Digital Identity: Call for Evidence
FLA Response

The Finance & Leasing Association (FLA) is the leading trade association for the UK consumer credit, motor finance and asset finance sectors. FLA member companies include banks, the finance subsidiaries of major manufacturers and independent finance firms. They offer credit services to customers from all social groups, via credit and store cards, personal loans, point of sale finance, motor finance and a number of other consumer credit products, as well as a wide range of leasing and hire purchase services to businesses of all sizes. In 2018, members of the FLA provided £137 billion of new finance to UK businesses and households.

We welcome the opportunity to comment on the Department for Digital, Culture, Media and Sport (DCMS) and the Cabinet Office's Call for Evidence in relation to digital identity. We strongly believe that a multi-purpose and re-usable digital identity system will add value and should also help to pick up those consumers with thinner credit files. Indeed, we believe that electronic identification schemes are unquestionably the future. However, firms will only make more use of electronic verification if they are given more certainty on its use. This is likely to lead to substantial savings for firms with the on-boarding process in comparison to traditional more time-consuming processes currently used. Indeed, the Cabinet Office alone estimates the transactional cost savings in billions of pounds. And a recent McKinsey's report 'Digital identification – A key to inclusive growth' estimates that digital ID could unlock economic value equivalent to 3% of GDP growth in the UK, with 43% of this economic value accruing directly to individuals.

In our response, we will address the high-level themes posed as opposed to the detailed questions. But in doing so, we take into account the detailed questions posed.

Executive Summary

- We strongly believe that a multi-purpose and re-usable digital identity system will add value and should also help pick up those consumers with 'thinner' credit files and further aid financial inclusion.
- The economic case for and savings for firms with the on-boarding process, in comparison to traditional more time-consuming processes, are likely to be substantial and run into billions of pounds.
- A joined-up approach to digital identity is likely to bring reduced duplication, increased conversions, comparatively frictionless customer journeys and reduced operational waste.
- We believe the private sector has a key role to play here but Government should drive and co-ordinate the journey to establishing a trusted digital identity ecosystem in the UK. This will require a heavily collaborative approach.

- The Information Commissioner's Office (ICO) will have a key policing role to play here as any such system will rely heavily on personal data and information.

Questions

Questions 1-6: Needs and problems

We believe a successful digital identity solution will bring significant benefit to UK citizens and regulated firms. There are multiple examples where positive outcomes have been achieved elsewhere, for example the BankID scheme in Scandinavia and/or the Estonian eID that was delivered as part of a wider transformation of public services. Each of those cases illustrated the benefits a joined-up approach to digital identity will bring which trickled through to firms from the perspective of reduced duplication, increased conversions, comparatively frictionless customer journeys and reduced operational waste. A Government-led approach to digital identity would be preferential in that it would minimise different silos of technology – encouraging broader transformation and/or making it easier for people to interact with both public and private services.

However, one of the barriers to existing solutions is the lack of accepted industry guidance/industry standards here in the UK. As good as the Joint Money Laundering Steering Guidance (JMLSG) is, we still lack the creation of technical standards, identity assurance standards and appropriate governance arrangements which will better ensure that digital identity solutions are interoperable and future proofed. This is because it is the job of Government to set these standards and then for the likes of JMLSG to interpret/explain the requirements and give practical advice on compliance.

The other current problem is around liability. This is a key question for many firms that requires clarification e.g. who is liable for the fraud loss where the underlying digital ID is compromised and/or who will have to face the criminal sanctions in instances where such an incident constitutes a criminal breach of the Money Laundering Regulations? (MLRs). Although not an insurmountable problem, like industry stands and who sets these, this needs to be worked through.

As alluded to in the Call for Evidence inclusivity will also be key. The use of broader public sector data sets and certifications would appear the most sensible and robust way to bridge the gap for the financially excluded. Other potential options may include 'digital vouching' e.g. where individuals have an ongoing relationship with a reputable service provider, such as a local authority or bank, and a trustworthy worker at that provider digitally 'vouches' for the individual's identity. The ability to rely on public sector data sets, or other initiatives such as vouching, would need to be permitted within the MLRs / industry standards etc., otherwise firms would invariably have concerns that they were operating outside of accepted practice and, consequently, may continue to utilise more traditional identity verification techniques. However, again this is not an insurmountable problem and we know that UK Finance

and its big banking members are already some way down the track of increasing inclusion and helping those with ‘thin files’.

More broadly, a flexible approach that caters for the different needs of individuals, and contrasting regulatory requirements that apply to firms, is an important success factor. Different firms (regulated and unregulated) and public services operate on a wide range of differing requirements for identification and authentication, and the information that those services require varies too. By contrast, a one-size-fits-all solution will not promote inclusion to the same extent and could impact consumer take-up.

Questions 7-13: Criteria for Trust

In order to aid take-up, we believe that Government branding enhances consumer trust as opposed to private sector branding which can be viewed with suspicion (see, for example, OIX research). It also encourages wider usage e.g. the same digital identity can be used for tax returns, local authority registrations (Medical, Dental, Educational), official identity applications as well as private sector processes (bank logons, lending applications, gambling logons, social media sites, etc.). Clearly, the ability to reuse existing certification results would be the most pragmatic/cost effective approach – however from a regulated firm’s perspective the ability to / conditions for the reuse of certifications would need to be clarified in statutory guidance / the Money Laundering Regulations (MLRs). The Information Commissioner’s Office (ICO) and GDPR clearly has a key policing role to play here too as any such system will rely heavily on personal data and information.

Questions 14-20: Role of the Government

The Government is seen as a trusted source of identity and their documents (e.g. passport, driving licenses etc.) should enable a re-useable verification to be used across different product types. The Universal Credit letters are a good example of how Government has made a further contribution e.g. for those with ‘thin files’ etc.

We believe that the digital availability of government documents will greatly help the uptake of digital identity and the development of a digital identity market. This should include a way for end-users and consumers to give permission for their government documents to be shared digitally, such as though secure APIs.

Similar to other key stakeholders in this debate, we would urge the Government to think broadly about the type of government documents that could be shared beyond passport and driving license data, which are currently only accessible to a limited group through the Document Checking Service (DCS) under GOV.UK Verify. Without this data identity providers would need to use other sources to reach the levels of assurances necessary for Financial Services, which would be costly and time consuming. Any sharing should be with the end-users agreement.

By opening up government issued documents, firms will be better able to fight financial crime whilst also helping them comply with their Customer Due Diligence (CDD) and ‘Know your Customer’ (KYC) obligations. As alluded to above, the use of

government data should also help financial service firms deliver services to customers with ‘thin files’ due to access to more information about them.

Question 21: Role of the Private Sector

We believe the private sector has a key role to play here but Government should drive and co-ordinate the journey to establishing a trusted digital identity ecosystem in the UK. This will require a heavily collaborative approach. But ultimately one trusted body needs to oversee the creation of a set of digital identity standards which can link up the public and private sectors to enable strong, secure and trustworthy methods of digital identity to be widely available to citizens and businesses. Again interoperability will be key. Finally, within the private sector the three main Credit Bureau’s / Credit Reference Agencies (CRA’s) will have a pivotal role with the key information and data they hold which is likely to complement and help verify trusted Government documents as well as potentially provide alternative data or other official data to help further support financial inclusion and access to credit.

Finance & Leasing Association
13 September 2019