Response to

The Home Affairs Select Committee Inquiry into:
“Harnessing the potential of new digital forms of identification”

31st July 2025

Introduction

The emergence and rapid growth of the well-functioning umbrella market has been a positive contributor to UK growth, productivity and wealth. Compliant bona fide umbrellas – also known as Specialist Payment Intermediaries (SPIs) – provide certainty and security to the workers engaged by them, ensuring that; they receive the full protections required by employment law, their tax affairs are simplified, and all required taxes are remitted to HMRC.

The Freelancer & Contractor Services Association (FCSA) is the UK's leading professional membership body dedicated to raising standards and promoting supply chain compliance for the temporary labour market. Our members provide umbrella employment (via an Overarching Contract of Employment), self-employed services, accountancy, and business support solutions to the contingent workforce.

At time of writing, FCSA has more than 80 Accredited Members who collectively represent circa 220,000 workers engaged as employees; making them, collectively, one of the largest employers in the UK. Around 1 in 3 of the workforce represented by FCSA are women. Annually, FCSA members alone collect circa £12.5 billion in taxes and NICs which are timeously remitted to HMRC.

FCSA has worked extensively with government and other stakeholders to promote the highest possible standards in the industry, most recently providing labour market intelligence and umbrella regulation advice to directorates in the Department for Business and Trade (DBT), such as Labour Market Enforcement and Employment Agency Standards and HM Treasury, as well as working with HMRC across a number of areas including the off-Payroll Working Forum.

It has also assisted Parliament, giving evidence to the All-Party 'Parliamentary Loan Charge and Taxpayer Fairness Group', 'Modernising Employment Group', and the House of Lords Finance Sub-Committee, as well as being an expert advisor to the DBT-supported JobsAware initiative, the Better Hiring Institute.

FCSA continues to promote compliance within the sector for the benefit of individual workers, HM Government, and the supply chain. As a representative of a unique subsection of the labour market, it has also submitted various bodies of evidence to Government with market-led recommendations on how to drive non-compliance out of the supply-chain.

This submission outlines FCSA's position and recommended approach to harnessing the potential of new digital forms of identification. With our key use case of interest being Right to Work Checks (RTW).

Executive Summary

FCSA welcome the Government's intention to harness the potential of new digital forms of identification. Digital ID is not something new, it has been a reality for a number of use cases for over a decade and there is significant potential for its application to reduce costs and burdens for; individuals, businesses, and the state.

The use cases FCSA can most effectively speak to is those relating to Right to Work Checks (RTWs), as well as Disclosure and Barring Services (DBS) checks. There is significant potential for Digital ID to make both of these types of checks cheaper, more efficient in a range of use cases.

If a DBS or RTW can be completed once and the individual is able to share it as part of their Digital ID, this could prevent multiple companies from having to pay for the same process and it would avoid adding to the DBS backlog/reduce the demand on this public service. This is a particularly relevant consideration for the contingent labour market – there is significant potential to reduce costs and burdens.

A key principle should be that the 'Data Subject' is in control and decides who gets to see which data points, and that they are able to time-limit access. That is unless criminality has been detected, in which case it would be legitimate for authorities to follow evidence trails. Generally, data should only be accessed on a 'need to know basis', with the Data Subject in control of any master permissions.

Inclusion is another key concern. The increased adoption of Digital ID should not make it harder for non-digitally able people to access services or complete administration. This lack of Digital access can be due to; ability, resource, or simply habit. Another key principle is that the adoption of Digital ID should not make accessing existing services unachievable or any more difficult for those that do not access services digitally.

There are a number of challenges that exist within Government, particularly around existing infrastructure and technical integrations to facilitate a better cross-government joined up approach. A key aim should be to make better use of the information already available to Government. Following a use-case-based approach to establishing what new information is required before seeking any will be key.

Whilst FCSA believe that changes do need to be made, and we are broadly supportive of increased use and ease of Digital ID, we believe that an approach that maintains respect for individual civil liberties is vital and that there is a clear and viable need and use-case for the collection and storage of any new data points.

Inquiry Questions

1. How effectively is data relating to individuals currently being used and shared by the Home Office and its agencies?

FCSA believe this can be improved. Currently, proving right to work (RTW) in the UK is not as straight forward as it could be. Increased application of Digital-ID would help.

The simplest of use cases for evidencing RTW is for an individual to supply a current passport to an Identity Service Provider (IDSP), such as firms like 'Trust ID' or 'Credas'. The IDSP then do the RTW checks with the valid passport, which cannot be out of date.

However, not everyone has a passport, and Driving Licenses cannot be used for RTW checks. A Driving License can be used as evidence of ID, i.e. to prove address. National Insurance proof alongside a birth certificate may be another option to evidence RTW, but many – perhaps most – will not have a copy of their Birth Certificate and requesting an official copy is not straightforward or fast. Perhaps Birth Certificates alongside National Insurance Numbers (NINos) are something that can be included within the back end of Digital-ID.

There is likely to always be a need to enable different approaches for RTW checks – a single user journey working for all is hard to envisage. That said, more can be done to enable Digital ID to streamline user journeys for most, but it will not work for everyone.

If RTW checks are conducted using Digital-ID by default, then it should not be made more restrictive. For example, passports can expire or be revoked – the system should be designed in such a way that any associated RTW Checks do not become automatically invalidated.

Furthermore, as proving your identity becomes more prevalent greater issues may be realised as many people neither drive or leave the country, so have no need for either a Passport or Driving License – this exemplifies the need for an opt-in reusable Digital-ID that can be applied to a wide range of use-cases, with the data subject in control of what information they share, and with whom they share it.

2.What potential benefits could the use of new forms of government-issued digital identification have for the Government's ambitions to reduce crime and to manage migration?

If what is developed is robust and secure – underpinned by good data governance principles – then Digital-ID could become a key tool in fraud prevention. Digital-ID can help individuals avoid falling victim to fraud, by enabling data subjects to share limited

data points (e.g. age), without sharing an entire document with numerous data points that may not necessarily be needed for a particular use case – this severely restricts the opportunity for fraudsters to obtain large amounts of an individual's personal data.

In terms of managing migration, for Digital-ID to be effective in serving one of its core purposes i.e. RTW Checks, it would need to be compulsory for all those migrating into the UK. All UK Citizens over the age of 16 are issued with a National Insurance Number to assist in them proving their RTW, this therefore compatible with the opt-in approach for UK nationals.

a. In particular, how could new forms of digital identification be used to:

i. Prevent and investigate crime, particularly fraud

Digital-ID enables traceability which is valuable to any investigation. There is the deterrent aspect in that if someone knows they are traceable, they are perhaps less likely to commit an offence. However, ID fraud could potentially increase as criminals adapt and evolve their methods to avoid detection. Tech is just as much of a tool for those committing crime as it is those tackling it.

ii. Manage border entries and exits

Particularly in the contingent labour market, Student Visa are a significant area of weakness in the UK's immigration and border system.

For example, the terms of the visa state that entrants can only work 20-hours per week in term time, employer are required to secure a letter from the University to confirm term time dates. However, the student may not attend all classes, the courses may change in duration, the student may leave and the employer has no sight of attendance.

There is also no means of an employer knowing whether or not their Student Visa Worker has more than one job, and therefore whether they are complicit in facilitating a breach of the terms of a visa (knowingly or inadvertently) as there is no enforcement.

Digital-ID could in theory help with traceability and therefore somehow be used to monitor the compliance with the terms of a visa – then again, so could the existing tax system if leveraged properly.

iii. Support immigration enforcement

Again, traceability is a key tool provided by Digital-ID. If you know how and when the Digital-ID has been used this is useful information for enforcement.

However, there are too many instances of people using other people's identity to complete work in the gig economy, whether that be app-booked taxis or food delivery drivers – the person that shows up does not necessarily match what your app says.

iv. Support labour market enforcement

Right to Work Checks (RTWs) are currently quite difficult and can be time and labour intensive. Digital-ID could be used to simplify this in a large number of use cases (but not all). If the traceability element of Digital ID is properly explored and developed, this could become a useful enforcement tool.

v. Administer the asylum system

If Digital-ID was mandatory for all Asylum Seekers it could help to streamline the processing system and enable traceability which will help with monitoring. This could lead to a less resource intensive approach to effectively managing the system.

b. Would government-issued digital identification need to be mandatory to realise these benefits?

For the migration and asylum system, yes Digital-ID would need to be mandatory for it to be effective. This should not be the case for UK nationals who automatically already receive a Birth Certificate and a National Insurance Number.

It is important to remember that most other countries have mandatory national ID card systems and therefore mandating Digital-ID for the UK's immigration and asylum system – in most cases – is merely mirroring the requirements of their country of origin.

As a side note: Given that there is already a lot Government needs to do to upgrade its infrastructure, now is clearly not the time to consider the options for mandating Digital ID for those turning 16 after a given date and year. This debate should not be started until we have a tried and tested system that has worked for a number of years.

If the Government did explore this, Digital inclusion would be a key question – it would be important not to disadvantage anyone with learning difficulties or any other issues that may not yet have been considered. If Government were to explore this idea, it would need to be expressly on the basis of not backdating the measure – continuing to allow those already above 16 to opt-out by default if they choose. Data Security would also need to be guaranteed, with safeguards built into systems.

3. What different categories of information about individuals could most usefully be included in government-issued digital identification?

For the contingent labour market, Right to work in the UK is fundamental. However, certain high risk DBS entries or alerts may be appropriate – employers need to know if someone has criminal record. Records of any allergies or medical conditions could also help to ensure an individual is cared for appropriately should a serious accident occur – the person's next of Kin would be useful, and potentially organ donation status. Clearly, information should only be able to be accessed if appropriate to a situation.

a. What implications would the inclusion of different categories of information have for the efficacy of digital identification for law enforcement and/or immigration enforcement purposes?

Assuming the information is up to date and accurate it will help with tracking and detection. If a Digital-ID is compiled using various different documents/information feeds, it is likely to be more accurate and informative.

4. What potential risks does the adoption of new forms of digital identification have for individuals, including risks to privacy and security of personal data?

There is a danger of a Digital ID falling into the wrong hands and being used to commit fraud, the more vulnerable and less digitally able or aware an individual is, the more they are at risk.

A big concern is whether or not a Digital ID can be cloned and used without the individual even being aware – how can this be tackled?

It is also important to ensure that those accessing or having sight of an individual's Digital ID are only seeing strictly necessary information. A key question should be: are people and organisations seeing more than they really need to see?

5. What capabilities would the Home Office and its agencies need to develop to effectively introduce and take advantage of new forms of digital identification?

They would need to integrate across different government systems held in different departments, which could be a significant challenge. Robust contingency plans will be needed for any shutdowns/technical faults and any systems falling victim to external attacks.

6. How could the adoption of new forms of digital identification improve efficiency and interactions between the Home Office, law enforcement agencies, and other Government departments?

Government could become better able to use and understand the information already in public hands, and become better able to use it for enforcement purposes. It is important to understand what would be useful to collect, and then understand which departments need information for what purpose and how to establish necessary links.

Digital ID would be a good solution for linking all existing information from multiple agencies together. However, we are concerned that Home Office, HMRC, DWP etcetera may not currently have access to the necessary infrastructure to enable the safe and effective sharing of data. The creation of the Department for Science, Innovation and Technology (DSIT) and moving all core Government digital services into a lead department could help with improving the coordination of this.

It perhaps makes sense to take a use-case-based approach to working out what is needed and what will work best – start small, test and build out into other use cases.

7. How can the Government learn from the use of new forms of digital identification work internationally?

There are perhaps two ways the UK can learn from international comparators. When building new infrastructure from scratch, countries such as Estonia who built their systems from scratch in the current Digital Age can provide helpful lessons.

However, a key disadvantage the UK has that comes with having been among the first to become a large developed country, is that many of our systems were developed long before the Digital Age and upgrading and innovating is therefore not as straight forward. Looking at what approaches have worked well/and less well in other developed countries would be a good starting point. Perhaps making use of international studies and reports conducted by bodies such as the OECD would be a good starting point.