the governing body affect your opinion?

Barclay agrees that the governing body should have responsibility for owning and running the trust framework.

However, while the governing body may retain overall ownership, it is important that it also looks to engage and leverage relevant technical expertise when developing and updating standards. We therefore support the government's proposals that advisory groups will be established to advise the governing body. We would specifically note the importance of the governing body engaging key sectors that will consume digital identities downstream, on an ongoing basis, to ensure regular feedback and to understand any developing risks or impacts. For example, any uplifts in identity theft, increases in the generation of false identities, financial exclusion etc.

Government should also consider whether a separate technical entity / expert committee could be established, responsible for developing or identifying existing standards for the governing body to adopt as part of its framework. This could exist below or at arm's length to the governing body, which would delegate specific technical tasks to this entity. It should also engage with existing Standard Setting Organisations (SSO), including the BSI, and other international SSOs. This separate entity could be required to lead any engagement and consultation with all relevant stakeholders and experts.

When developing or updating standards, the governing body (or the standard-setting entity described above) should seek to ensure they are considering any international standards that may exist. In an increasingly digital and global world, the governing body should seek to ensure that the UK digital identity landscape is interoperable with those in other jurisdictions. The standard setting entity described above could also be responsible for monitoring the development of international standards, and gathering any lessons learned from frameworks in other jurisdictions.

5. Is there any other guidance that you propose could be incorporated into the trust framework?

We recognise that the proposed trust framework is intended to set only the rules of the road for digital identity in the UK, rather than dictate any specific model or standard for digital identity propositions. However, we would highlight that this approach is likely to result in multiple different proposition standards developing, with no predominant model – at least for an initial period. Such an approach may encourage competition and innovation in the identity space for the benefit of the consumer, with a potential impact on the speed of driving adoption and scalability of the models. To mitigate this possible risk, over time as the market develops, government should constantly review the balance between market and industry dynamics vs the speed and scale of adoption, and should discuss with market and industry participants and relevant experts to explore whether consolidation of models would help maintain balance between the two.

6. How do we fairly represent the interests of civil society and public and private sectors when refreshing trust framework requirements?

Barclays supports the Government's proposed approach to broad stakeholder consultation. See our response to Q4, regarding a specific standard setting entity that could be responsible for consultation of relevant stakeholders.

Ultimately, to ensure the success of this digital identity framework, government and the governing body need to ensure it provides commercial opportunities for private sector entities, to encourage participation, and high levels of security for data, to build consumer trust.

7. Are there any other advisory groups that should be set up in addition to those suggested?

The governing body / standard setting entity should also ensure to engage with the Joint Money Laundering Steering Group (JMLSG), which has significant experience in providing guidance to the financial services sector regarding KYC. There are likely to be areas in the digital identity trust framework where JMLSG expertise would be relevant.

Accreditation & certification

8. How should the government ensure that any fees do not become a barrier to entry for organisations while maintaining value for money for the taxpayer?

Barclays supports the government's proposed approach to accreditation and certification, which we consider would ensure firms can be trusted to have met the standards of the trust framework.

When considering fees for organisations in the trust framework, a starting point should be to consider the costs of the governing body to operate and undertake its assigned functions. The fees from organisations must be sufficient to meet this cost, and should be covered by all entities. Barclays considers that an onboarding fee would be appropriate to reflect initial joining costs, as well a smaller annual fee to cover BAU costs for the governing body.

One option being considered may be to charge different organisations according to their size (e.g. quantity of verified identities), to minimize any barriers to entry. However, while it is important to maximise participation in the framework, it is more important to ensure all entities - irrespective of their size or scale - are subject to a minimum standard of robust checks in the certification process. It is critical, therefore, that any charging model does not see lower fees accompanied by lower standard of certification checks.

An alternative option could be to charge different fees, for providers looking to provide digital identities at a higher or lower degree of assurance. For example, those intending to provide very high level of assurance, e.g. bank-grade, could be subject to higher fees, as the required certification checks would be more detailed. In contrast, providers looking to provide relatively low levels of assurance could be subject to the minimum certification checks, and therefore a lower fee.

We would also suggest that any fines imposed on trust framework entities for breaches of the rules, should be used to cover ongoing costs of the governing body.

Oversight/Management of organisations/schemes

9. Do you agree with this two-layered approach to oversight where oversight is provided by the governing body and scheme owners?

Barclays supports the Government's proposed two-layer oversight model.

Complaints, redress and enforcement

10. Do you agree the governing body should be an escalation point for complaints which cannot be resolved at organisational or scheme level?

Yes, Barclays considers that customers should raise any concerns at the organisation/entity level in the first instance. If unresolved, they should then be raised at the scheme level (where applicable), and subsequently to the governing body as the escalation point. As noted above, it is important that the governing body covers the entire framework rather than separate entities for specific sectors, so that any escalated complaints are dealt with consistently across the framework.

11. Do you think there needs to be additional redress routes for consumers using products under the trust framework? (Y/N)

It is critical that firms understand the importance of protecting the data that customers entrust to them, when verifying and storing their identity information. Just as banks build strong vaults to protect their customers' deposits, so must all firms in a digital identity ecosystem ensure that every step has been taken to protect customers' identity and data. The governing body must therefore ensure that all entities in the trust framework take appropriate steps to protect consumers' data aligning to GDPR where relevant. In the event that a breach occurs – wherever in the data chain – customers must have the right of redress against, and compensation from, the specific firm which allows its security to be breached. Without this, customers will surely lose confidence in the digital identity ecosystem.

At this early stage in the ecosystem's development, it could be preferable to facilitate appropriate redress and compensation through mandatory clauses in firms' contracts with customers. This would also facilitate a nimbler, and less resource intensive approach, which would best suit an emerging ecosystem, as it avoids introducing significant cost and complexity at this early stage, particularly given the desire to encourage early movers into the market, and participation in the framework. As outlined in point 2.6.2.8, the governing body should reserve the right to consult on implementing an alternative approach (such as an alternative dispute resolution scheme), once the market has established, and it is possible to consider what customer harms are being observed, and whether the contractual clauses are sufficient for redress, or whether another body is required.

12. Do you see any challenges to this approach of signposting to existing redress pathways?

Barclays does not support consumers being signposted to existing redress pathways, as this could create markedly different customer outcomes, depending on which actor in the ecosystem has potentially been at fault. If the entity is a financial services organisation, for example, then the customer could seek financial compensation through the Financial Ombudsman Service (FOS). However, this wouldn't be possible for customers that may have created an identity with a provider that doesn't fall under the FOS or an alternative existing redress pathway. These customers would face very different outcomes, simply because one chose to create their digital identity with a firm that happens to be subject to a redress entity, due to other regulated activity that it undertakes.

Furthermore, having multiple redress pathways could cause confusion for the customer, who may not be clear on which firm in the chain they are seeking redress from, given there are multiple firms operating across a range of roles in the market (from digital identity provider, to orchestration service provider etc).

Therefore, to avoid poor customer outcomes for some customers, we would encourage a single approach to redress, covering all providers and schemes in the market. Sectoral regulators and appropriate ADR schemes should direct any complaints relating to digital identity services via this single approach, to help ensure consistency across the market. This approach would also meet an intended aim of avoiding duplication of regulatory functions, while also providing a centralised oversight of the root cause of complaints.

13. How should we enhance the 'right to rectification' for trust framework products and services?

Barclays recognises that data inaccuracy could create challenges for consumers, especially if it prevents them from accessing a required service. It is right therefore that government consider system wide options to enable consumers to quickly repair or complete data in their digital identity.

However, we have significant concerns regarding the proposed 'no wrong door' policy. A consumer may be engaged with many entities regarding their digital identity, and in the event of any issues, it would be extremely challenging for one firm within this ecosystem to support that customer in identifying erroneous data held across all of the other firms in the ecosystem. That entity may not have a right to access the data from the third parties, and/or they may not have technically integrated with all of the entities in an ecosystem to enable them to do so (for example a customer may have a university as an attribute provider, certifying their degree, but a bank may not choose to technically integrate with the university, as university degrees may not be attributes that the bank would ever require from their customers). Therefore, the proposed 'no wrong door' policy is likely to be incredibly burdensome, time consuming and costly for firms that choose to participate in the trust framework. Instead we firmly believe the onus should be on the consumer themselves to approach relevant trust framework entities they have engaged with to seek rectification. The governing body and/or scheme owner should provide a supporting role to assist consumers with this, with any costs reflected in their fees to trust framework participants.

Separately, it is not clear how this 'no wrong door' policy is commensurate with the concept of 'self-sovereign identity'. Under self-sovereign identity, only the consumer knows the entities that they are accessing data from, and who they are sharing it with. The other entities are not aware of that information. The no wrong door policy would necessarily involve the consumer sharing with an organisation, all the other organisations that may hold data on them. This is further argument for the governing body / scheme owner to play a key role in rectification, aligned to the complaints and redress process.

14. **Should the governing body be granted any of the following additional enforcement powers where there is non-compliance to trust framework requirements?**
    - **Monetary Fines**
    - **Enforced compensation payments to affected consumers**
    - **Restricting processing and/or provision of digital identity services**
    - **Issue reprimand notices for minor offences with persistent reprimands requiring further investigation**

The governing body should be granted all of the above listed powers, in order to effectively undertake their role of overseeing and monitoring the digital identity market. Remit and scope should be clarified, to ensure that overlaps with other bodies (e.g. ICO's supervisory role over UK GDPR and the Data Protection Act) are identified and managed. In particular, duplication of enforcement should be avoided, and an approach to achieve coordination between relevant authorities is needed.

15. **Should the governing body publish all enforcement action undertaken for transparency and consumer awareness?**

Barclays supports the proposal for the governing body to publish all enforcement action for transparency and consumer awareness purposes. This approach aligns with that taken by the FCA.

Security & Fraud

16. What framework-level fraud and security management initiatives should be put in place?

Barclays agrees with the Government's assessment that as well as offering significant benefit to the UK, a digital identity ecosystem will inevitably become a target for criminals looking to exploit the framework. It is critical therefore that the governing body takes appropriate and necessary action to minimise fraud risks, beyond just setting standards in the trust framework.

Barclays has a number of thoughts on this issue:

- **Trust marks**: while we understand the intention behind the use of trust marks for certified entities in the framework, we have significant concerns that the simple use of a logo is very vulnerable to misuse by nefarious actors. There is very little to stop a fraudulent entity adding the logo to their website, which risks consumers having misplaced confidence that the entity is legitimate. It is for these reasons why the firms involved in Open Banking (OBIE and the CMA9) considered and rejected the concept of a trust mark for the Open Banking framework.
- **Central directory of certification**: In contrast, we support the concept of a central directory list of trusted/certified entities to be run by the governing body, which can also be digitally accessed via an API. Given this is managed centrally by the governing body, there is much less risk of fraud/misuse. Furthermore, each certified entity should have a digital and 'live' version of their certification, enabling other entities to check in real time that the entity has a live valid certificate. It is important that any bad actors in the system have their certification removed, and all other entities in the framework are able to see that immediately. Further, if an entity suspects that something is 'wrong' with another entity in the framework, they should have the ability to reject any digital identity/attribute data sharing requests, until any concerns are resolved. We also believe that the removal or suspension of regulated entities within the trust framework via this directory could help foster trust and quick detection of rogue entities.
- **Service provider right to vet relying parties**: Schemes, and/or identity and attribute service providers, should be able to determine which relying parties they agree to contractually engage with for the provision of identity and attribute data, allowing them the opportunity to run any checks on those organisations that they deem necessary. There should not be any requirement upon schemes or identity and attribute service providers to allow any and all relying parties to connect to their service.
- **Encryption of data and data security**: we firmly believe that the trust framework should require minimum standards of cryptography to be used when digital identity or attribute data is shared. This would help minimise the risk of data leakage through interception. Similarly, it is critical that relying parties have appropriate provisions in place to ensure any data they receive is appropriately handled.
- **User self-audit of digital identity use:** consumers should have the ability to undertake a 'self-audit' of how and where their digital identity has been accessed and used, similar to their being able to see their financial footprint on their credit file. This would enable them to self-identify whether their identity has been fraudulently used e.g. where they didn't initiate or authenticate a check.
- **Central fraud function:** Government should consider whether the governing body should have a specific department dedicated to managing fraud and resolving any issues stemming from compromised digital identities. This central fraud function should play a coordinating role in ensuring all relevant stakeholders are informed where fraudulent activity is identified. For example, if a digital ID is compromised, where feasible (from a technical, operational and commercial perspective) the identity owner should be informed if they are not already aware, as well as entities that may have leveraged that identity so they can take

any necessary remediating action – e.g. a bank may need to take action if an account opened with a digital identity is subsequently found to be fraudulent.

- **Collaboration and intel sharing:** Barclays supports the proposal for the governing body to coordinate information sharing between relevant stakeholders to minimise security and fraud risk. While we recognise that a new information sharing initiative may be required between trust framework entities, we would encourage Government to leverage and engage with existing initiatives where possible, e.g. the CSISP, CIFAS and the CDA. It is right and important that the governing body seeks to collaborate wherever possible with law enforcement, security, government and industry organisations, as well as internationally with other jurisdictions.

Inclusion

17. How else can we encourage more inclusive digital identities?

Barclays supports government's intentions to ensure the digital identity framework is as inclusive as possible. It is important that all efforts are made to support consumers in creating and using digital identities as the world develops to become more digitally focused. However, it is important that no consumer is left behind by the introduction of digital identity and so it is right that digital identity will not be mandatory and traditional physical options are still accepted.

Barclays strongly supports the government's objectives in this space, and is heavily focussed on digital inclusion and upskilling. Barclays has colleagues, known as Digital Eagles, dedicated to upskilling consumers at all skill levels to become more confident in digital engagement, covering access to banking but also accessing a range of digital services as part of everyday life.

Government should consider whether it or the governing body can play a role in boosting digital inclusion, by supporting certain consumer cohorts who may face issues with exclusion to create their digital identities. For example, supporting groups such as school leavers, released prisoners, consumers receiving long-term government support, those leaving the military.

Barclays is concerned by the proposal for consumers to be able to create or use a digital identity based on a 'vouch' or declaration from a third party user. Whilst we support objectives to ensure inclusion, we have strong concerns that this could create a weak point in the framework, or a 'back-door', enabling criminals to create fraudulent identities that can then be used across the framework. It is critical that any initial identity verification, whether physical or digital, is completed to a high, trustworthy standard.

18. What are the advantages and disadvantages with this exclusion report approach?

Barclays agrees with the advantages listed in the consultation document. In terms of disadvantages, we would note that publication of such reports containing data on demographics of consumers that have been unable to create or use a digital identity, could create reputational risk for firms. This may be sufficient to prevent firms from joining the framework.

As an alternative, Government could consider allowing firms to share their report confidentially with the governing body, and work with them to consider and understand why there may be any undesired exclusions taking place, and possible solutions. This could achieve the same desired effect,

of ensuring that firms work to prioritise inclusion, whilst limiting the reputational risk considerations that may deter firms from joining the trust framework.

19. What would you expect the exclusion report to include?

Barclays considers that the content listed is the right content. Further we would suggest that a standardised format should be used across the framework, with prescribed content requirements to boost comparability and aid understanding.

Government should consider whether firms should be required to identify any commonalities between those excluded, in order to draw conclusions on potential solutions.

However, we would note that the proposed approach to follow a principle of data minimisation may mean that firms may not always have key information to compile the exclusion report. While data could be specifically requested for the purpose of compiling this exclusion report, we consider that this would not align with the data minimisation principle, and the data minimisation should take priority. Ideally, there should be a way to create exclusion reports without firms having to ask for specific data for the sole purpose of doing so.

Section 2 – Enabling a Legal Gateway Between Public and Private Sector Organisations for Data Checking

20. Should membership of the trust framework be a prerequisite for an organisation to make eligibility or identity checks against government-held data?

Yes, Barclays supports the proposal that membership of the trust framework should be a pre-requisite for an organisation to make eligibility or identity checks against government-held data. This will ensure appropriate checks and due diligence is undertaken, which helps build and maintain trust for all parties.

21. Should a requirement to allow an alternative pathway for those who fail a digital check be set out in legislation or by the governing body in standards?

Barclays agrees it is important that where consumers fail a digital check against their government held data, they are able to pursue an alternative route to accessing the service in question. However, we do not believe this should be provided for in legislation. Rather the governing body should be responsible for ensuring all entities across the framework are providing this capability as part of their inclusion obligations.

22. Should disclosure be restricted to a "yes/no" answer or should we allow more detailed responses if appropriate?

Barclays considers that restricting checks against government data to yes/no answers would limit innovation and potential use cases/propositions. While we recognise that a yes/no tool may be easier to implement, we would encourage government to develop this functionality over time to provide richer data in their data check responses.

23. Would a code of practice be helpful to ensure officials and organisations understand how to correctly check information?

Barclays supports the Government's proposal for a code of practice.

24. What are the advantages or disadvantages of allowing the onward transfer of government-confirmed attributes, as set out?

Barclays considers that permitting the onward transfer of data checked against a government-held source would be a necessary requirement of the UK digital identity framework. Of course, we recognise that for certain data it may be appropriate for a digital check to be undertaken again, to re-ensure accuracy. We therefore support the proposal for data controllers to determine the extent to which onward data transfer is permitted and the frequency of required checks

Section 3 - Establishing the Validity of Digital Identities and Attributes

25. Would it be helpful to affirm in legislation that digital identities and digital attributes can be as valid as physical forms of identification, or traditional identity documents?

Yes, to help the development of digital identity in the UK, Government should clearly establish that digital identities and attributes are as valid as physical or traditional forms of identification. However, Government should be clear that firms are not legally required to accept digital identities or play any role in providing them. Rather, firms are enabled to do so if they wish.

Finally, in the context of the regulated financial services sector, government should review the relevant financial services regulatory rules to clarify that financial services firms can accept digital identities to satisfy 'know your customer / ID and verification' requirements in order to provide products.