JUNE 2026

Digital Identity Market Analysis

2026 Findings

Prepared by Perspective Economics, commissioned by the Office for Digital Identities and Attributes (OfDIA), part of the Department for Science, Innovation and Technology (DSIT)

perspective economics

CONTENTS

Contents

EXECUTIVE SUMMARY

Executive summary

The Office for Digital Identities and Attributes (OfDIA), part of the Department for Science, Innovation and Technology (DSIT), has commissioned Perspective Economics (with survey support from Survation) to conduct an updated study of the digital identity sector in the UK. This research provides an annual update to the 2025 baseline study, published on GOV.UK in May 2025. It explores how the market has evolved in the previous year, including an assessment of market growth, new entrants, market changes, and consumer attitudes towards use and adoption of digital identity.

We set out key findings below:

The UK Digital Identity Market

- We estimate **275 firms** are currently providing digital identity products and services in the UK, a net increase of 9 firms (+3%) since the baseline study. Of these, 233 are dedicated providers and 42 are diversified firms.
- The sector generated an estimated **£2,027 million in annual revenue** in 2024/2025.
- Estimated **Gross Value Added (GVA) reached £1,037 million**, an increase of £149 million (+17%) since the baseline, suggesting an improvement in sectoral productivity.
- **GVA per employee rose to £107,800**, up from £86,600 at baseline, comparable to the cyber security sector (£116,200) and the wider digital sector (£89,200) and is approximately 46% above the estimated UK workforce average.
- An estimated **9,624 Full-Time Equivalents (FTEs)** are employed in digital identity roles across the UK, a decrease of 6% from the baseline (10,246). We note that this reduction is concentrated among large and medium firms and is consistent with market consolidation, increased use of AI, and broader tech sector headcount pressures.
- **75% of providers** are involved in identity or attribute verification, with document-based verification (60%) and biometrics and liveness detection (57%) the most common sub-categories. Providers are broadening their offerings: professional and credential verification rose from 28% to 55%, and age assurance from 23% to 31%.
- The sector is **highly internationalised**. 73% of firms are UK-headquartered, of which 36% have at least one international office. Among 28 firms filing geographic revenue data, 62% of revenue was generated from international markets, up from 57% at baseline. Over a third of the sector's c.£2bn revenue (£686m) is attributable to export activity.
- **Investment activity** totalled £49 million across 14 deals in 2025. Approximately three in ten dedicated firms have received external investment since incorporation. Merger and Acquisition (M&A) activity has continued, including the acquisitions of TrustID, Keyless, and DataTools.

Digital Identity Market Adoption

- Almost **4,700 unique customers and partnerships** were identified across providers. Financial and professional services remain the core customer sector (90% of firms), with healthcare and public services rising notably from 58% to 72%.

- The top reported use cases are **Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance (53%)**, fraud prevention (50%), secure access management (43%), and right to work checks (41%). Almost 100 firms appear to support with right to work checks. Age verification for online services has doubled to 33%, consistent with Online Safety Act implementation.
- Providers increasingly frame their value proposition around compliance and user experience rather than purely operational efficiencies. This appears to coincide with a more demanding regulatory environment, though the data does not directly attribute the shift in framing to specific regulatory drivers.

Consumer Attitudes to Digital Identity

- A consumer survey of **5,658 UK residents** was conducted by Survation in November 2025, with results weighted by age, sex, region, income, qualifications, employment status, socioeconomic group, and ethnicity.
- **81% of respondents** report some level of understanding of digital identity, up from 71% at baseline. The proportion reporting limited or no understanding has fallen from 29% to 19%.
- **77% of respondents** report having used a digital identity service for at least one purpose. The most common digital use cases include insurance, credit applications, and bank account opening (each 40%), followed by property and right to work checks.
- Among non-users of digital identity services (23%), the most commonly cited reasons were **preference for physical ID (29%)** and not having had to prove their identity (29%). Access barriers such as lack of a digital option (15%) and lack of documents (13%) also featured.
- Consumer preference for digital identity usage is **strongest for online contexts**. 39% prefer digital for age-restricted online purchases, and 36% for accessing public services. Physical preference remains dominant for in-person scenarios such as proving age in a bar or cinema (41% physical vs 23% digital).
- **71% of respondents** believe digital identity services will be important over the next five years, even though only 43% view the current direction of development positively; suggesting many see digital identity as increasingly embedded in services regardless of personal sentiment.

How to read this report

This report provides an updated view of the UK digital identity sector since the 2025 baseline study. We note four key points below.

Estimates versus observed data: Many of the economic figures presented such as digital identity related revenue, Gross Value Added (GVA), and employment are modelled estimates based on a combination of audited accounts, web data and proportional weighting across diversified firms. Where directly observed data is available (for example, number of firms in each taxonomy area, or external investment raised), this is identified in the relevant section. Estimates are signposted throughout the report.

Comparability with the 2025 baseline: The majority of measures in this report are directly comparable to the baseline (e.g. firm count, taxonomy classification, and location). However, some figures have been revised (as set out in Section 2.2). Further, an expanded consumer survey sample (3,561 to 5,658) with weighting has been deployed, alongside a revised set of consumer use cases, and improved data coverage on the supply side. Where comparisons are drawn, they are caveated accordingly.

Causality and interpretation: Several findings (for example, the modest reduction in sectoral headcount, the rise in international revenue share, and the broadening of provider offerings) may have multiple explanations and vary between firms. Where the report offers an interpretation, this is framed as one of several possible drivers rather than a firm attribution.

Scope and remit: This is an independent market assessment and does not analyse the impact or potential impact of policy intervention. Where policy developments are referenced (including the Data (Use and Access) Act 2025, the Digital Verification Services Trust Framework, and recent announcements regarding a national digital ID), they are noted as context for the market analysis.

SECTION 01

1. Introduction & background

1.1 Introduction

The Office for Digital Identities and Attributes (OfDIA), part of the Department for Science, Innovation and Technology (DSIT), has commissioned Perspective Economics and Survation to conduct an updated study of the digital identity sector in the UK. This research provides an annual update to the Digital Identity Sectoral Analysis 2025 report, and explores growth, adoption, innovation, and consumer attitudes to digital identity.

The baseline study (2025) was the first overarching assessment of the UK's digital identity ecosystem and highlighted the breadth and capacity of the products and services that underpin digital identity. It also demonstrated the economic scale of the sector in the UK, with 266 providers directly generating in excess of £2.1bn in annual revenues, £888m in Gross Value Added, and employing over 10,200 individuals in the UK through their digital identity solutions.

Since May 2025, there have been several policy announcements and developments relevant to the digital identity ecosystem. These are noted in this report as context for the market analysis that follows, but the report does not attribute market development in relation to these announcements or policies.

- In May 2025, Government Digital Service (GDS) commenced its formal engagement with the technology sector in designing and developing the proposed GOV.UK Wallet, as part of the wider Blueprint for Modern Digital Government.
- In June 2025, the Data (Use and Access) Act 2025 received Royal Assent. OfDIA also published the final 'gamma (0.4)' Trust Framework and the initial right to work, right to rent, and DBS Supplementary Codes in June 2025. In December 2025, the Digital Verification Services Trust Framework (DVSTF) was placed on a statutory footing.
- In September 2025, Prime Minister Sir Keir Starmer announced a national digital ID scheme.
- In October 2025, the digital HM Armed Forces Veteran Card launched in the GOV.UK One Login app, as the UK Government's first 'digital credential', with over 15,000 downloads to date. GDS has also started private testing for the digital driving licence in partnership with the Driver and Vehicle Licensing Agency (DVLA).
- In October and November 2025, industry and civil society groups engaged with the proposed national digital ID scheme through a series of position papers, feedback, and written evidence. This includes contributions from techUK, the AVPA, Yoti, and the Digital Poverty Alliance.
- In March 2026, the Cabinet Office launched a public consultation seeking views on a proposed national digital ID system. This closed on 5th May 2026, to be followed by a 'People's Panel on Digital ID'.

As such, this research recognises that the digital identity ecosystem should not be viewed as a single product or a binary debate. It is a diverse ecosystem with deep capabilities, established standards and accreditation, and international recognition. We note that policy announcements, public sentiment, market structures, and international competitiveness can shape this market. However, this market assessment aims to capture and reflect the reality and breadth of company activity, highlighting areas of strength and opportunity, as well as considering structural challenges with regards to use, adoption, and scaling.

This updated research therefore recognises and explores:

- What the digital identity ecosystem provides to customers and users, through the development of a market taxonomy, and review of products, services, solutions and use cases provided by the digital identity sector.
- An assessment of demand and supply, considering what the market provides commercially (including a review of the size and scale of the UK's private digital identity sector), in addition to domestic and international demand across a range of public and private sector use cases.
- How policies, legislation and regulation, standards and accreditation are shaping the market. Digital identity can involve verification or attribute checks on individuals across a range of markers such as age, employment, or immigration status. It can also involve advanced data science, including estimation techniques, linkage, or attribute verification across a range of financial and population datasets, and use of physical or facial checks. New use cases continue to become embedded such as social media age gates, mobile driving licences, identity verification for company directors, and continue to evolve. We explore the range of policies, legislation, regulation, and standards shaping the underlying market.
- Public attitudes towards the use of digital identity, including current and existing adoption, how views or adoption many vary across a range of use cases, and sentiment towards new and emerging policies and proposed uptake of digital identity overall.

This research aims to provide industry, policy-makers, and the public with updated intelligence and statistics regarding the size, scale, potential, and uptake of the digital identity ecosystem.

1.2 Methodology

Overview of Study Methodology

As set out in the baseline research published in 2025, we recognise that defining and measuring the Digital Identity ecosystem requires several methodological considerations. Further, as with any sectoral classification, definitions and scope may be considered subjective or contested by stakeholders. This study seeks to capture the breadth of market activity and includes a taxonomy and overarching definition for understanding digital identity provision in the UK.

This document reflects the research team's **best estimate of firm level activity in the UK relating to digital identity provision**, based upon review of extensive data sources, definitional and taxonomy assessment, extensive review and analysis of known providers (such as those included within the Digital Verification Services Trust Framework (DVSTF), and identification of similar providers across the UK economy.

The UK's digital identity sector, like other technology markets (such as the cyber security sector measured in the DSIT Cyber Security Sectoral Analysis), lacks a formal Standard Industrial Classification (SIC) code. This necessitates the development of a robust definitional framework to identify and measure relevant market activity.

The research approach continues to combine two key scoping considerations with a multi-stage methodology. These include a high-level definition developed by OfDIA and industry consultation to establish clear boundaries of what constitutes 'digital identity' as set out in Section 2.2; and functional scope whereby firms must be UK-registered, commercially active, and provide digital identity products or services with identifiable revenue or employment.

For market analysis, the research methodology continues to include:

- **Desk review and definitional scoping**: A comprehensive review of trust framework providers, industry events, and an initial web review to identify provider terminology and service offerings.
- **Identification of providers**: Review of over 1 million active UK company descriptions (with more than one employee), and use of web data review to develop an initial longlist with relevancy scoring and filtering.
- **Taxonomy development**: The use of stakeholder workshops to validate definitional scope and to create and refine a digital identity sector taxonomy (see 'Defining Digital Identity' section).
- **Market shortlisting**: All firms were matched against Companies House and web data, reviewed to confirm active status, and included in a final dataset for analysis and enrichment.
- **Data enrichment**: The research team has used web data, company accounts, and proprietary datasets to develop a digital identity sectoral dataset, including key measures such as registered entity, size, location, revenue, employment, investment, and description data.
- **Market analysis**: This document sets out an economic assessment of sector revenue, employment and Gross Value Added (GVA). This report presents an updated view on market size and definition, providing a snapshot of the UK's digital identity landscape. This also includes additional coverage on the ecosystem analysis, with further data regarding supply chains, partnerships, routes to market, and specific product and service offerings.

In addition, Chapter 4 includes a Consumer Survey on Digital Identity (conducted by Survation in November 2025, with 5,658 responses), with a full UK resident population sample, and additional sample boosts for specific groups of interest[1]. This builds upon previous survey work at baseline; however, this survey is also weighted based on derived variables from the ONS for age, sex, region, household income, qualifications, employment status, socioeconomic group, and ethnicity to provide further insight into consumer views and adoption.

1.2.1 Consistency with the Baseline Study

Market Analysis: The market analysis methodology is broadly retained from the baseline study, ensuring consistency in how providers are identified, classified, and measured. The research continues to draw upon web data, Companies House filings, proprietary datasets, and automated and manual review of providers to estimate firm-level and digital identity related revenue, employment, and Gross Value Added. Where methodological updates have been made (as set out in below), these are clearly identified to support interpretation and transparency and improve the findings from the study.

Definitional Scope: The high-level definition and taxonomy developed during the baseline remains in use for this updated study. This enables time-series comparison and ensures that the scope of what constitutes 'digital identity' provision remains consistent. All 275 firms identified in this study have been assessed against the same definitional criteria. As noted in Section 2.2, the taxonomy has been expanded slightly to include 'verification security' as a sub-category within Identity Verification, reflecting the growth and emerging coverage of solutions to counter deepfakes and biometric injection attacks.

Consumer Survey: The consumer survey has been updated and expanded for this wave, with several improvements intended to strengthen the reliability and relevance of findings. These include an increased sample size (from 3,561 to 5,658 respondents), the introduction of data weighting to improve population level estimates, and a revised set of use cases to better reflect the current digital identity landscape. As a result of these changes, direct time-series comparisons between the baseline and updated survey are limited

[1] These include UK residents aged 18+ with: a disability expected to last 12 months or more; no UK/EU passport or driving licence; those with low digital skills according to the Lloyd's Digital Index; or those have legally changed their name or gender

to measures such as self-reported understanding, where question design remained consistent. Where comparisons are drawn, these are clearly caveated. Further detail on survey design changes is set out below and in Section 4.1.

1.2.2 Methodology Updates

Improved Data Coverage: This updated study has used improved data coverage across several areas. The research team has expanded the use of web data and natural language processing (including LLMs) to classify firms against the taxonomy, enabling more granular identification of products, services, and use cases. We have also reviewed over 4,700 unique product and service markers across the 275 providers, compared to approximately 3,800 in the baseline. In addition, the financial data has been strengthened through improved matching against Companies House filings and datasets, and through the identification of additional firms filing full accounts with geographic revenue breakdowns. This has improved the robustness of revenue, GVA, and employment estimates.

Updated Consumer Survey: The consumer survey conducted by Survation in November 2025 includes several design improvements relative to the baseline. These are intended to strengthen the quality and representativeness of findings, but they also limit direct comparability on some measures. Key changes include an increased sample size, providing greater statistical power across demographic sub-groups; the introduction of data weighting by age, sex, region, income, qualifications, employment status, socioeconomic group, and ethnicity, improving population-level estimates; a revised set of use cases; and the adjustment of reported digital identity usage questions within the baseline. These improvements mean that the updated survey provides a more robust and representative picture of current consumer attitudes and usage, but direct comparison with the baseline is limited to measures where question design was consistent, such as self-reported understanding of digital identity.

SECTION 02

2. The UK Digital Identity Market

2.1 Introduction

In the baseline study (published in May 2025), the research set out several novel findings regarding the size, scale and activity within the digital identity market. This study provides a time-series analysis one year on.

2.2 Taxonomy & Definition

The UK's digital identity sector, like other technology markets (such as the cyber security sector measured in the DSIT Cyber Security Sectoral Analysis), lacks a formal Standard Industrial Classification (SIC) code. As part of the baseline research, the research team developed a market definition to help identify and assess relevant market providers:

'The digital identity sector provides solutions for creating, managing, and verifying digital representations of individuals. This enables secure, trusted, and effective proof of identity and attributes across online and in-person interactions, and a way to gain verified access to products and services.'

(DSIT Market Definition, 2024)

Further, the Office for Digital Identities and Attributes (OfDIA) definition of digital identity also encompasses the breadth of how this works for end-users, with a focus on how digital identity can span domains such as identity issuance, verification, assurance, and data services and minimisation:

"A digital identity is a digital representation of your identity information, like your name and age. At your request, it can also contain other information about you, like your address, or biometric information, like a fingerprint or face scan. It enables you to prove who you are without presenting physical documents." [2]

Further, the research team also considered a range of practical and wider applications for digital identity solutions that help to inform the definitional and scoping aspect of this research. This refers to where providers can help customers and individuals through:

- Creating, managing, and verifying digital identities, attributes and credentials for individuals and organisations.
- Providing authentication, authorisation and biometric solutions for secure access to digital services.
- Providing identity verification services to establish the authenticity of digital identities.
- Enabling regulatory and compliance checks, such as background screening, right to work verification, and DBS checks.
- Developing systems that give users control over their digital identity and data sharing.

The purpose of a sectoral taxonomy is to explore areas of product and service provision to help understand the strengths and capabilities of the market. The taxonomy was developed through identifying and reviewing digital identity firms in scope and analysing web data regarding product and service provision.

[2] GOV.UK (2024) 'Enabling the use of digital identities in the UK'. Available at: https://www.gov.uk/guidance/digital-identity

This involved extraction and analysis of hundreds of unique keywords, and a workshop with OfDIA and the wider research team to identify areas of relevance, market knowledge, and policy context. Each company identified can offer multiple products or services, tagged against the taxonomy.

The taxonomy comprises five primary categories, each representing distinct but aligned capabilities across the identity lifecycle.

This begins with foundational stages, such as creating or using a digital identity and configuring which attributes can be shared.

It then moves to identity verification and attribute verification, which involves confirming an individual's identity and validating key attributes or checks relevant to the process.

The taxonomy also includes Trust Services (aligned to a 'trust service provider' definition). This typically includes eSignatures, certificates for website authentication, electronic seals and time stamps.

We also consider the role of identity data and intermediary providers e.g. ensuring access to relevant data for checks, risk, fraud, credit, and analytical purposes.

Table 2.1. Overview of a UK Digital Identity Taxonomy

Digital Identity				
Identity Foundations	**Identity Verification**	**Attribute Verification**	**Trust Services**	**Identity Data and Intermediaries**
Identity Issuance	Document Based	Age Assurance	Digital Signatures (eSignatures)	Data Brokerage
Identity & Consent Management	Biometrics & Liveness Detection	Professional & Credential Verification	Certificates	Orchestration and Interoperability
Digital Wallets	Knowledge Based Verification	Background Screening	Authentication	Risk, Fraud & Credit
Identity Services	Social Verification (Vouching / Proofing)	Financial & Address Verification	Governance & Compliance	Analytics & Insights
Identity Standards & Protocols				

The taxonomy is summarised below, and set out in full in Annex A:

- **Identity Foundations:** infrastructure for creating, managing and storing digital identities, including Identity Issuance, Identity and Consent Management, and the wider role of Digital Wallets and Identity Services.
- **Identity Verification:** technologies and processes to verify individual and organisational identities, including Document Validation, Biometrics, Liveness Detection and Verification Security, Knowledge-Based and Social Verification.
- **Attribute Verification:** technologies and processes to validate specific characteristics or credentials, including Age Assurance, Professional and Credential Checks, Background Screening, and Financial and Address checks.
- **Trust Services:** services to provide trust in digital transactions, including Digital Signatures, seals and certificates, the role of website authentication, and wider governance and compliance tools (e.g. time stamps, registered delivery services).

- **Identity Data and Intermediaries:** services enabling data flow and integration, including data brokerage, orchestration, risk, fraud and credit data, and wider analytics.

This taxonomy is broadly retained for use[3] within this updated study to enable time-series analysis. This seeks to capture the main areas of product and service provision (by count and scale) and ensure that sufficient breadth of provision can enable the identification of as many relevant providers as possible. However, as we explore new products and services in Section 2.4, we set out novel areas that may warrant further tracking or embedding within an updated taxonomy in future.

It is worth noting that taxonomies in technology sectors require ongoing refinement and can involve subjectivity regarding definitions and scope. The research team reviewed several data sources to understand how providers operate within the market and conducted an industry workshop in October 2024 to further develop and refine the methodology. This approach enables our analysis to explore the current market in a way that can be used by industry and policymakers. This taxonomy represents a point-in-time assessment that should continue to evolve alongside the digital identity ecosystem.

2.3 Number of Digital Identity Firms

We estimate that, as of January 2026, there are currently 275 firms providing digital identity products and services registered within the UK. This is a net increase of nine firms (+3%) since the baseline study. We find 233 'dedicated' firms (firms that only or mainly provide digital identity related products or services), and 42 'diversified' firms (firms that provide digital identity among other products or services, to the extent that the study captures the proportional activity only i.e. number of people working in a digital identity role only).

We identified 266 firms within the baseline study. All firms have been reviewed with respect to active web presence (i.e. the research team has confirmed the website is active and appears to be trading) and active Companies House registration status. We note that 20 firms have since dissolved or entered liquidation or administration since the baseline study. A further seven firms appear to have inactive websites with limited evidence of current trading. As such, 27 firms (10%) have been removed from the baseline list. This is broadly in line with business closure rates across the UK economy (9.8% of businesses closed in 2024[4]) The remaining 239 firms (90%) have been retained in the sample, following review of wider mergers or changes in business structure. Further, the research team has undertaken additional desk review, review of business and web data (over 1m UK companies), firms actively involved with the Digital Verification Services Trust Framework (DVSTF), and wider signals such as public frameworks, social media, international firms establishing a UK office, and wider registration of new startups to identify 36 firms to add to the dataset of digital identity firms.

[3] As part of this research, review of market provision has revised Biometrics and Liveness Detection to include additional coverage for Verification Security e.g. firms involved in assessing and preventing biometric injection attacks and countering deepfakes e.g. IDTechwire (2025) 'New Standard Introduced for Assessing Biometric Injection Attacks' Available at: https://idtechwire.com/new-standard-introduced-for-assessing-biometric-injection-attacks/; and iProov (2025) 'iProov is First Biometrics Vendor to Demonstrate Deepfake Resilience, Under New NIST Digital Identity Requirements) Available at: https://www.iproov.com/press/nist-digital-identity-requirements-first-biometrics-vendor-demonstrating-deepfake-resilience

[4] ONS (2025): 'UK Business: Activity, Size and Location (2025)' Available at: https://www.ons.gov.uk/businessindustryandtrade/business/activitysizeandlocation/bulletins/ukbusinessactivitysizeandlocation/2025 and ONS 'Business Demography (2024)': Available at: https://www.ons.gov.uk/businessindustryandtrade/business/activitysizeandlocation/bulletins/businessdemography/2024

Table 2.2. Review of Digital Identity (2024) Baseline and Update (2025)

Stage:	Count
Baseline Study	266 firms
Removing Dissolved or Inactive Firms, or firms no longer offering relevant products or services	Less 27 firms
Remain	239 firms
Identify and add newly registered firms, or firms appearing to now offer relevant products or services	Add 36 firms
Total Estimate (January 2026)	**275 firms**

We also note that identification and enrichment processes to explore how firms operate in the market continue to improve over time, in addition to how firms may discuss and offer digital identity products or services. As such, a firm may have had a more limited presence in previous years in the market but subsequently evolved its offering to include digital identity as aligned to the research parameters. This means that this research may continue to identify both newly registered firms in the market, inward investment from international firms into the UK, and existing firms that appear to meet the agreed definition and taxonomy.

2.4 Products and Services

Within this study, we consider the products and services offered by providers mapped against the taxonomy. For example, a firm may offer digital verification and trust services. Further, there are several partnerships and collaborations within the market, where vendors offer a shared portfolio of identity solutions to customers.

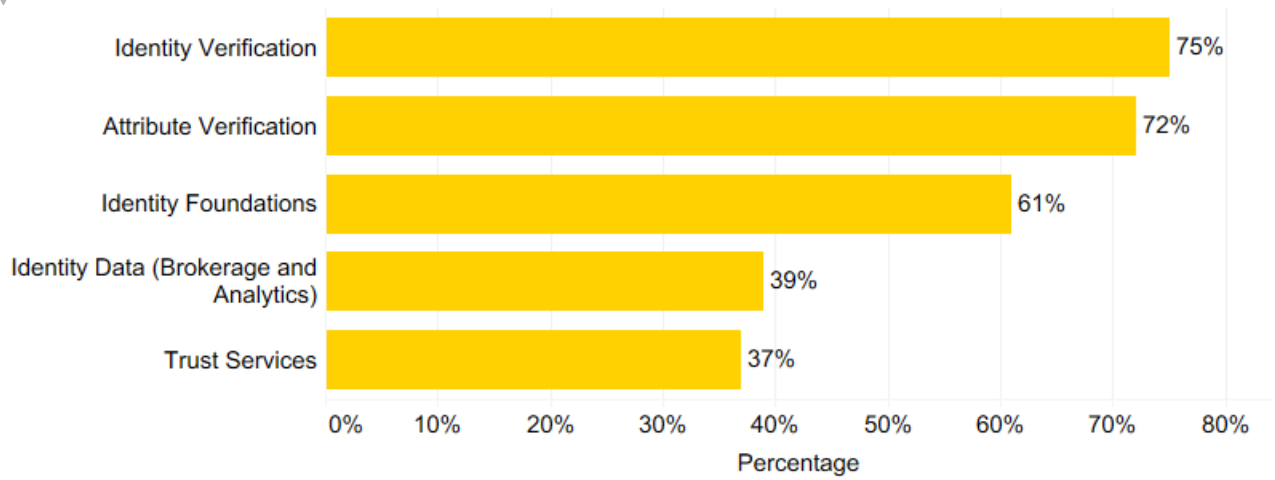
Within this updated study, we have reviewed additional web and text data for each firm, and classified firms using industry-leading LLMs. Given the breadth of provision (where providers offer a range of solutions), we classify companies using multiple tags to provide greater granularity regarding provision.

Within this study, we have reviewed over 4,700 unique product and service markers against the 275 providers identified. We subsequently apply a taxonomy and sub-taxonomy tag for each provider where sufficient trading data is identified and classified. As identified within the baseline study, the digital identity sector contains extensive breadth and expertise, with providers often providing multiple solutions in areas such as background checks, age assurance, eSignatures, and document and digital verification support.

Further, the sector is also considered highly collaborative, with several providers offering partnerships and data sharing across vendors to maximise interoperability, consumer ease of use, and data coverage for verifying individuals.

We set out the estimated proportion of firms offering products or services aligned to the taxonomy and sub-taxonomy areas in Figure 2.1 and Figure 2.2 below.

Figure 2.1. Taxonomy Coverage by Category



Source: Perspective Economics (n = 275)

Figure 2.1 highlights that:

- **75% of the providers are involved in identity or attribute verification**. This is a slight increase from the baseline study (69%), reflecting the emphasis upon digital identity verification techniques.
- **Over six in ten (61%) providers** are involved in issuing usable and reusable digital identities or supporting with identity data consent and privacy management. This is an increase from 51% in the baseline study.
- **Approximately two-fifths (39%) provide identity data or analytics** e.g. data brokers sharing identity data for supporting with financial transactions, etc. This is a notable increase from the baseline (24%), reflecting the increased use of data brokerage and sharing for enabling digital verification.
- **37% offer solutions aligned to 'trust services'** (i.e. offer simple, advanced or qualified solutions such as digital signatures, seals and certificates), an increase from 33% in the baseline study.

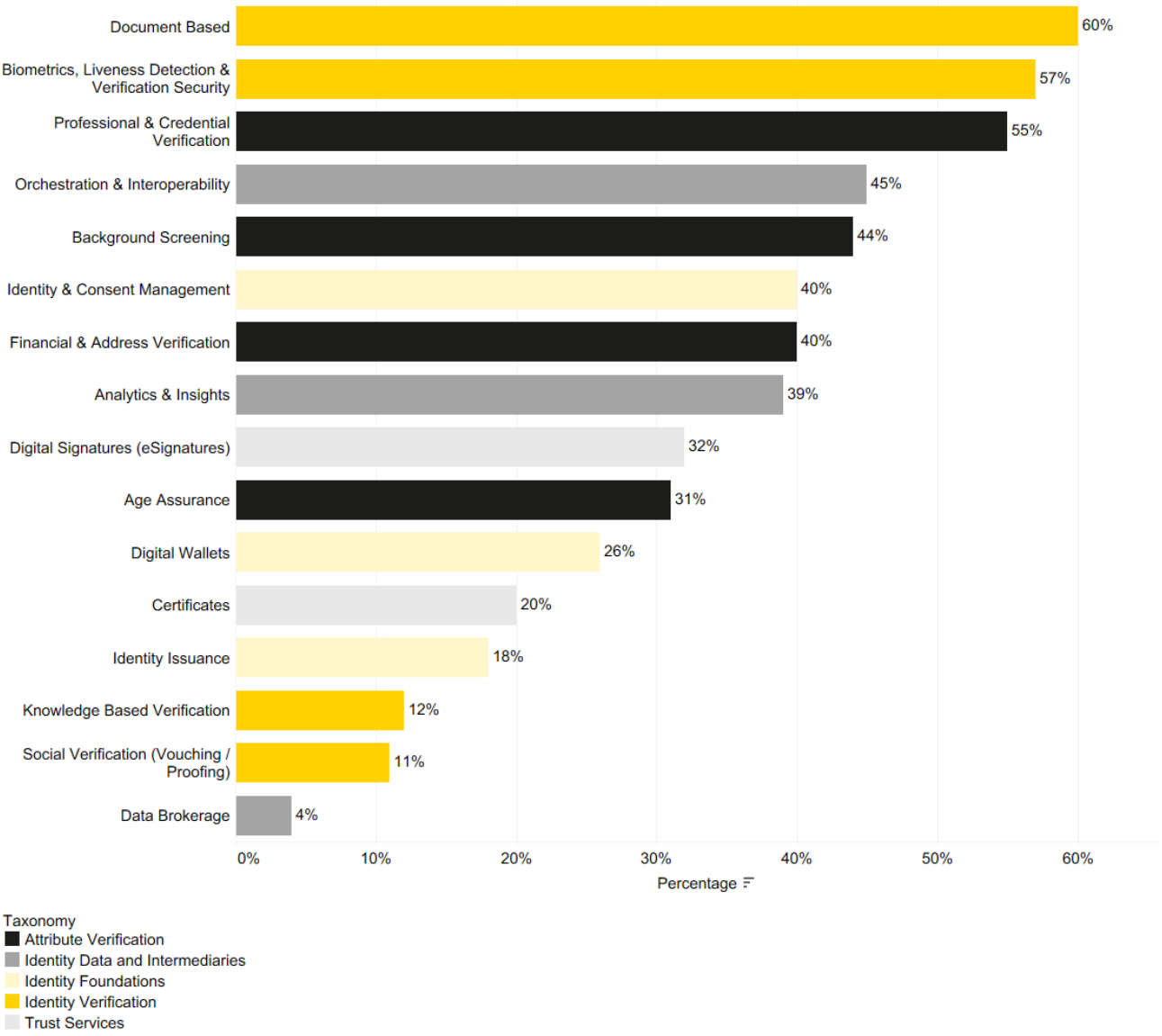
We note that all areas have seen an increase in coverage since the baseline study, which continues to highlight that several digital identity firms work collaboratively and extensively to support their customers with a range of use cases (explored in Section 3).

Figure 2.2 provides additional granularity for the percentage of providers that mention providing products or services aligned to each sub-category. This highlights that document-based verification (60%) remains the most provided approach cited by providers (compared to 54% at baseline). This is followed by biometrics, liveness detection and verification security (57% compared to 45% at baseline). The research team has identified a notable emergent uptick in the number of providers involved in biometrics and liveness detection building new solutions to counter deepfakes, and counter injection attacks (e.g. false video or audio feeds to circumnavigate identity checks). As such, this sub-category has expanded to include 'verification security' as an important component of the industry. This also highlights the increasing complementarity between digital identity technologies, and wider AI and cyber security provision.

In the UK market, we note a significant increase in the number of firms mentioning support with professional and credential verification (55% from a baseline estimate of 28%) and background screening (44% from a baseline estimate of 29%). This may be driven by increased provision from firms offering several layers of background and wider credential checks as part of wider right to work and pre-employment checks. This

research identifies almost 100 firms operating in the UK market that appear to support with right to work checks on behalf of UK employers, either directly, or through broader support with onboarding. The baseline study noted how the importance of age assurance as a market offering. The updated data suggests that the proportion of firms offering support with age assurance has also increased from 23% to 31% in the last twelve months, reflecting increased provision amidst implementation of age checks as part of the Online Safety Act.

Figure 2.2. Taxonomy Coverage by Sub-category

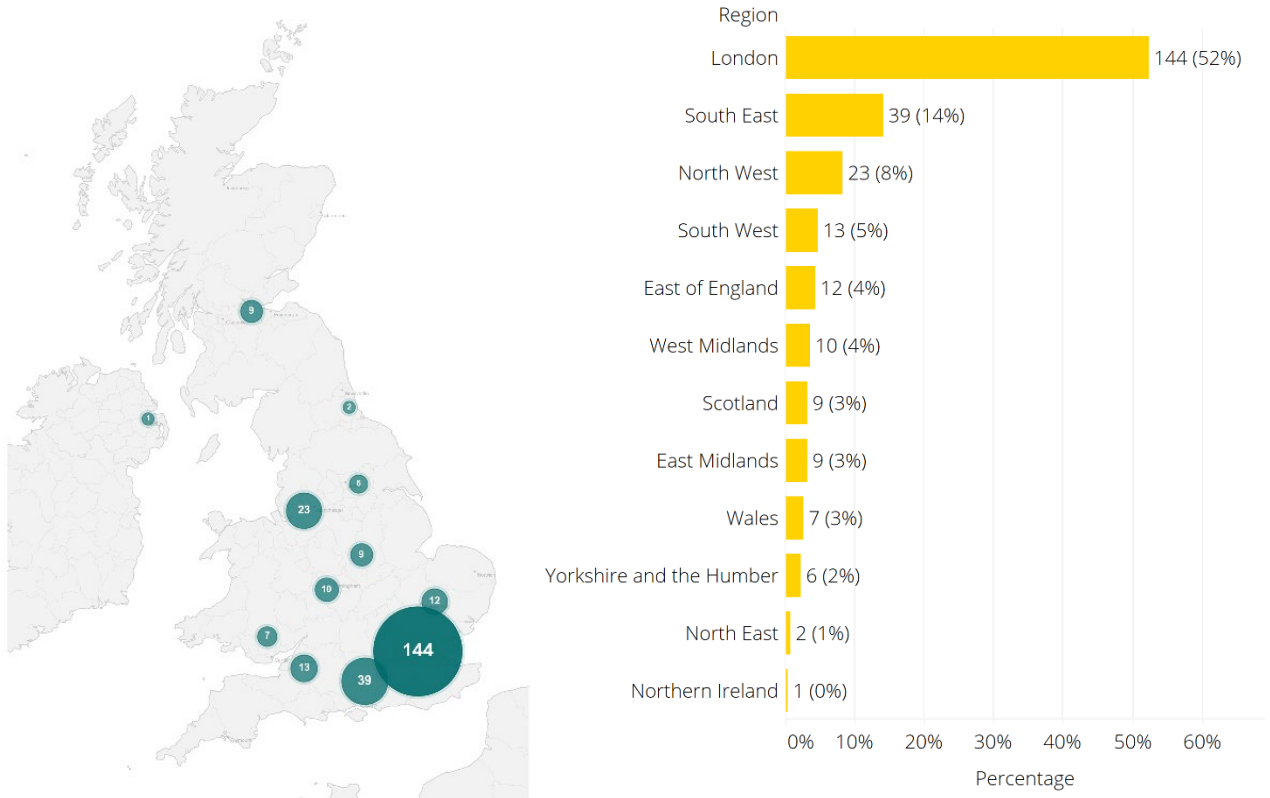


Source: Perspective Economics (n = 1,467 mentions of product or service provision mapped against the sub-taxonomy across 275 providers). This suggests an average of five taxonomy 'matches' per firm.

2.5 Location

Figure 2.3 sets out the registered UK location of the 275 digital identity firms identified.

Figure 2.3. Registered Location of UK Digital Identity Firms



In line with the previous baseline, just over half of firms are registered in London (52%) followed by the South East (14%). However, the data also suggests firm level activity in the North West (which accounts for 8% of firms, but 21% of the sectoral revenues as explored in the next section).

Further, the research team has identified domestic and global office locations for all firms in scope. This data suggests that the majority of firms are founded or headquartered in the UK (73%, 202 firms), and over one in four (27%, 73 firms) are founded or headquartered internationally, but have a UK presence via a registered entity. Further, of the 202 UK headquartered firms, 73 (36%) appear to have at least one office outside of the UK.

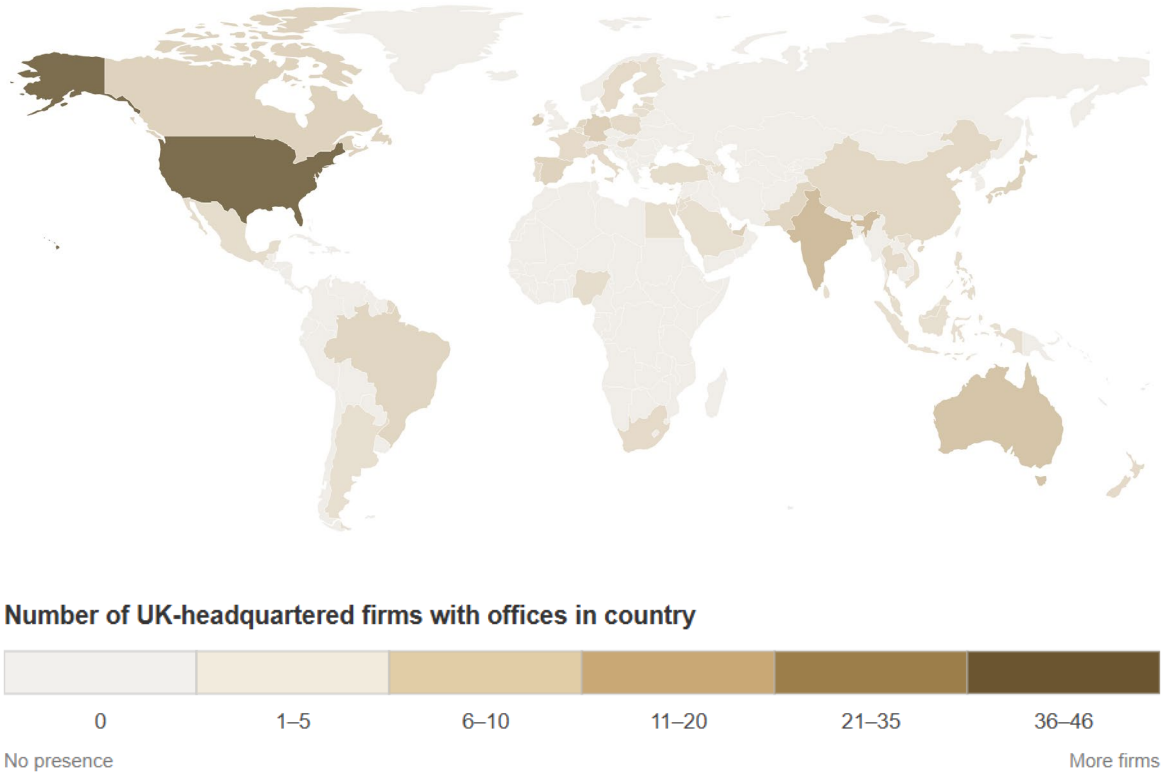
This data continues to emphasise how highly internationalised the digital identity market is within the United Kingdom. This includes its key role as an export market (explored subsequently with respect to domestic and international revenues), and the attractiveness of the UK for foreign direct investment and international trade among multinational digital identity firms.

As with the baseline study, the majority of internationally headquartered firms are based in the United States (45) with the remainder from countries such as Switzerland, France, Israel, Australia, the Netherlands, and twelve other countries.

For the 73 UK-headquartered firms with a physical presence in international markets, we find 214 offices across 51 countries. This includes 30 UK headquartered firms with a European Union / European Economic

Area (EEA) (41%) presence, as well as 46 firms with a presence in the United States (63%), 15 in India (21%), 13 in Singapore (18%), 12 in Australia (16%), and 8 in the United Arab Emirates (11%).

Figure 2.4. UK headquartered companies with a physical presence in other countries



Source: Perspective Economics (n = 73). Please note a darker colour denotes greater office count.

2.6 Economic Estimates:

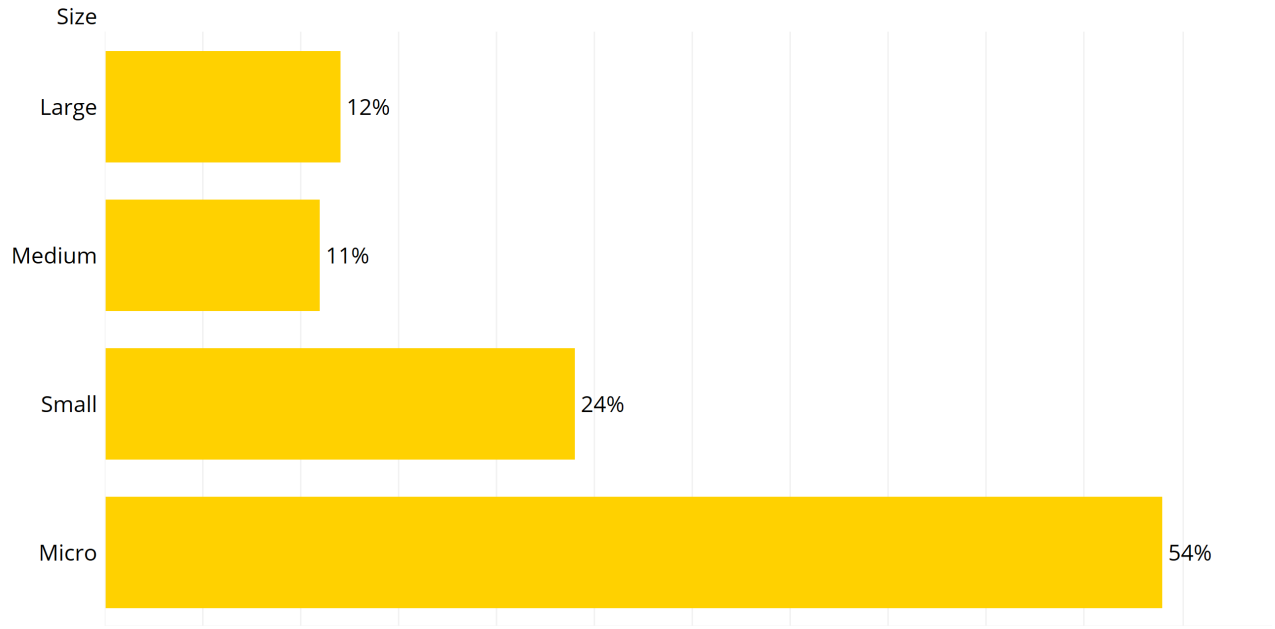
This section explores digital identity related revenue, Gross Value Added (GVA), and employment. It also explores how the sector has changed since the baseline study. Please note that the figures presented in this section are estimates, derived from a combination of Companies House filings, audited accounts, third party and web datasets, and proportional allocation for firms where digital identity activity sits within a wider business.

As established in the baseline, the digital identity ecosystem comprises firms of varying maturity, from long-standing providers in areas such as background screening and data brokerage, to newer entrants in identity verification and trust services that have emerged since the early 2000s. More recently, the ecosystem has also expanded into areas such as age assurance, liveness detection, and behavioural analysis, and continues to evolve as new technologies shape how identity is and can be generated, verified, and trusted online. The ecosystem spans both established and emerging capabilities, supported by deep domain expertise across legal, regulatory, and technical dimensions. The following analysis sets out the aggregate size and scale of the ecosystem as of January 2026 and explores how this varies across providers.

This section examines the size distribution of these firms based on their UK operations. As set out in the baseline, we also recognise that many firms will have varying global and UK footprints, e.g. a multinational firm may have a 'large' global presence with thousands of employees, but a small research and development office in the UK. Figure 2.5 highlights a relatively similar size composition to that of the baseline study, with

large firms (typically over 250 employees) representing 12% of providers (same as baseline), 11% medium (compared to 14% at baseline), and 78% small or micro (compared to 74% at baseline).

Figure 2.5. Digital Identity Companies by Estimated UK Size



Source: Perspective Economics (n = 275)

As set out in the baseline report, the UK is an attractive location for major international players in digital identity, with 20% of firms identified being globally 'large' enterprises. These multinationals maintain varying UK footprints, from dedicated research and development facilities to full-scale service delivery operations.

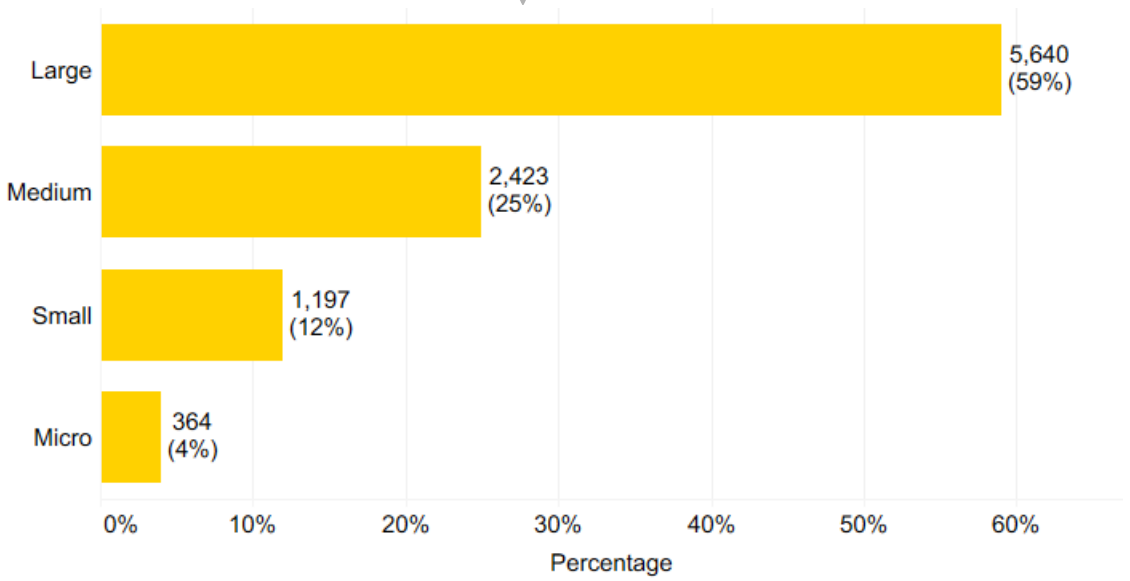
Estimated Employment:

We estimate that there are **9,624 Full Time Equivalents (FTE)** working in a digital identity related role in the UK across the 275 firms identified. Most of these roles (82%, 7,934) are employed within 'dedicated' firms[5] emphasising a specialist market.

This reflects a decrease in sectoral employment of 6% since the baseline study (n = 10,246 FTEs). As set out in Figure 2.6, we find the majority of this reduction has been recorded in large firms (from 6,017 FTEs at baseline to 5,640 FTEs (-6%)) and medium firms (from 2,637 FTEs to 2,423 FTEs (-8%)). Several of the largest individual reductions relate to firms where digital identity headcount is estimated proportionally as part of wider UK operations, and where broader corporate restructuring may be taking place at a firm level, rather than digital identity activity only. Collectively, employment within small and micro firms has had a small reduction in the past year (from 1,592 FTEs to 1,561 FTEs (-2%)).

[5] The research team has also reviewed company and accounts data (Companies House) to estimate relevant headcount in diversified firms (e.g. large consultancies with a digital identity offering).

Figure 2.6. Digital Identity Headcount by Size



Source: Perspective Economics (n = 9,624)

Review of employment data highlights a range of potential factors that may be shaping employment within the sector. These include:

- **Market consolidation**: As noted in the baseline study, in recent years, we found a number of examples of established security and data companies acquiring UK identity verification specialists, and a range of public-private collaborations formed to scale digital identity services. For example, Entrust's acquisition of Onfido, and LexisNexis Risk Solutions (part of RELX)'s acquisition of IDVerse. As larger firms integrate, this may in turn lead to rationalisation in areas such as compliance, engineering, and sales.
- **AI and automation:** Across the broader tech sector globally, 2025 was a challenging year. It is estimated that global tech sector layoffs surpassed 244,000 roles in 2025 alone.[6] AI and automation, particularly where tooling can replace or reduce demand for roles in areas such as data processing, administrative checks, and customer support have all been cited as key reasons for company-level layoffs. In digital identity specifically, moving from manual checks to the use of AI-driven document and liveness checks may reduce demand for human teams, particularly in larger firms.

Further, increased use of AI for coding and engineering development may also place downward pressure on demand for engineers and technical staff. However, we note that several digital identity providers have used AI and automated processes within solutions to reduce time and burden for their end customers for decades, particularly in document scanning, and automated verification processes.

Estimated digital identity related employment can be segmented by a range of other variables such as region, international and domestic markers as explored below.

Estimated Employment by Region (Registered Level):

Employment remains concentrated within London-registered firms (37%); however, this represents a reduction from the baseline study (42%), with London-based FTEs falling from 4,323 to 3,537. The South East has emerged as a more significant cluster, increasing from 15% to 22% of sectoral employment (from

[6] RationalFX (2026) 'Global Tech Sector Layoffs' Available at: https://www.rationalfx.com/forex-brokers/global-tech-sector-layoffs/

1,586 to 2,107 FTEs), while the North West has remained broadly stable at 17% (1,642 FTEs). This is broadly comparable to other studies, such as the DSIT Cyber Security Sectoral Analysis where 72% of employment (at a registered level) is based in London and the South East.

Beyond these three regions, the South West (8%), East Midlands (5%), and Yorkshire and the Humber (5%) have maintained consistent shares since the baseline. Wales has recorded a decline, falling from 6% (587 FTEs) to 3% (321 FTEs). Scotland, East of England, West Midlands, North East, and Northern Ireland continue to represent relatively small proportions of overall sectoral employment.

Table 2.3. Estimated Digital Identity Employment by UK Region (Registered Level)

Region	Estimated FTEs	Percentage of UK Digital Identity Employment
London	3,537	37%
South East	2,107	22%
North West	1,642	17%
South West	807	8%
East Midlands	496	5%
Yorkshire and the Humber	451	5%
Wales	321	3%
Scotland	128	1%
East of England	72	c. 1%
West Midlands / North East / Northern Ireland	63	c. 1%

Source: Perspective Economics (n = 9,624)

Estimated headcount by domestic and international marker

The UK continues to attract considerable interest from international firms operating within the digital identity ecosystem. International firms account for around 37% of estimated UK digital identity employment (3,583 FTEs), broadly consistent with the baseline study (38%, 3,863 FTEs). UK-headquartered firms account for the remaining 63% of sectoral employment (6,041 FTEs).

International employment remains primarily driven by US-headquartered firms, which account for approximately 74% of all international FTEs in the sector (2,647 FTEs) across a broad range of firms including Entrust, Ping Identity, Okta, Deloitte, and First Advantage. A further range of firms headquartered across Europe, including France, Ireland, Switzerland, and the Netherlands, as well as Israel, Japan and Australia

also maintain digital identity related operations in the UK, reflecting the sector's role as a significant market for international providers.

While the overall balance between domestic and international employment has remained stable, both categories have recorded modest reductions in absolute terms since the baseline, suggesting that the employment decline identified has been distributed relatively evenly across UK-headquartered and international firms.

Table 2.4. Estimated Digital Identity Employment by UK-founded or International Marker

	FTEs		Percentage
UK Headquartered	6,041		63%
International	3,583		37%

Source: Perspective Economics (n = 9,624)

Estimated headcount by taxonomy

Analysis of employment across the digital identity taxonomy categories highlights the breadth of service provision across the sector. As many providers operate across multiple taxonomy categories, figures below reflect the total number of FTEs employed within firms offering each capability, and as such firms may be counted across multiple categories.

Identity Verification remains the most prevalent capability across the sector, with 92% of estimated employment (8,825 FTEs) within firms offering some form of identity verification — an increase from 80% at baseline. Attribute Verification has also grown in prevalence, with 86% of employees (8,252 FTEs) now working in firms providing attribute verification services, up from 76%.

Identity Foundations (71%), Identity Data and Intermediaries (66%), and Trust Services (39%) account for significant but smaller shares of sectoral employment. The general increase in coverage across most taxonomy categories continues to highlight that providers are widening their offerings and operating across the taxonomy.

Table 2.5. Estimated Digital Identity Employment by Taxonomy (Multiple Fit)

Taxonomy (Multiple Fit)	FTEs	Percentage
Identity Foundations	6,815	71%
Identity Verification	8,825	92%
Attribute Verification	8,252	86%
Trust Services	3,755	39%
Identity Data and Intermediaries	6,359	66%

Source: Perspective Economics (n = 9,624)

Estimated Revenue and Gross Value Added:

In the most recent financial year (2024/2025), we estimate that total annual digital identity related revenue was **approximately £2,027 million across the 275 firms identified**. This relates to revenue attributable to digital identity activity only. This marks a reduction of £86 million (-4%) since the baseline study (£2,113 million across 266 firms).

However, this headline figure is influenced by a methodological refinement to one firm, whose baseline revenue estimate has been revised downward to reflect the nature of its workforce — which predominantly comprises part-time, casual workers engaged in age verification checks on a per-visit basis, rather than full-time salaried staff. This adjustment accounts for the majority of the headline decline. *Excluding this adjustment, estimated sectoral revenue among all other firms actually grew by approximately 4%.*

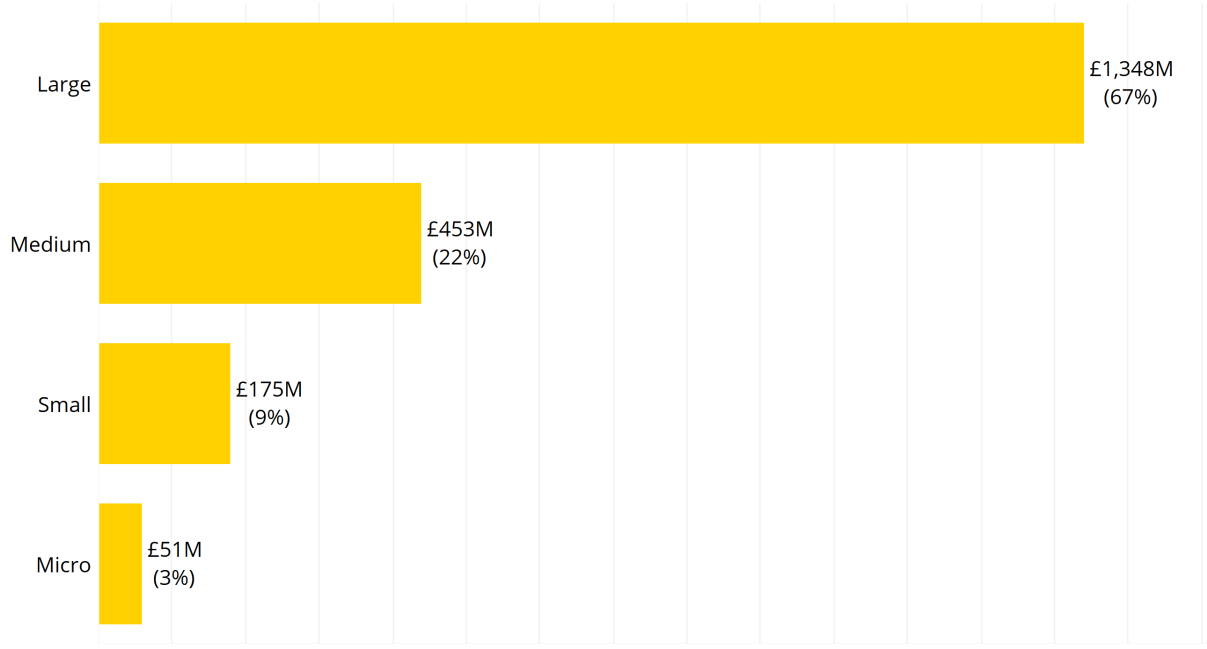
Across the wider dataset, more firms recorded revenue growth than decline: 124 firms grew by more than 2%, compared with 99 that recorded a reduction of more than 2%. A number of dedicated digital identity providers recorded strong growth, including firms operating in identity verification, behavioural analytics, and background screening. Conversely, several larger diversified firms recorded reductions in estimated DI-related revenue, in part reflecting the challenges of attributing digital identity activity within broader service offerings.

Revenue remains concentrated among a relatively small number of firms. For example, the largest ten firms by revenue account for approximately 51% of total estimated sectoral revenue, and the top twenty for 68%. This concentration is broadly consistent with the baseline and reflects the structure of the market, in which a small number of large providers operate alongside several specialist firms.

Estimated Revenue by Size

Revenue remains highly concentrated among large providers, which account for 67% of total estimated sectoral revenue (£1,348 million), consistent with the baseline (69%). Medium firms account for 22% (£453 million), while small and micro firms collectively represent 11% (£175 million and £51 million respectively). The share accounted for by small and micro firms has increased slightly since the baseline (from 9% to 11%), consistent with continued growth among newer and smaller specialist providers entering the market.

Figure 2.7. Digital Identity Estimated Revenue by Size



Source: Perspective Economics (n = £2,027m)

Estimated Revenue by Region

London remains the largest regional concentration of digital identity related revenue at £736 million (36%); however, this represents a reduction from the baseline both in absolute terms (from £847 million) and as a share of sectoral revenue (from 40%).

The North West has consolidated its position as the second largest regional hub, increasing from £405 million (19%) to £430 million (21%). The South East has also recorded notable growth, rising from £238 million (11%) to £294 million (14%), again reflecting the regional employment trends identified earlier in this analysis. The South West has remained broadly similar at £214 million (11%).

Wales suggests a reduction in estimated revenue, falling from £199 million (9%) to £144 million (7%). The East Midlands (6%), Yorkshire and the Humber (3%), and Scotland (1%) have maintained broadly consistent shares since the baseline. West Midlands, North East England, and Northern Ireland continue to account for less than 1% of sectoral revenue.

Table 2.6. Estimated Digital Identity Revenue by Registered Region

Region	Revenue	Percentage
London	£736m	36%
North West	£430m	21%
South East	£294m	14%
South West	£214m	11%
Wales	£144m	7%
East Midlands	£119m	6%
Yorkshire and the Humber	£52m	3%
Scotland	£21m	1%
East of England	£9m	0%
West Midlands	£8m	0%
North East	£1m	0%
Northern Ireland	<£1m	0%

Source: Perspective Economics (n = £2,027m)

International Revenue:

The research team has undertaken analysis of 28 dedicated digital identity firms that file full financial accounts with Companies House and provide a breakdown of annual revenue by geographic market. Firms filing abbreviated or micro-entity accounts are not required to disclose geographic revenue data, and as such this analysis is typically weighted towards larger and more established providers.

These 28 firms collectively generated combined digital identity related revenue of £1,105 million in the most recent financial year, accounting for approximately 55% of total estimated UK digital identity revenues. The revenue breakdown across international markets continues to demonstrate the global footprint and export strength of the UK's digital identity sector. Our analysis of combined known revenue for these providers suggests the following geographic distribution (where geography is provided):

- UK market: £419 million (38% of total revenue)
- European market: £259 million (23% of total revenue)
- US market: £206 million (19% of total revenue)
- Asia: £52 million (5% of total revenue)
- Rest of World: £145 million (13% of total revenue)
- Unknown / Not Disclosed (Variance): £24m (2%)

The data continues to highlight a highly internationalised sector, with c. 60% of revenue generated from international markets, an increase from 57% at baseline. Further, the EU/EEA has emerged as a larger destination market than the US for this sample of providers (23% vs 19%), compared with the baseline where the US accounted for 26% of revenue and Europe for 13%. This shift may in part reflect growing demand for digital identity services driven by EU regulatory frameworks, alongside the routing of EMEA revenues through UK based subsidiaries of international firms.

Among UK-headquartered firms in the sample, 56% of revenue was generated from international markets, reinforcing the export focus of medium and larger domestically grown providers. Among internationally headquartered firms operating in the UK, 31% of revenue was attributable to the UK market, with the remainder often generating intercompany revenue through their UK operations (i.e. the parent company investing in UK based research and development, engineering, and sales operations).

As this analysis reflects only those firms required to file full accounts, further research may be merited to explore international activity across the wider market, particularly among small and micro firms. However, this analysis does highlight that of the overarching c. £2bn market (by revenue), approximately a third (£661m) can be attributed to export activity.

Gross Value Added (GVA):

GVA is used as a measure of productivity (at a firm level, or above). It captures the sum of a firm's gross profit, employee remuneration, amortisation and depreciation. In this respect, any increase in GVA can highlight an improvement in the performance of a firm or a sector, as evidenced through higher profitability or enhanced earnings.

We estimate that total annual digital identity related GVA reached approximately £1,037 million across the 275 firms identified. This represents an increase of £149 million (+17%) since the baseline study (£888 million across 266 firms), suggesting a notable improvement in sectoral productivity despite the modest reductions in employment and revenue identified above. The majority of GVA (75%) remains concentrated within large firms (£782 million), broadly consistent with the baseline (76%). However, the share accounted for by medium firms has increased from 15% to 21% (£218 million), while small and micro firms have seen their combined share reduce from 10% to 4% (£29 million and £9 million respectively)[7]. The combination of

[7] However, we note that shifts in the distribution of GVA across size bands may in part reflect changes in size band classification between study periods, as firms grow, contract, or are reclassified, rather than necessarily indicating a change in underlying performance within a given size band.

increased GVA alongside a reduction in employment implies an increase in productivity per FTE across the sector. This is consistent with the broader dynamics identified in this analysis including consolidation, increased adoption of AI and automation, and a shift towards more capital and technology intensive business models.

Table 2.7. Estimated Digital Identity Gross Value Added by Size

Size	Estimated GVA	Percentage
Large	£782m	75%
Medium	£218m	21%
Small	£29m	3%
Micro	£9m	1%
Total	**£1,037m**	

Source: Perspective Economics (n = £1,037m)

GVA per employee:

Based on current employment estimates, we estimate that GVA per employee within the digital identity sector is approximately £107,800. This represents a significant increase from the baseline estimate of £86,600. The digital identity sector's GVA per employee is broadly comparable to the cyber security sector (£116,200) and the wider digital sector (£89,200), and approximately 46% higher than estimated UK workforce levels, confirming its role as a high productivity sector.

Table 2.8. Estimated Digital Identity GVA per employee and benchmarks

Sector	GVA per employee (change since baseline)
Digital Identity (2025)	**£107,800**
Benchmarks:	
Artificial Intelligence (2024)[8]	£137,000
Cyber Security (2025)[9]	£116,200
Digital Sector (All, 2023)	£89,200[10]

Source: Perspective Economics

[8] DSIT Artificial Intelligence Sector Study 2024 (published September 2025). GVA of £11.8 billion divided by 86,139 FTEs across dedicated and diversified AI companies.
[9] DSIT Cyber Security Sectoral Analysis 2025 (published March 2025). GVA per employee increased from £106,300 in 2024 to £116,200 in 2025, an increase of 8%.
[10] DSIT Economic Estimates: Digital Sector Annual GVA (2010 to 2024), published February 2026. Revised 2023 estimate of £168.5 billion GVA divided by 1.89 million filled jobs (DSIT Economic Estimates: Employment in the Digital Sector, April 2023 to March 2024). We note that the 2023 GVA figure was substantially revised upward from the previously published estimate of £153.5 billion. The 2024 provisional estimate of £177.2 billion GVA has not been used here, as the corresponding employment estimate of 1.77 million is based on Annual Population Survey data for which ONS accreditation was temporarily suspended in October 2024 due to data quality concerns.

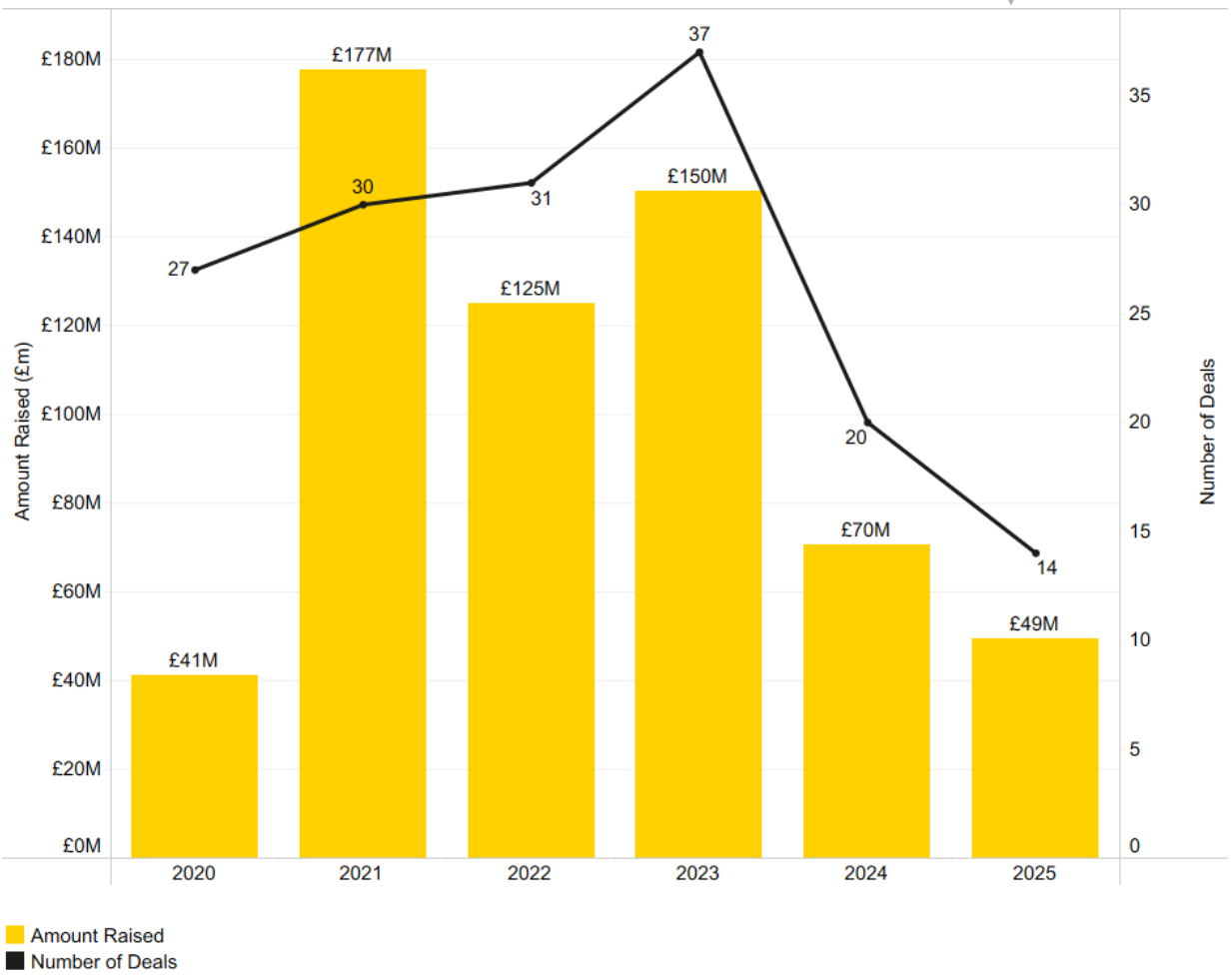
2.7 Investment Activity

This section draws upon the Beauhurst platform, which tracks announced and unannounced investments in high-growth companies across the UK. The research team has matched company registration numbers and company names identified within this analysis with the platform, identifying 277 fundraisings associated with 71 tracked companies. In other words, approximately three in every ten dedicated firms identified within the analysis has received some form of external investment or fundraising since incorporation.

Figure 2.8 sets out the annual investment for dedicated digital identity firms between 2020 and 2025. Between 2020 and 2023, the sector raised an average of £123 million per annum across an average of 31 deals. This period included a peak in 2021 (£177 million across 30 deals), driven by higher venture capital activity across the wider technology sector during this period, and strong performance in 2023 (£150 million across 37 deals). Investment activity subsequently declined significantly in 2024, with £70 million raised across 20 deals. However, we note this is an increased revised figure compared to the baseline estimate for 2024 (£46m).

This reduction is consistent with a tightening of venture capital across the technology sector more widely, where interest rates, macroeconomic uncertainty, and more cautious investor sentiment contributed to reduced deal activity since 2023.

Figure 2.8. Amount raised and number of deals by dedicated digital identity firms



Source: Perspective Economics analysis of Beauhurst data

At the time of analysis, in 2025, 14 deals have been recorded with a combined value of approximately £49 million. The largest individual deal in 2025 was a £30 million fundraising by TMT ID, a London-based firm that uses mobile network data to help organisations validate identities, detect fraud, and meet online safety requirements. This single deal accounted for approximately 60% of the total value raised in the year to date. Other notable disclosed investments included:

- A £1.7 million raise by Keyless[11], a London-based provider of privacy-preserving biometric authentication tackling injection attacks in advanced deepfakes; and
- A £1 million investment in Vouchsafe[12], a DVSTF-certified identity verification platform designed to tackle identity poverty by accepting alternative forms of evidence, including trusted referee vouches, for individuals who lack conventional identity documents.

The breadth of activity, from early-stage rounds to largest deals suggests that investor interest remains across the full digital identity ecosystem, albeit at reduced volumes compared to prior years. These trends are consistent with the wider UK venture capital landscape, where deal volumes and values have continued to contract from the 2021 peak, as increased interest rates and macroeconomic uncertainty have reduced late-stage activity. Across the technology sector more broadly, there has been a notable flight to quality and profitability, with investors increasingly focusing on companies with clear regulatory tailwinds and established revenue models.

Mergers and acquisitions

As noted in the baseline study, the digital identity sector has also experienced significant merger and acquisition activity in recent years, with established security and data companies acquiring specialist identity verification providers. Recent examples include the acquisition of Onfido by Entrust (April 2024) and the acquisition of IDVerse by LexisNexis Risk Solutions (late 2024), both set out in the baseline report.

This consolidation activity has continued into 2025, with several transactions directly involving UK-headquartered digital identity firms. In March 2025, The Citation Group acquired TrustID, a UK market leader in right to work and identity verification services. TrustID serves over 3,000 clients across recruitment, healthcare, hospitality, and professional services, completing more than 3 million right to work checks annually[13].

In October 2025, Ping Identity, a US-headquartered identity security platform backed by Thoma Bravo, announced the acquisition of Keyless[14]. As mentioned, Keyless had raised £1.7 million earlier in 2025, both raising external investment and subsequently acquired within the last twelve months. This highlights how innovative firms are attracting the interest of larger international platforms to help improve domains such as AI security.

In October 2025, GBG, a UK-headquartered global identity firm, acquired DataTools Pty Ltd, a leading provider of address validation and data quality solutions in Australia and New Zealand, for AUD $16 million

[11] EU Startups (2025) 'Keyless raises €1.9 million to tackle deepfakes'. Available at: https://www.eu-startups.com/2025/01/authentication-in-one-glance-keyless-raises-e1-9-million-to-tackle-deepfakes/
[12] Vouchsafe (2025) 'Vouchsafe raises £1m to build the next generation of identity verification' Available at: https://vouchsafe.id/vouchsafe-raises-1m/
[13] The Citation Group, 'The Citation Group acquires Digital Identity Verification Leader TrustID' Available at: https://thecitationgroup.com/news_article/the-citation-group-acquires-digital-identity-verification-leader-trustid/
[14] Thoma Bravo (2025) 'Ping Identity Strengthens Defence Against AI-Driven Impersonation with Privacy-Preserving Biometrics ' Available at: https://www.thomabravo.com/press-releases/ping-identity-strengthens-defense-against-ai-driven-impersonation-with-privacy-preserving-biometrics

(£7.9 million) in October 2025, extending its identity data capabilities in the region[15]. These transactions are consistent with the broader consolidation dynamics identified elsewhere in this analysis. For the sector's investment profile, whilst this may remove high-growth firms from the VC investment pipeline, it also suggests commercial buyers continue to see value in the UK's digital identity ecosystem.

Section Summary

- On a like-for-like basis, firm count is broadly stable, with 275 firms identified in 2026 compared with 266 at baseline (a net change of nine firms).
- Estimated GVA has risen to £1,037 million, with GVA per employee of £107,800 — above the wider digital sector and approximately 46% above the UK workforce average. Productivity, rather than headcount, is the main source of the year-on-year increase.
- Estimated employment fell modestly (to 9,624 FTEs, from 10,246), concentrated in large and medium firms. This is consistent with several possible explanations, including selective restructuring, increased automation, and reclassification of digital identity activity within wider corporate operations.
- Investment activity remained below the 2020–2023 average, with M&A activity continuing, with three UK relevant transactions during 2025. We set out the key summary economic estimates across the sector below.

Table 2.9. Summary Economic Estimates

Size	Firm Count	Estimated Digital Identity Related Revenue	Estimated Digital Identity Related GVA	Estimated Digital Identity Related FTEs	Revenue per FTE	GVA per FTE
Large	32	£1,348m	£782m	5,640	£239,050	£138,603
Medium	30	£453m	£218m	2,423	£187,011	£90,072
Small	65	£175m	£29m	1,197	£146,300	£23,863
Micro	148	£51m	£9m	364	£139,410	£24,207
Total	**275**	**£2,027m**	**£1,037m**	**9,624**	**£210,644**	**£107,787**

Source: Perspective Economics

[15] GBG (2025) 'Acquisition of DataTools', Available at: https://www.gbg.com/en/news/acquisition-of-datatools-pty-limited/

SECTION 03

3. Digital Identity Market Adoption

3.1 Introduction

As set out in the baseline report, the digital identity ecosystem is underpinned by a wide range of innovative technologies, systems, and approaches to verification and trust. Given this breadth, there is no single customer type, but rather thousands of businesses, public services, and billions of individuals interact with these solutions every day. Digital identity providers often provide a range of case studies and articles regarding their substantial partnerships across the economy. For example, this might include a digital verification specialist working closely with a major national employer to improve employment checks, or it could also include a global gaming provider using age estimation technologies to keep users safer online.

This chapter explores sectoral demand (using supply side web analysis), factors influencing the uptake of digital identity solutions, and broader innovation trends. This analysis is based upon identification of case studies and customer citations, followed by classification and analysis by the research team. It should be viewed as experimental, as this analyses how the market articulates its customers (via example case studies etc), rather than definitive coverage. However, this does provide significant insight into thousands of buyers of digital identity solutions globally.

3.2 Customers and Partnerships

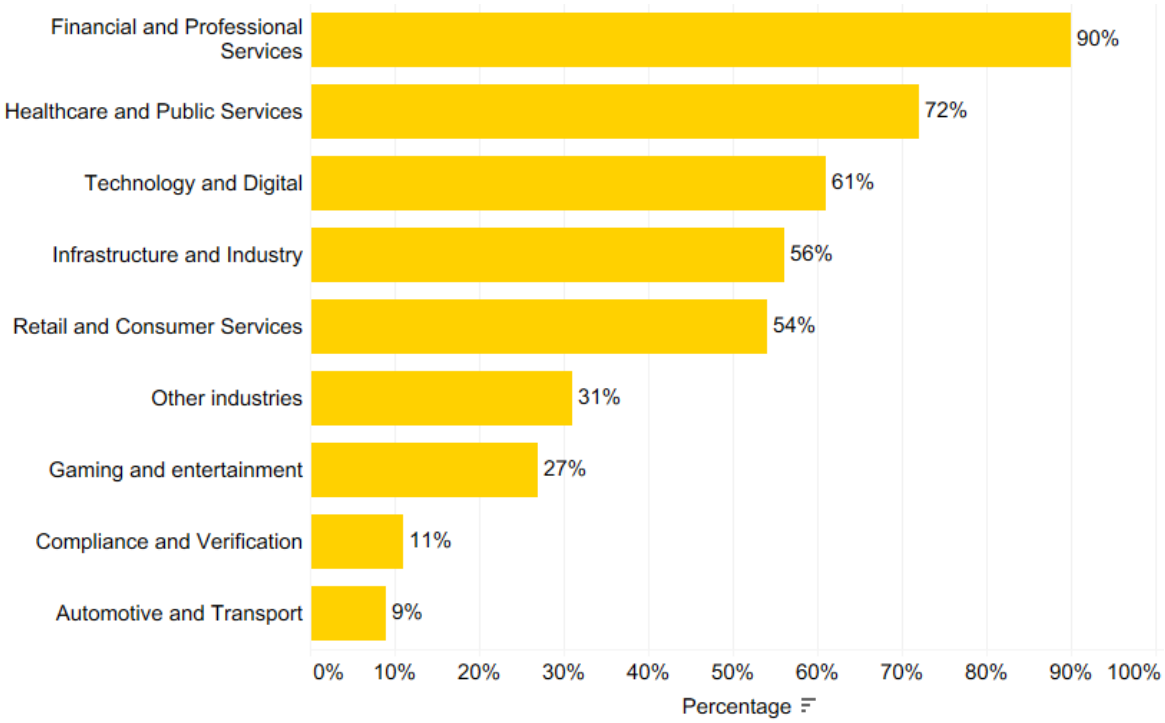
This section explores levels of sectoral demand for digital identity products and services. The research team has reviewed web data for providers (where available), and developed a classification approach to identify company descriptions, products and services offered, customers and partnerships, industries served, and standards and accreditations.

We have identified almost 4,700 unique customers and partnerships mentioned by digital identity providers. We find mention of customers or partners via analysis of company web data, case studies and testimonials. We classify each customer against ten sectors below. Figure 3.1 and Figure 3.2 highlight the percentage of digital identity providers that mention at least one customer in one or more of the respective sectors.

Figure 3.1 highlights that financial and professional services remain the core sector for digital identity providers, with 90% of firms reporting at least one customer in this sector, up from 85% in the baseline. Healthcare and public services have seen a significant increase, rising from 58% to 72%, potentially reflecting growing adoption of digital identity solutions across NHS services, local government, and wider public sector onboarding. Infrastructure and industry have also seen growth, from 39% to 56%, suggesting broadening demand for identity verification across sectors such as real estate, logistics, and construction. Technology and digital (61%, up from 57%) and retail and consumer services (54%, broadly stable from 56%) remain significant customer segments.

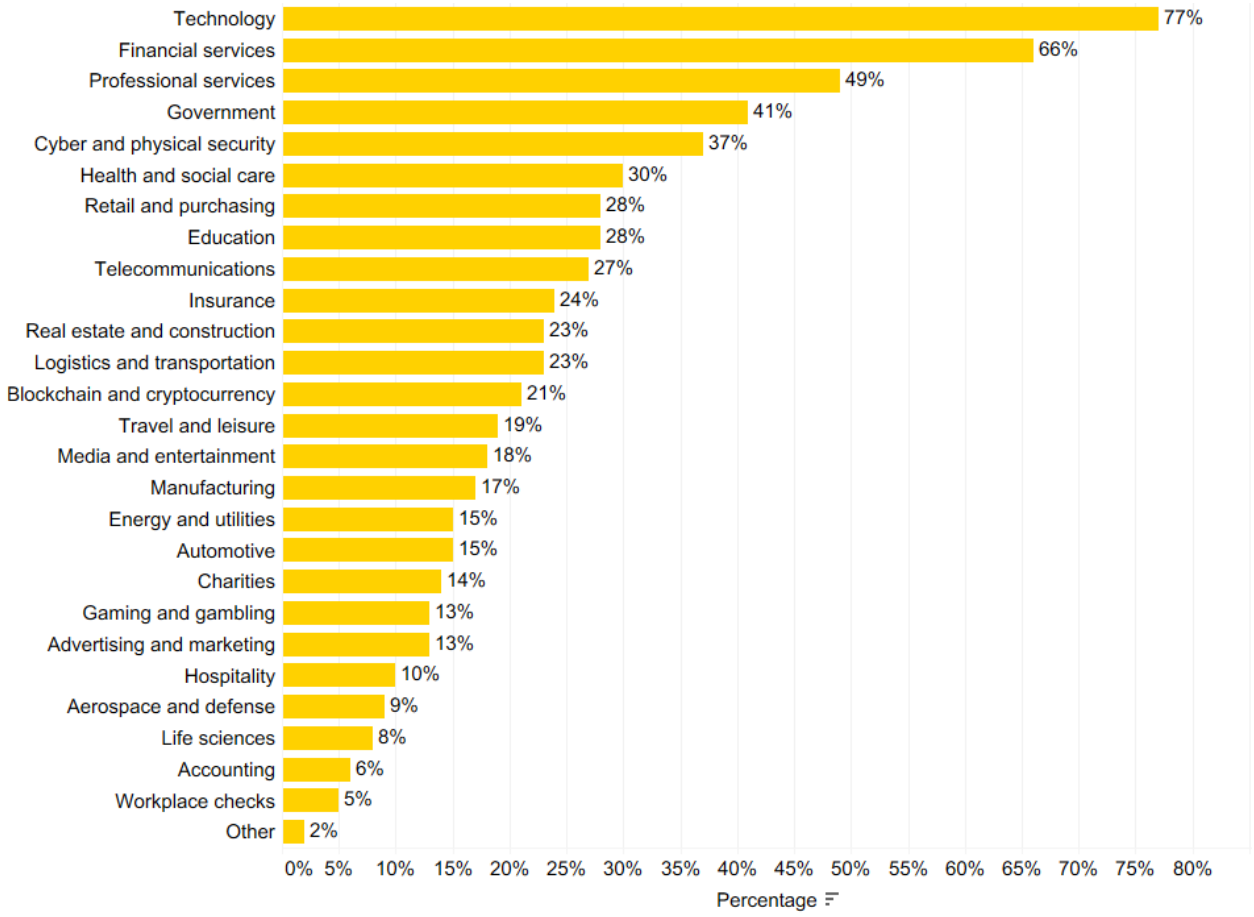
Figure 3.2 provides a more granular sub-sectoral breakdown. The breadth of customer sub-sectors, with over 25 distinct categories represented, reinforces the finding from the baseline study that digital identity solutions are applied across a far wider range of use cases than consumers might initially perceive, spanning financial services, government, healthcare, education, real estate, travel, and areas such as security and defence.

Figure 3.1. Percentage of digital identity firms supplying each sector



Source: Perspective Economics

Figure 3.2. Percentage of digital identity firms supplying each sector (subsectoral)

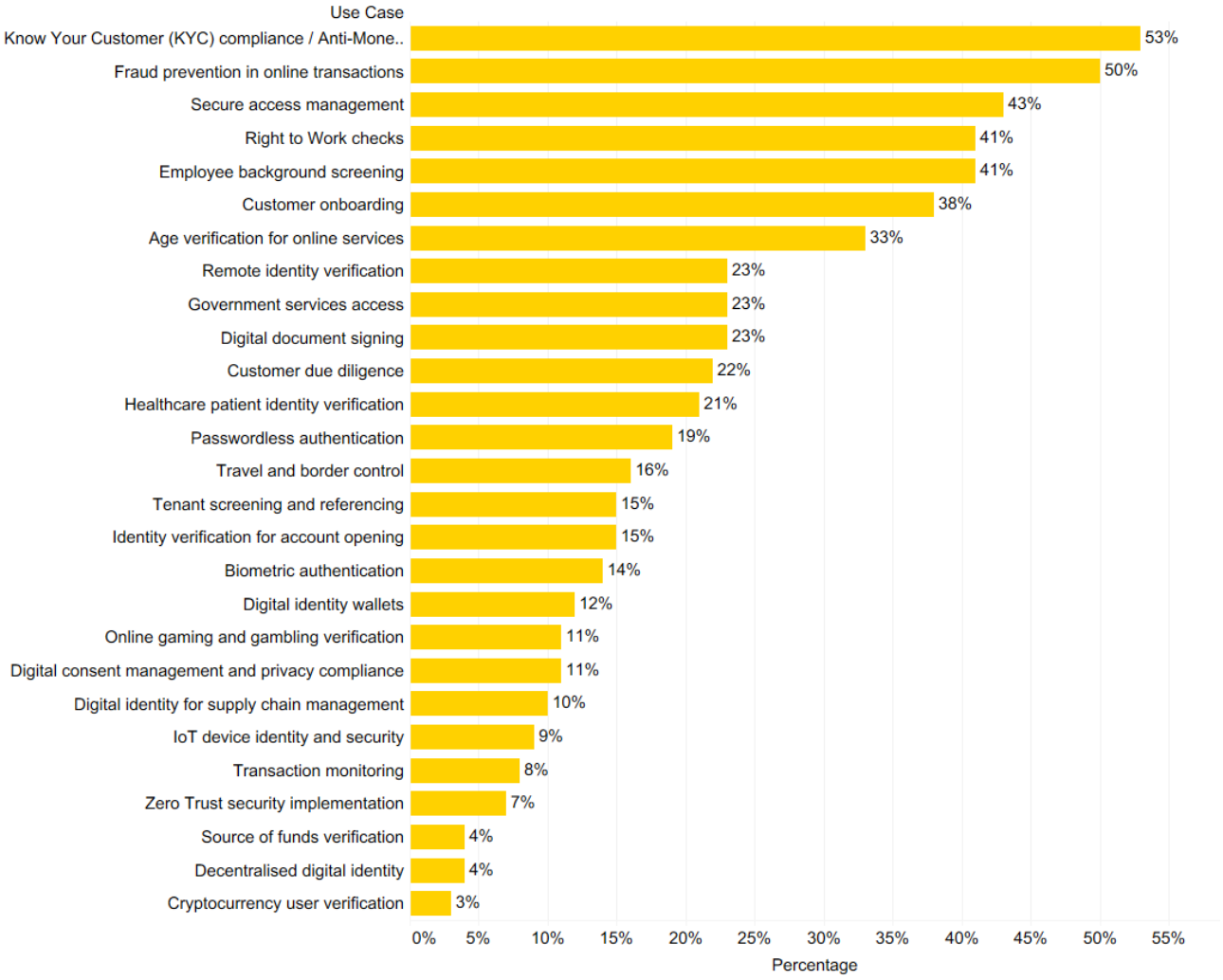


Source: Perspective Economics analysis of 270 companies

3.3 Digital Identity Use Cases

Understanding how digital identity solutions are applied in practice is central to assessing how these technologies are being embedded across the economy. Figure 3.3 sets out over 1,500 reported use cases identified through provider web data and classified by the research team into over 25 categories. This notes where providers appear to state they offer products or solutions that can support end customers with each particular use case.

Figure 3.3. Reported use cases for digital identity providers (web, classified)



Source: Perspective Economics

The data highlights that supporting firms with KYC/AML compliance is reported by 53% of providers (up from 32% at baseline), and fraud prevention in online transactions by 50% (up from 37%), placing regulatory and security use cases as a key area of focus. Secure access management (43%, up from 33%) has also grown, potentially reflecting increasing enterprise adoption of identity-led security architectures.

The research team has undertaken an extensive deep-dive into the proportion of firms that can directly or indirectly support with right to work checks (41% of providers), and employee background screening (41% of providers). This is consistent with an increased policy focus on employment compliance, including right to work checking and the identity verification requirements under the Economic Crime and Corporate

Transparency Act 2023. Age verification for online services has also doubled (33%, up from 16%), consistent with ongoing implementation of the Online Safety Act 2023 and regulatory requirements around age assurance.

Further, several emerging use cases have increased in visibility since the baseline. Digital identity wallets (12%, up from 8%), digital identity for supply chain management (10%, up from 2%), and IoT device identity and security (9%, up from 1%) suggest increasing demand to verify individuals, humans, devices, and processes across digital systems.

It is worth noting that while this sectoral analysis focuses primarily on the verification of individuals and attributes, the use case data highlights that many providers support a broader set of commercial verification requirements that sit alongside or build upon individual identity checks. For example, areas such as KYC/AML compliance, customer due diligence, source of funds verification, and transaction monitoring all extend beyond confirming identity into areas such as assessing risk, establishing trust, and regulatory compliance. In practice, verifying an individual's identity is often the first step in wider checks. For example, a financial institution onboarding a new customer will typically verify their identity before proceeding to income checks, screening, and transaction monitoring. The prevalence of these commercial use cases among digital identity providers suggests a sector whose capabilities increasingly span compliance, rather than identity verification in isolation.

Increasingly, consumers experience digital identity on what is effectively a B2B2C (business to business to customer) basis, encountering identity verification at the point of opening a bank account, starting a new job, renting a property, or accessing an age-restricted service. As such, individuals may increasingly utilise digital identity but view this experience as part of the firm’s offering, rather than the third-party digital identity provider. We explore this further in Section 4.

The use case distribution in Figure 3.3 reflects this structure, as the demand signals captured are those of the businesses and organisations procuring digital identity solutions, but the underlying driver in most cases is a regulatory or commercial requirement to verify the individuals they serve.

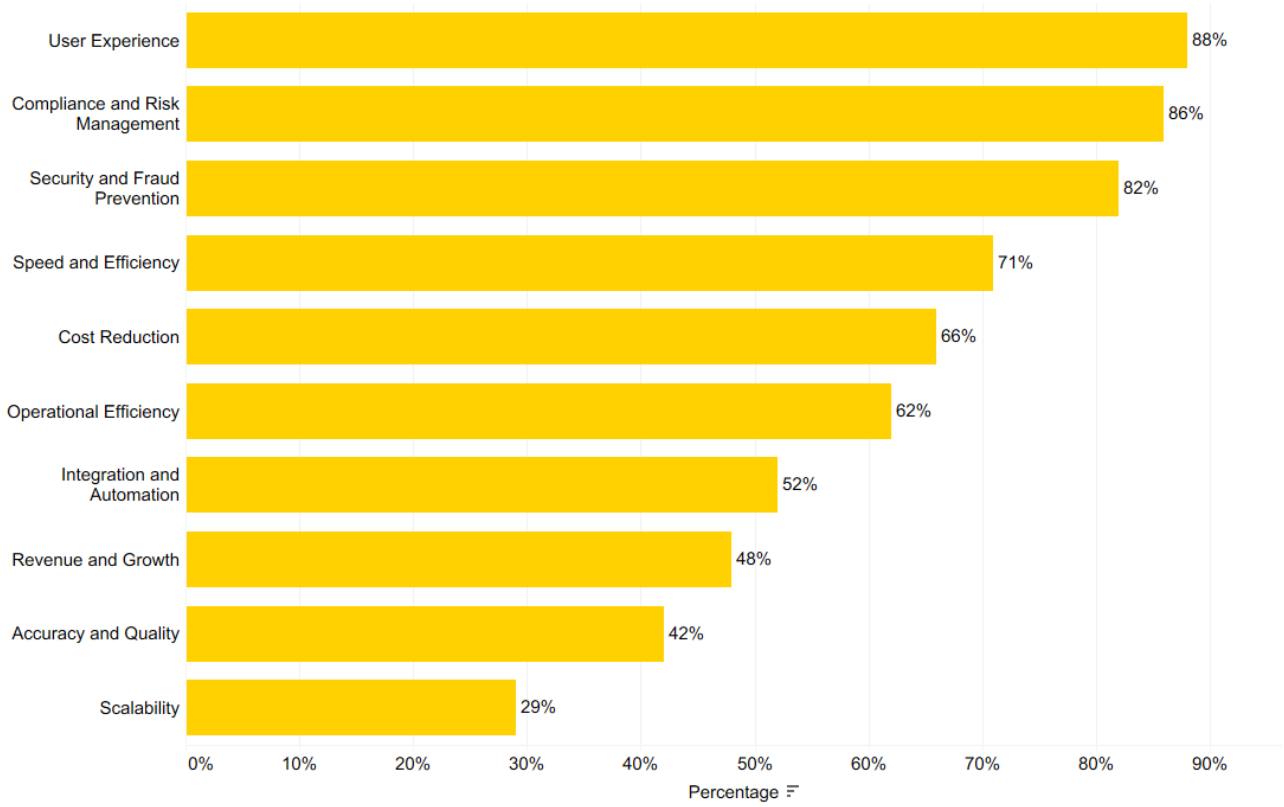
The overall pattern suggests a sector whose use case profile is maturing and diversifying. Where the baseline demonstrated relatively broad, horizontal applications (such as onboarding and fraud prevention), the updated data shows a potential tilt towards specific regulatory requirements, alongside early-stage growth in newer verticals. This has implications for future demand whereby use cases are increasingly shaped by regulation, and the sector's growth trajectory is likely to be highly sensitive to the pace and scope of policy implementation across government, financial services, and online safety.

Further, the research team’s classification process also identified a small number of new use cases, where digital identity capabilities are being applied in new and novel contexts. For example, the emergence of AI agent identity, where providers such as Ping Identity and Cheqd are developing authentication and governance frameworks for autonomous AI agents. As agentic AI becomes more prevalent in workflows, demand to verify, authorise, and audit non-human actors represents an extension of the sector's competencies, and is expected to grow significantly. We also find increased use of identity solutions that enables audience targeting and measurement in a post-cookie environment, using telecommunications signals or pseudonymous identifiers rather than traditional personal data; and increased use of tooling for content authenticity and provenance checks such as cryptographic signing.

3.4 Benefits of Digital Identity

The research team reviewed web data to identify how providers describe the benefits of their digital identity solutions to end users and customers. This analysis is experimental, drawing on provider websites, case studies, and marketing materials to capture how commercial benefits are articulated to the market. We classify these into ten distinct benefit categories, set out in Figure 3.4.

Figure 3.4: Percentage of providers mentioning end-user benefits by type



n = 158 companies with user / customer benefits identified

User experience (88% of providers) and compliance and risk management (86%) are now the most commonly cited benefits, followed by security and fraud prevention (82%). In the baseline, the leading benefits were speed and efficiency (57%), user experience (53%), and operational efficiency (51%). This update suggests that the market has increased focus on positioning towards compliance and user experience as the primary selling points; however, we note this may be subject to reclassification and new web data in review in this study.

This shift is consistent with the broader trends identified across this analysis. The regulatory environment around digital identity has intensified considerably since the baseline, with the Online Safety Act 2023, digital right to work checks, the Data (Use and Access) Act 2025, and Companies House identity verification requirements all increasing the compliance requirements on individuals and organisations. It is therefore unsurprising that providers are increasingly framing their offer in terms of regulatory compliance rather than time or operational savings alone.

Taken together, the data suggests a market whose commercial positioning is maturing alongside the regulatory context. The emphasis on compliance, security, and user experience points to a sector that is positioning digital identity not simply as a cost-saving tool, but as core infrastructure for meeting regulatory obligations while minimising friction in customer journeys.

Within our review, we find that several providers set out commercial and Return on Investment (ROI) benefits of investing in digital identity. We set out some updated examples below, selected to illustrate different technology approaches, sectors, and use cases. Please note that these are case studies as reported by vendors. The statistics have not been independently verified by this research team.

Keyless:

- Keyless is a London-founded provider of privacy-preserving biometric authentication, using Zero-Knowledge Biometrics technology that authenticates users without storing biometric data. As noted in the investment section of this report, Keyless raised £1.9m in early 2025 before being acquired by Ping Identity later that year.
- Keyless publishes several named case studies on its website. Working with one of Europe's largest banks, Keyless reports that its solution delivered '$4 million saved in helpdesk and SMS OTP costs in the first year, a 79% reduction in account takeover fraud rates, and an estimated $2 million in savings from prevented fraud attempts.' The bank deployed Keyless for self-service account recovery and payment authentication, replacing call centre processes and SMS-based one-time passcodes.

Vouchsafe:

- Vouchsafe is a DVSTF-certified identity verification platform designed to address identity poverty, accepting a broad range of evidence including trusted referee vouches alongside traditional documents.
- Vouchsafe reports that 11 million people in the UK lack a passport or driving licence, making it difficult for them to access banking, credit, and other essential services. The platform is designed to verify individuals who would otherwise be excluded by conventional document-based approaches. Vouchsafe has been selected by the Scottish Government's CivTech programme to improve access to public services for people who struggle with proving their identity[16].
- In a case study with Right Way Credit Union, Vouchsafe reports a 68% reduction in member drop-off rates, with over 85% of verifications completed automatically within one hour and a 'perfect verification success rate' in a pilot with 60 new members[17].

Thirdfort:

- Thirdfort provides automated client due diligence for the legal sector, combining digital identity verification, anti-money laundering screening, and source of funds checks through Open Banking technology. The platform has verified over three million individuals on behalf of more than 1,500 regulated businesses, including law firms and estate agents.
- Thirdfort reports that its platform can reduce the time spent on client due diligence by up to 80%. Named law firm clients include Mishcon de Reya, whose onboarding period for straightforward matters was reduced from days to minutes after implementing Thirdfort. Laytons, a full-service law firm, reports cutting client onboarding times by around 75%, and Direction Law reported a '50% improvement in the speed of its compliance process'[18].

[16] Fintech Global, 'Identity verification startup Vouchsafe secures £1m pre-seed funding to tackle ID poverty', March 2025, available at: https://fintech.global/2025/03/19/identity-verification-startup-vouchsafe-secures-1m-pre-seed-funding-to-tackle-id-poverty/
[17] Vouchsafe (2025) 'Fair finance starts here: How Right Way Credit Union modernised member onboarding' Available at: https://vouchsafe.id/right-way-credit-union/
[18] Thirdfort 'Our Clients', Available at: https://www.thirdfort.com/our-clients/category/law-firms/

- In addition, over 200 firms using Thirdfort's partnership with Inperio report benefiting from reduced professional indemnity insurance (PII) premiums, reflecting the risk reduction that digital verification provides relative to manual document checking[19].

VerifyMy:

- VerifyMy (formerly VerifyMyAge) is a UK-based age verification provider offering a range of verification and age estimation methods for online retailers and platforms selling age-restricted products and services. The company reports having verified over 15 million orders to date, with verification typically completed in under a minute.
- In a case study with Toolstation, VerifyMy reports a 50% reduction in cancellations of orders containing age-restricted products following implementation. The automated solution also enabled Toolstation to reposition the equivalent of 2.5 full-time employees who had previously been focused on processing manual age checks.[20] Toolstation noted that the majority of their customers were verified in 'stealth', meaning they did not need to actively engage with the age verification process, resulting in minimal disruption to customer journeys. Separately, Camden Town Brewery deployed VerifyMy during a high-profile television advertising campaign for 'free beer', achieving a 99.4% pass rate while handling over 3,000 verifications in under 60 minutes during each ad airing. The solution was integrated within the Shopify checkout flow on the same day, with no requirement for customers to enter credit card details or undergo ID checks at delivery.

Section Summary

- Adoption of digital identity solutions is broadening across customer sectors and use cases, with the value proposition increasingly framed around compliance and user experience.
- Almost 4,700 unique customers and partnerships were identified across providers. Financial and professional services remain dominant (90% of firms), while healthcare and public sector engagement rose notably (from 58% to 72% of firms).
- KYC / AML compliance, fraud prevention, secure access management and right-to-work checks remain the most cited use cases. Age verification for online services has roughly doubled in provider coverage, consistent with the wider regulatory environment.
- The case studies highlight that providers are increasingly tracking measurable operational benefits at the level of individual deployments, which may offer insight into how digital identity solutions can lead to longer term economic benefits.
- Providers are increasingly refining their value proposition, with areas such as compliance and user experience increasingly cited by vendors.

[19] Thirdfort 'How Thirdfort's technology is allowing firms to unlock reduced PII premiums', Available at: https://www.thirdfort.com/our-clients/how-firms-are-reducing-PII-premiums-with-thirdfort/
[20] VerifyMy, 'Case Studies' Available at: https://verifymy.io/resources/case-studies/

SECTION 04

4. Consumer Attitudes to Digital Identity

4.1 Introduction and Methodology

Within the baseline research, a consumer survey was undertaken to understand views on digital identity, including take-up and adoption, experiences of use or non-use, and broader views and sentiment regarding digital identity. This also included an assessment of inclusion and access challenges associated by groups with using digital identity.

This section sets out updated consumer research conducted by Survation, undertaken in November 2025. This survey involved online surveying of 5,658 UK residents aged 18-66.

This represents a significant increase in sample size from the baseline survey (3,561 respondents in January 2025), strengthening the statistical robustness of the findings.

The research methodology includes:

Step 1: Survey design and sampling approach

The research team reviewed and confirmed the research objectives, target audience, and methodology. Relevant questions were developed with a clear layout to ensure accuracy, ease of completion, and to minimise response bias. The topic guide was updated to include a focus upon usage, preferences in use cases, and overall sentiment regarding digital identity adoption in a series of scenarios.

The research employed a stratified sampling approach, with specific recruitment targeting participants across the following populations:

- UK residents aged 18+ with a long-term disability
- UK residents aged 18+ with no UK/EU passport or driving licence
- UK residents aged 18+ with low digital skills (as defined by the Lloyds Bank Consumer Digital Index)
- UK residents aged 18+ who have legally changed their identity attributes such as name or gender

Different response rates from different demographic groups were considered. Quotas were monitored throughout data collection, with additional recruitment as needed to maintain balance. Participants were provided with an overview of the research and had the opportunity to opt out at any stage, ensuring informed consent.

Step 2: Survey

Survation conducted the survey via online panel on a sample of the UK population aged 18 and over, achieving a total sample size of 5,658 respondents across the population groups set out above. All charts are shown in line with the theme and question wording put to respondents. The survey involved 24 questions (including screening and survey questions) and was conducted in: English, Welsh, Panjabi and Urdu as per the most common languages in England, Wales and Scotland. Additional focus was undertaken to ensure representation in survey participants from groups at greater risk of exclusion, including individuals with lower levels of ID, with changes in aspects of their ID, and with low digital skills and limited digital access. Annex B includes a detailed breakdown of these groups.

Step 3: Analysis

The research team analysed the 5,658 responses in February 2026. A key methodological improvement over the baseline is the application of data weighting to strengthen population-level estimates:

- **Nationally representative sample:** weighted to the profile of all UK adults aged 18+, by age, sex, region, annual equivalised household income, highest level of qualification, employment status, socioeconomic group, and ethnicity.
- **Access challenges sample:** weighted to the profile of all UK adults aged 18+ with a long-term disability by age, sex, and region.
- **Low ID sample:** weighted to the profile of all UK adults aged 18+ with no passport, by age and region.
- **Changed identity and low digital skills samples:** unweighted, given the targeted nature of these populations.

Weighting targets were derived from Office for National Statistics data. The baseline survey analysed unweighted data across all groups; the introduction of weighting in this wave represents an improvement in the reliability of population-level findings. As such, any time-series comparisons are not undertaken beyond base levels of self-reported understanding between the two surveys. To gain insights from the survey data, several analytical approaches were employed:

- **Demographic segmentation:** data was analysed by demographic variables, digital skill levels, and access to identification documents to identify differences in experiences and needs.
- **Comparative analysis:** findings for specific demographic groups were compared against the wider sample to identify unique challenges and needs.

Survey limitations:

The use of a survey can provide useful insights into understanding and adoption of digital identity. However, we note the following limitations that should be considered when interpreting these findings:

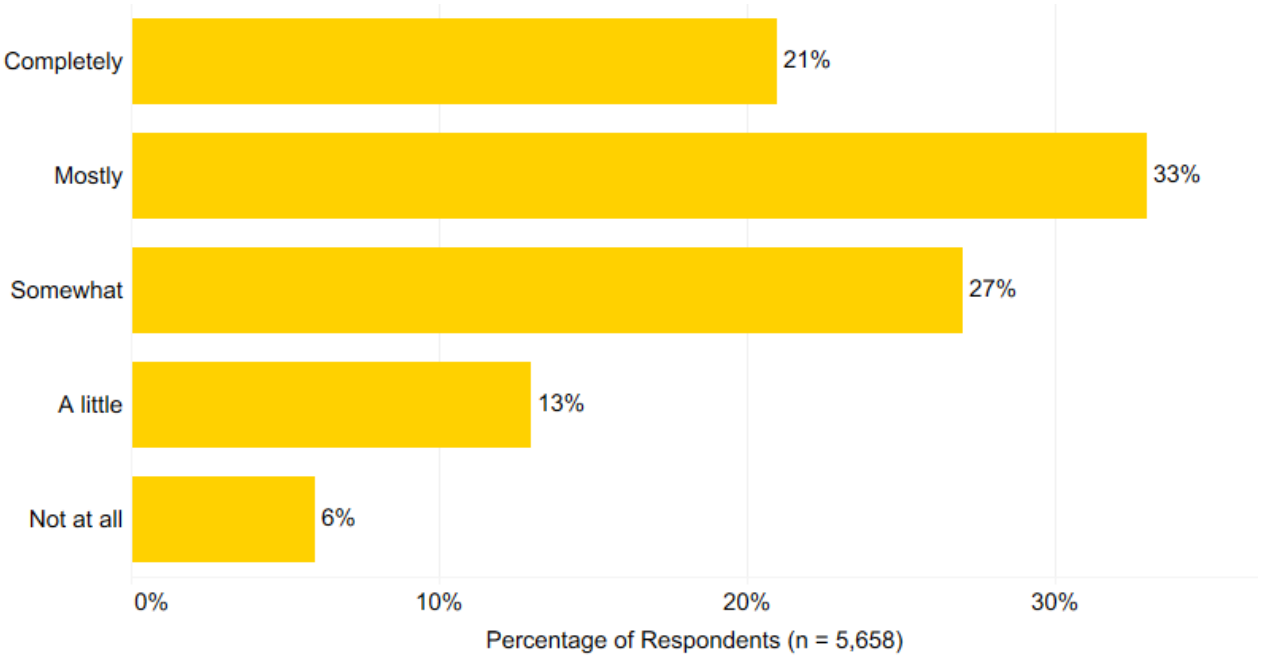
- **Margin of error:** This survey achieved a strong response rate, with an estimated margin of error of 1.3% for aggregate responses. However, for sub-group analysis, the margin of error may be subject to increase.
- **Subgroup sample sizes:** some specific demographic subgroups had relatively small sample sizes. Findings related to these subgroups should typically be considered indicative rather than definitive and may benefit from targeted qualitative research.
- **Interpretation and self-reporting:** the survey relies on self-reported experiences, which may be affected by recall or varied understanding of technical concepts. This remains a challenge in understanding population-level feedback on use and views.
- **Variations in sample size:** for some questions, the sample size may vary slightly depending on whether the respondent fully completed the question, or if the survey logic applied to their own demographic or experiences. Some figures may also not sum due to rounding.

4.2 Digital Identity Use in the UK

The research explored public understanding of digital identity services, which allow individuals to prove their identity or personal attributes without physical documents. After being provided with a brief definition[21], respondents were asked to assess their level of understanding, by being asked 'To what extent, if any, do you understand the concept of a digital identity service?'

Figure 4.1 shows that approximately one in five (21%) respondents claim to have a 'complete understanding' of the concept of digital identity, while one-third (33%) report that they 'mostly' understand. Combined with those who 'somewhat' understand (27%), **this suggests that 81% of respondents feel they have some level of understanding of the concept of digital identity**, an increase from 71% in the baseline survey.

Figure 4.1: Self-reported consumer understanding of digital identity



Source: Perspective Economics, Survation (n = 5,658 responses)

The proportion reporting 'a little' understanding has fallen from 21% to 13%, and those reporting no understanding at all has declined from 8% to 6%. The improvement is concentrated in the 'mostly' category, which rose from 24% to 33%, suggesting levels of self-reported public understanding have increased in the last twelve months. Overall, the proportion of respondents reporting limited or no understanding has fallen from 29% to 19%.

The survey findings also continue to highlight variation across demographic groups, indicating different levels of exposure, usage, and engagement with digital identity services.

[21] See Annex B.

Figure 4.2: Self-reported consumer understanding of digital identity by age

Response	18–24	25–34	35–44	45–54	55–66
Completely	17%	29%	23%	21%	12%
Mostly	28%	34%	37%	33%	37%
Somewhat	31%	23%	27%	27%	32%
A little	17%	9%	9%	13%	14%
Not at all	8%	5%	4%	6%	5%
Some understanding	**76%**	**86%**	**87%**	**81%**	**80%**
Limited understanding	**24%**	**14%**	**13%**	**19%**	**20%**

Source: Perspective Economics, Survation (n = 4,001 with age coverage) including 18–24 (n = 397), 25–34 (n = 863), 35–44 (n = 886), 45–54 (n = 860), 55–66 (n = 995).

All age groups report higher levels of understanding compared to the baseline. Adults aged 25–44 continue to report the highest levels, with c. 87% indicating some understanding (compared to c. 76% in the baseline). The most notable increases are among the previously lower percentage groups. For example, the 55–66 cohort has risen from 65% to 80%, and the 18–24 cohort from 64% to 76%.

The data observed in the baseline, where those in mid-age bands report higher understanding, likely driven by tangible usage of identity verification during events such as property purchases, employment checks, and financial applications continues to apply. However, the increased understanding across all age groups suggests increased population familiarity with digital identity concepts. This may in part reflect recent government announcements and policy developments relating to digital identity, as well as wider deployment of digital identity and age assurance across public and private sectors over the past year.

Figure 4.3: Self-reported consumer understanding of digital identity by annual household income

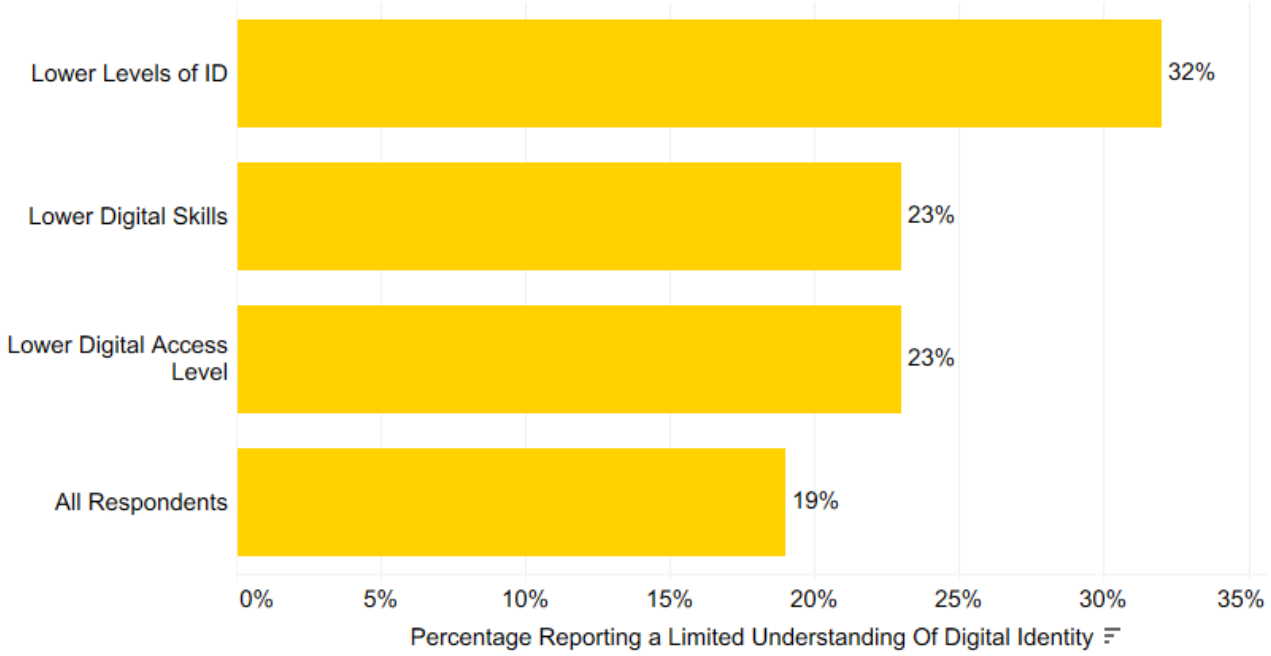
Response	< £19,999	£20,000–£39,999	£40,000+
Completely	16%	19%	27%
Mostly	24%	34%	38%
Somewhat	32%	27%	22%
A little	17%	14%	9%
Not at all	10%	5%	4%
Some understanding	72%	81%	88%
Limited understanding	28%	19%	12%

Source: Perspective Economics, Survation (n = 5,658 responses) (< £19,999 (n = 1,762), £20,000–£39,999 (n = 1,834), £40,000+ (n = 2,062).

Figure 4.3 highlights that the strong relationship between annual household income and perceived understanding of digital identity observed in the baseline remains in this study. All income groups report improved understanding, with the highest income cohort (£40,000+) now at 88% with some understanding (up from 78%) and the lowest (under £19,999) at 72% (up from 65%). However, respondents in the lowest income group (under £19,999 annual household income) remain almost three times more likely to report no understanding at all (10%) compared to those in the highest income group (£40,000+, at 4%). The lowest income group is also more than twice as likely to report limited understanding overall (28%) compared to the highest income group (12%).

While all groups appear to show increased awareness of digital identity, the gap reinforces the case for inclusive service design that accounts for the access, experiences and capabilities of users across socio-economic backgrounds. This report also considers those with lower digital skills, lower digital access levels, and lower levels of ID as groups at potentially higher risk of exclusion (definitions found in Annex B) with regard to digital identity understanding. This is set out in Figure 4.4.

Figure 4.4: Percentage of those who reported limited understanding of digital identity by groups at higher risk of exclusion



Source: Perspective Economics, Survation. Lower digital skills (n = 408), Lower digital access level (n = 418), Lower levels of ID (n = 520), All respondents (n = 5,658)

Figure 4.4 suggests that individuals in groups at higher risk of exclusion continue to report lower understanding of digital identity than all respondents. However, all groups have seen an improvement in perceived understanding since the baseline. The proportion reporting limited understanding among those with 'lower digital skills' has halved, from 47% to 23%, and the equivalent figure for those with lower digital access has fallen from 40% to 23%. Those with lower levels of ID have also improved, albeit to a lesser extent, from 37% to 32%.

Those with lower levels of ID remain 15 percentage points above the overall figure, suggesting that limited access to identity documents continues to act as a more persistent barrier to understanding or engagement with digital identity services to date.

Levels of Use

In addition to levels of understanding, respondents were asked about their participation in daily use cases that involve identity and/or identity verification. All survey respondents were asked *'To your knowledge, have you had any experience proving your identity when doing any of the following?*' and were provided with a list of use cases:

- Opening a bank account
- Applying for a credit card or loan online
- Proving you have the right to work in the UK after receiving a job offer
- Accessing online games or gambling accounts
- Verifying your identity for HMRC Self-Assessment
- Accessing public or government services such as the NHS or receiving state benefits
- Setting up and managing insurance policies (e.g. making claims and verifying eligibility)
- Proving who you are when doing a DBS (Disclosure and Barring Service) check
- Verifying your identity when buying a property (e.g. ID checks for mortgage applications, estate agents or solicitors)
- Accessing discounted travel schemes (e.g. student railcards)
- Verifying your identity when renting a property
- Verifying your identity for Companies House
- Proving how old you are when going to a cinema or buying something age-restricted like a lottery ticket in a shop

The list of use cases has been revised from the baseline to better reflect the breadth of contexts in which consumers may encounter digital identity verification. New use cases include the HMRC Self Assessment, accessing public and government services, and Companies House verification. The baseline survey also asked respondents about linking their identity to Apple Pay and Google Pay and about buying tickets for events requiring proof of identity; these were removed to reduce risk of misinterpretation, and the latter was replaced by more targeted use cases. Respondents were asked whether they had completed each use case digitally, non-digitally, or both. Analysis of these responses can be used to understand overall perceived levels of digital identity use. We note, however, that in many instances, users may have undertaken digital identity checks and been unaware (e.g. scanning an ID or taking a selfie for age verification) that this constitutes use of digital identity. Further, respondents may have used manual methods (e.g. photographing a physical ID). However, we take respondent feedback as provided to explore self-reported usage and engagement to date.

Figure 4.5: Level of self-reported use of any digital identity product or service

Level of digital identity use	Update (2025)	Baseline (2024)
Has used digital identity services for at least one purpose	77%	44%
Have never used digital identity services	23%	38%

Source: Perspective Economics, Survation (n = 5,658 responses). A respondent is classified as having used digital identity services if they selected 'I proved my identity digitally' for at least one of the 13 use cases.

Over three-quarters (77%) of respondents report having completed at least one digital identity use case at some point, an increase from 44% in the baseline. The proportion reporting that they have never used a digital identity service has fallen from 38% to 23%.

Several factors are likely to have contributed to this. The expanded list of use cases, particularly the addition of HMRC Self Assessment and public and government services, increased use of age assurance, and Companies House verification may capture a wider range of contexts in which respondents may have encountered digital identity verification, some of which were not prompted in the baseline.

Please note the validation filter applied in the baseline (which reclassified 18% of respondents as not having used digital identity according to the scope of the research) was not applied in this wave.[22] As such, the two surveys are not directly comparable on this measure.

However, the data does suggest an underlying rise in digital identity engagement over the past year, consistent with the improvement in reported understanding above and with the broader trend of increased deployment of digital identity services across financial services, labour markets, and government. The following tables show breakdowns of demographic and selected groups for survey respondents that have used at least one digital identity service at some point.

Digital identity use by age

Figure 4.6: Level of self-reported use of any digital identity product or service (by age)

Age group	Has used (2025)	Has used (baseline)
18–24	83%	46%
25–34	87%	59%
35–44	85%	48%
45–54	74%	43%
55–66	69%	34%

Source: Perspective Economics, Survation (n=4,001 responses) including 18–24 (n = 397), 25–34 (n = 863), 35–44 (n = 886), 45–54 (n = 860), 55–66 (n = 995)

Individuals aged 25–34 remain the most likely to report having used a digital identity service (87%), whereas those aged 55–66 remain the least likely (69%). The gap between the most and least likely age groups has narrowed from 25 percentage points in the baseline to 18 percentage points, suggesting that digital identity use may be becoming more distributed across age cohorts.

As observed in the baseline, this pattern is likely driven in part by the concentration of life events that require identity verification, such as opening a bank account, applying for a loan, or buying or renting a property within the 25–44 age range. However, the increase among older cohorts suggests that broader deployment of digital identity across government and public services may be bringing previously less familiar groups into

[22] The baseline survey applied validation questions to determine whether respondents' understanding of digital identity matched the definition used by the research. Respondents who provided evidence suggesting they had not used a digital identity service according to the scope of the research were reclassified accordingly. This filter was removed in the updated wave on the basis of not overriding respondents' self-reported experience, particularly given the diversity of services and contexts that consumers may reasonably interpret as digital identity verification, even if the extent of third party usage is more limited in some use cases than others. This subsequently informed questions regarding user preference for digital, physical, or any type of identity verification in the survey.

contact with these services. The relationship between reported understanding and reported use continues to show an interesting divergence among the youngest cohort. While 18–24 year olds remain among the least likely to report 'some understanding' of digital identity (76%), their reported usage (83%) is higher than their reported understanding, suggesting that younger respondents may be engaging with digital identity services without necessarily recognising or labelling them in this way, or recognising the use cases required identity verification when completing the survey.

Digital identity use by annual household income

Figure 4.7: Level of self-reported use of any digital identity product or service (by household income)

Income	Has used (2025)	Has used (baseline)
< £19,999	65%	31%
£20,000–£39,999	76%	48%
£40,000+	87%	59%

Source: Perspective Economics, Survation (n=5,658 responses), < £19,999 (n = 1,762), £20,000–£39,999 (n = 1,834), £40,000+ (n = 2,062).

Households earning more than £40,000 per year remain the most likely to have used digital identity (87%), while those in the lowest income bracket report the lowest usage (65%). All income groups show increases from the baseline, with the lowest income group more than doubling its reported usage (from 31% to 65%).

Reasons for non-use of digital identity services

Respondents who reported that they had never used a digital identity service were asked to identify their main reasons for non-use. This group represents 23% of all respondents (n = 1,307, weighted).

Figure 4.8: Reasons for non-use of digital identity services

Reason	% of non-users
I prefer using physical ID when possible	29%
I haven't had to prove my identity	29%
No digital option has been provided	15%
I am not comfortable using this technology	15%
I didn't have the right documents available (passport, driving licence etc.)	13%
I have privacy or security concerns about using digital identity services	12%
I don't trust the provider	10%
Don't know	10%

I don't understand how to use it	7%
I tried but had to use a physical option	5%
I didn't have the required technology (smartphone, device)	4%
Other	3%

Source: Perspective Economics, Survation (n=5,658 responses. Base: respondents who have not used digital identity services (n = 1,307, weighted). Multiple choice question therefore percentages do not sum to 100%.

The most commonly cited reasons for non-use were preference for physical ID (29%) and not having had to prove one's identity (29%). Together, these suggest that for a significant portion of non-users, the barrier is not inability or opposition but rather a combination of established habit and perceived lack of need. These respondents may represent a group that could use digital identity in future as more services adopt digital identity solutions as required.

However, this does highlight some challenges regarding access and availability. The data suggests that 15% of non-users reported that no digital option had been provided, and 13% cited a lack of the right documents. These findings are consistent with the supply side analysis in this report, as while deployment of digital identity services is expanding, coverage is not universal, and document requirements can act as a barrier for those without a passport or driving licence[23], a group already identified as potentially higher risk of exclusion.

Further, comfort and confidence barriers were also cited, with 15% reporting that they are not comfortable using the technology and 7% stating that they do not understand how to use it. Trust and privacy concerns also remain for some non-users, with 12% citing privacy or security concerns and 10% reporting a lack of trust in the provider. While these figures are lower than the comfort and access barriers, they suggest that for a proportion of non-users, the decision not to engage may reflect concerns about how personal data is handled.

A small proportion (5%) reported having tried to use a digital identity service but ultimately having to revert to a physical option, and 4% cited a lack of the required personal technology such as a smartphone. These groups highlight the importance of maintaining non-digital alternatives alongside digital options, and of ensuring that services are designed to function across a range of devices and connectivity levels.

Reasons for non-use by age

Figure 4.9: Reasons for non-use of digital identity (by age)

Reason	18–24	25–34	35–44	45–54	55–66
I haven't had to prove my identity	4%	15%	25%	42%	42%
I prefer using physical ID when possible	22%	23%	31%	39%	35%

[23] 16% of all respondents to this survey reported they did not have a valid passport or driving licence.

No digital option has been provided	6%	19%	13%	21%	13%
I am not comfortable using this technology	9%	18%	15%	13%	17%
I have privacy or security concerns	7%	16%	10%	15%	13%
I didn't have the right documents available	1%	6%	6%	10%	9%
I don't trust the provider	8%	8%	17%	7%	9%
I don't understand how to use it	7%	1%	6%	6%	8%
I tried but had to use a physical option	9%	2%	8%	4%	4%
I didn't have the required technology	0%	6%	3%	4%	4%
Don't know	19%	26%	7%	3%	8%
Prefer not to say	22%	5%	8%	4%	1%

Source: Perspective Economics, Survation (n = 778 responses) including 18–24 (n = 58), 25–34 (n = 96), 35–44 (n = 122), 45–54 (n = 205), 55–66 (n = 297). Weighted figures. Caution: sample sizes for the 18–24 and 25–34 age groups are small; findings for these cohorts should be treated as indicative rather than definitive.

The age breakdown in Figure 4.9 regarding non-use also reveals some variance by age groups. However, findings should be interpreted with caution given the small sample sizes involved.

Among non-users aged 45 and over, the most commonly cited reason was not having had to prove their identity (42%), compared with just 4% of 18–24-year-olds and 15% of 25–34-year-olds. This suggests that older non-users are more likely to view digital identity as something they simply have not encountered, rather than something they have avoided.

Preference for physical ID follows a broadly similar pattern, rising from around a quarter of non-users in the youngest cohorts, to approximately one in three among those aged 35 and over. This suggests that the preference for physical documents is higher among older respondents.

How are individuals using digital identity?

All respondents were asked whether they had completed each of the thirteen use cases, and if so, whether they verified their identity using a digital or non-digital method.[24]

Figure 4.10: Percentage of respondents who have proved their identity digitally, by use case

Use case	Proved digitally (2025)	Baseline
Setting up and managing insurance policies	40%	28%
Applying for a credit card or loan online	40%	36%
Opening a bank account	40%	27%
Verifying your identity when renting a property	36%	18%
Verifying your identity when buying a property	35%	21%
Proving you have the right to work in the UK	32%	21%
Verifying your identity for Companies House	30%	-
Accessing public or government services (NHS, benefits)	30%	-
Verifying your identity for HMRC Self Assessment	28%	-
Proving how old you are (age-restricted, in person)	28%	10%
Accessing online games or gambling accounts	23%	38%
Proving who you are when doing a DBS check	23%	26%
Accessing discounted travel schemes	20%	27%

Source: Perspective Economics, Survation, (n = 5,658) (weighted). Baseline figures shown where a comparable use case was used.

The most commonly reported digital use cases include identity verification for insurance, credit or loan applications, and opening a bank account (40%), followed by property transactions, and right to work checks (32%). Three new use cases were introduced in this wave, including Companies House verification for directors (30%), accessing public or government services (30%), and HMRC Self Assessment (28%), all of which show meaningful levels of reported digital engagement. At the lower end, accessing online games or gambling accounts (23%), DBS checks (23%), and discounted travel schemes (20%) had the lowest levels of reported digital use.

Consumer preferences for digital versus physical identity verification

Respondents were subsequently asked to indicate their preference for digital or physical identity verification across nine everyday scenarios, should they encounter these despite current or existing levels of

[24] These figures are based on self-reported experience and should be interpreted accordingly. As with all self-reported survey data, individual responses may reflect varying levels of recall and interpretation.

engagement. This provides improved insight regarding tangible preference given the option under each broad scenario.

Figure 4.11: Consumer preference for digital versus physical identity verification, by scenario

Scenario	Prefer digital	Prefer physical	Either	Wouldn't do this	Don't know
Making age-restricted purchases online	39%	25%	20%	8%	7%
Accessing government or NHS services	36%	28%	25%	4%	7%
Opening a bank account or financial product	31%	35%	24%	4%	6%
Applying for jobs and right to work checks	29%	32%	24%	7%	7%
Healthcare appointments	28%	35%	25%	5%	7%
Travelling outside of the UK or Ireland	27%	37%	24%	6%	6%
Making age-restricted purchases in shops	26%	38%	23%	8%	6%
Renting or purchasing property	24%	36%	24%	8%	7%
Proving my age in person (e.g. bar, restaurant, cinema)	23%	41%	21%	9%	6%

Source: Perspective Economics, Survation (n = 5,658 (weighted))

Consumer preferences for digital or physical identity checks vary considerably depending on the context, and the data suggests that the nature of the interaction, particularly whether it takes place online or in person, is a strong driver of preference.

Digital preference is highest for making age-restricted purchases online (39%), the only scenario in which digital clearly outweighs physical preference (25%). Accessing government or NHS services is the next strongest for digital preference (36% vs 28%), consistent with the growing adoption of digital identity across public services and the increasingly digital-first design of services such as the NHS App and GOV.UK accounts.

For the remaining scenarios, physical ID is the more popular choice, though the margin varies. In-person contexts show the strongest physical preference such as proving age in a bar, restaurant or cinema (41%

physical vs 23% digital) and making age-restricted purchases in shops (38% vs 26%). Travelling outside the UK also leans physical (37% vs 27%), likely reflecting the assumed usage of physical passports.

However, there is a consistent proportion of respondents who would be comfortable using either method, ranging from 20% to 25% across all scenarios. When combined with those who actively prefer digital, the proportion of respondents who would be willing to use digital identity verification reaches a majority in six of the nine scenarios, including online purchases (59%), government and NHS services (61%), opening a bank account (55%), right to work checks (53%), healthcare (53%), and property transactions (48%). This suggests that while outright preference for digital remains a minority position in most contexts, acceptance of digital identity use as an option is substantially broader.

The scenarios where digital willingness (digital preference plus either) is lowest are proving age in person (44%) and age-restricted purchases in shops (49%), both of which involve face-to-face interactions where physical documents remain an established norm. These findings suggest that the path to adoption may be most applicable in contexts that are already conducted remotely or online, as part of existing online usage.

Perceived benefits of digital identity

All respondents were asked what they consider to be the benefits of using a digital identity service compared to physical forms of ID such as a passport or driving licence.

Figure 4.12: Perceived benefits of digital identity services

Benefit	% of respondents
It would be a quicker process than verifying with physical ID	32%
It would allow me to verify my identity when I do not have physical ID to hand	32%
It could save me time or money	30%
It would be a more convenient process than verifying with physical ID	29%
It allows me to prove my identity when otherwise I would not be able to	26%
I would be able to re-use a digital identity I have already used previously	23%
The information I provide about myself would be stored securely	21%
The service would protect me against potential identity theft or fraud	21%
I would not have to share more information than is necessary	18%

I would be able to get support and assistance when I need it	17%
I do not perceive there to be any benefits	13%
Don't know	8%

Source: Perspective Economics, Survation (n = 5,658 (weighted)), Multiple choice question (percentages do not sum to 100%)

The perceived benefits of digital identity tend to focus upon three broad themes for end users, including convenience and speed, access and inclusion, and security and data minimisation. The most commonly cited benefits relate to convenience and speed. Approximately a third of respondents cited quicker verification (32%), the ability to verify without having physical ID to hand (32%), time or money savings (30%), and greater overall convenience (29%). The consistency across these four items suggests that the primary appeal of digital identity for most consumers is a practical one, where this can be used as a faster and more flexible alternative to physical documents or waiting for manual checks.

Access and inclusion is also important for several respondents, where a quarter (26%) cited the ability to prove their identity when they otherwise would not be able to, and 23% valued the ability to re-use a digital identity across multiple services. For respondents who lack access to traditional identity documents, digital identity may represent a means of accessing services that would otherwise be harder to access.

Approximately one in five respondents cited secure storage of personal information (21%) and protection against identity theft or fraud (21%), while 18% valued the principle of data minimisation i.e. not having to share more information than necessary.

Notably, 13% of respondents stated that they do not perceive any benefits to digital identity, and a further 8% selected 'don't know'. Taken together, approximately one in five respondents (21%) either see no benefit or are uncertain.

Overall views on the development of digital identity in the UK

Respondents were subsequently asked how they view the overall development of digital identity services in the UK, and how important they believe these services will be over the next five years.

Figure 4.13: Overall view on the development of digital identity services in the UK

View	% of respondents
Very positive	17%
Somewhat positive	26%
Neither positive nor negative	28%
Somewhat negative	10%
Very negative	14%
Don't know	6%

Source: Perspective Economics, Survation (n = 5,658 (weighted))

Overall sentiment towards the development of digital identity services is moderately positive. Over four in ten respondents (43%) hold a positive view (17% very positive, 26% somewhat positive), compared with approximately a quarter (24%) who hold a negative view (10% somewhat negative, 14% very negative). The largest single group is those who are neither positive nor negative (28%), suggesting a high portion are either uncertain, or waiting for further enaction of digital identity policy and use cases prior to forming an overall view. The proportion holding a negative view (24%) is somewhat higher than the proportion who reported no perceived benefits of digital identity (13%), suggesting that some respondents who recognise the potential benefits of digital identity nonetheless have reservations about the direction of its development in the UK. The 14% who are 'very negative' is also higher than the 10% who are only 'somewhat negative', which may reflect deeper concerns around perceived surveillance, data security, or the perceived risk of digital identity becoming embedded or required by certain services.

Figure 4.14: Perceived importance of digital identity services in the next five years

Importance	% of respondents
Very important	34%
Quite important	37%
Not that important	9%
Not at all important	8%
Don't know	12%

Source: Perspective Economics, Survation (n = 5,658 (weighted))

Regardless of whether they view the development positively or negatively, a clear majority of respondents (71%) believe that digital identity services will be important over the next five years (34% very important, 37% quite important). Only 17% consider them unimportant (9% not that important, 8% not at all important), with 12% unsure. While only 43% of respondents view the development of digital identity positively, 71% believe it will be important. This suggests that many consumers see digital identity as an increasingly significant part of how services will operate, whether or not they personally welcome that trajectory. In other words, the perception is that there will be an increased rollout of digital identity solutions. This finding has practical implications for the sector. It suggests that adoption is likely to continue growing as digital identity becomes embedded into more services and use cases, but that building public confidence and trust, alongside expanding availability, will be critical to ensuring that growth is accompanied by consumer support.

Section Summary

- Consumer understanding and use of digital identity appears to have risen since the baseline. 81% of respondents report some level of understanding of digital identity, up from 71% at baseline. 77% report having used a digital identity service for at least one purpose. Both figures use a refreshed and weighted survey design, so direct comparisons should be read in line with the methodology updates.
- Preference for digital identity appears strongest in online contexts (age-restricted online purchases, accessing public services). Physical document preference remains dominant for in person scenarios. The survey highlights that preferences can vary substantially across different use cases.
- Among non-users of digital identity services (23%), the most frequently cited reasons are preference for physical ID and absence of a perceived need, rather than access barriers.
- 71% of respondents believe digital identity services will be important over the next five years. 43% view the current direction of development positively and 24% negatively.

Annex

Annex A: Taxonomy

Taxonomy and Sub-area	Definition
Identity Foundations	
Identity issuance	Creating and distributing identity credentials
Identity and consent management	Individuals can control their identity data and its usage (e.g., consent dashboards, data rights management, privacy controls)
Digital wallets	Protected digital storage solutions for identity credentials and verified attributes (e.g., mobile identity storage, credential apps)
Identity services	Platforms providing identity-related services to support other systems
Identity Verification	
Document based	Verifying identity using official documents (e.g., passport verification, driving license validation)
Biometrics, liveness detection and verification security	Using physical characteristics to verify identity and presence, and verifying the authenticity and provenance of biometrics
Knowledge Based Verification	Verifying identity through personal information questions (e.g., historical data)
Social verification (vouching / proofing)	Verifying identity through social connections or professional references
Attribute Verification	
Age assurance	Verifying a person's age without full identity disclosure (e.g., age band estimation, date of birth validation)
Professional and credential verification	Validation of qualifications and credentials through authoritative sources (e.g., right to work checks, qualification verification, professional memberships)
Background screening	Comprehensive verification of personal and organisational history through multiple data sources (e.g., criminal record checks, sanctions screening)
Financial and address verification	Verification of financial and residence information (e.g., bank account validation)

Trust Services	
Digital signatures (eSignatures)	Electronic signatures to verify document authenticity or establish audit trails (e.g., qualified electronic signatures and seals)
Certificates	Digital documentation confirming identity or attributes (e.g., SSL certificates)
Authentication	Verifying the identity of a user or system
Governance and compliance	Ensuring identity systems meet regulatory requirements
Identity Data and Intermediaries	
Data brokerage	Services that aggregate and distribute identity data
Orchestration and interoperability	Coordinating various identity systems and ensuring they work together with established standards
Risk, fraud and credit	Evidence-based assessment of identity risks and financial standing (e.g., fraud detection, risk scoring)
Analytics and insights	Analysing identity data for patterns and insights

Annex B: Survey Questionnaire

We set out indicative questions included within the consumer attitudes survey (Section 4) below. Please note these have been summarised for use within this annex.

Section A: Demographics and Screening

S1. What is your gender?

S2. What is your household income?

S3. How many dependents aged 13–17 years old do you have, if any?

S4. Which of the following types of housing tenure best describes the accommodation you live in?

S5. Question for Socio-Economic Groups

S6. Highest level of qualification

Section B: Health and Disability

D1. Do you have any physical or mental health conditions or illnesses lasting or expected to last for 12 months or more?

D2. Do any of these conditions or illnesses affect you in any of the following areas?

- Vision (for example blindness or partial sight)
- Hearing (for example deafness or partial hearing)
- Mobility (for example walking short distances or climbing stairs)
- Dexterity (for example lifting and carrying objects, using a keyboard)
- Learning or understanding or concentrating
- Memory
- Mental health
- Stamina or breathing or fatigue
- Socially or behaviourally (for example associated with autism, attention deficit disorder or Asperger's syndrome)
- Other

D3. Does your condition or illness/do any of your conditions or illnesses reduce your ability to carry out day-to-day activities?

Section C: Language

L1. What is your main language?

Section D: Identity Documents

ID1. Do you possess any of the following forms of ID? Please select all forms of ID you possess.

- A UK or Northern Ireland photocard driving licence (full or provisional)

- A driving licence issued by the EU, Norway, Iceland, Liechtenstein, the Isle of Man or any of the Channel Islands
- A UK passport
- A passport issued by the EU, Norway, Iceland, Liechtenstein or a Commonwealth country
- None of the above

ID2. Do you possess any of the following forms of ID?

Type: Multi-select

Note: *Secondary and supplementary identity documents.*

- PASS card (National Proof of Age Standards Scheme)
- Blue Badge
- eVisa or biometric residence permit (BRP)
- Defence Identity Card (MOD form 90)
- National identity card issued by the EU, Norway, Iceland or Liechtenstein
- Northern Ireland Electoral Identity Card
- Voter Authority Certificate
- Anonymous Elector's Document
- Older person's bus pass
- Disabled person's bus pass
- Oyster 60+ card
- Freedom Pass
- Scottish National Entitlement Card (NEC)
- 60 and Over Welsh Concessionary Travel Card
- Disabled Person's Welsh Concessionary Travel Card
- Northern Ireland concessionary travel pass
- None of the above

ID3. Have you ever legally changed either your name or your gender? For example, this could be if you have changed your name when you got married, or if you have changed your gender on official documents.

ID4. Thinking of the children in your household, do they possess any of the following forms of ID? Please select all forms of ID they possess.

Note: *Asked of respondents with children in household.*

- UK or Northern Ireland photocard driving licence (full or provisional)
- Driving licence issued by the EU, Norway, Iceland, Liechtenstein, the Isle of Man or any of the Channel Islands
- UK passport

- Passport issued by the EU, Norway, Iceland, Liechtenstein or a Commonwealth country
- PASS card (National Proof of Age Standards Scheme)
- Blue Badge
- eVisa or biometric residence permit (BRP)
- National identity card issued by the EU, Norway, Iceland or Liechtenstein
- Northern Ireland Electoral Identity Card
- Concessionary Travel Card (e.g. a bus pass with proof of age)
- None of the above

Section E: Digital Access and Skills

DA1. Which of these best describes your use of the internet? Please include all use of the internet, on all of your devices. This may include use of internet browsing, internet banking, online shopping, use of email and social media.

DA2. Thinking about your digital skills, please indicate whether you can or cannot do the following tasks on any device (e.g. phone, computer, or tablet).

Type: Multi-item grid (can/cannot for each) *Based on Lloyds Consumer Digital Index foundation-level tasks.*

- You can turn on the device and enter any account login information as required
- You can use the available controls on your device (e.g. mouse, keyboard, touchscreen)
- You can use the different settings on your device to make it easier to use (e.g. changing the font size)
- You can find and open different applications/programmes on your device
- You can set up a connection to a Wi-Fi network on your device
- You can open an internet browser to find and use websites
- You can keep your login information and passwords for a website safely
- You can update and change your password when prompted to do so

DA3. Do you or do you not have the following things?

- WiFi connection at home
- A computer, laptop, or tablet/iPad at home
- A personal mobile phone
- A mobile phone with access to cellular data (wireless mobile internet connection)

Section F: Understanding and Experience of Digital Identity

Q1. To what extent, if at all, do you understand the concept of a digital identity?

Type: Single select (scale)

Q2. To your knowledge, have you had experience proving your identity when doing any of the following? Please select all that apply.

Type: Multi-item grid (digitally/physically/both/neither for each use case)

Note: *For this question, 'proving your identity digitally' means using an app or website to verify who you are, rather than showing physical documents in person. Use cases presented include financial services, employment, government services, healthcare, travel, age-restricted purchases, property, education, and other contexts.*

Q3. You haven't proved your identity with digital services. What are the main reasons for this?

Type: Multi-select

Note: *Asked of respondents who indicated no digital identity experience at Q2.*

- I haven't had to prove my identity
- No digital option has been provided
- I didn't have the right documents available (passport, driving licence etc.)
- I didn't have the required technology (smartphone, device)
- I am not comfortable using this technology
- I tried but had to use a physical option
- I have privacy or security concerns about using digital identity services
- I don't trust the provider
- I prefer using physical ID when possible
- I don't understand how to use it
- Other (please specify)
- Don't know
- Prefer not to say

Section G: Usability and Support

Q4. Thinking about the last time you used a digital identity service, was the service easy to use?

Note: *Asked of respondents with digital identity experience.*

Q5. Was there a time when you were unable to access a digital identity service online due to an error or problem (e.g. could not load the page)?

Type: Single select

Q6. How often have you experienced any technical issues or downtime when using digital identity services?

Type: Single select (frequency scale)

Q7. Have you ever needed help or support from the service provider while using a digital identity service?

Type: Single select

Q7a. Did you receive support from the service provider when needed?

Type: Single select

Note: *Asked of respondents who needed support at Q7.*

Q8.1. Please describe your experience of receiving support. Please select all that apply.

Type: Multi-select

Note: *Asked of respondents who received support.*

- I accessed support online
- I asked for support non-digitally (by phone or in person)
- It was difficult to find
- Getting a response took a long time
- I was able to find support, but they were not able to give me the assistance I needed to resolve my issues
- None of the above

Q8.2. Please describe your experience of not receiving support. Please select all that apply.

Type: Multi-select

Note: *Asked of respondents who did not receive support.*

- I was not able to find the online support (e.g. email or chat assistance) I wanted
- I wanted non-digital support (e.g. phone or in-person assistance) and was unable to find it
- None of the above

Section H: Transparency and Privacy

Q9. When you last used a digital identity service, did it give you enough information to feel safe and confident sharing information about yourself?

Type: Single select

Q10. When you last used a digital identity service, how transparent do you feel the service provider was about who they are, how they operate, and how the process works?

Type: Multi-item grid (scale for each)

- Who the provider was (the company or organisation behind the service)
- What they do with your information
- How the identity verification process works

Q11. For you to feel safe and confident in sharing information about yourself, how important, if at all, is it to know the following information about the digital identity service?

Type: Multi-item grid (importance scale for each)

- Who the provider is
- What they do with your information
- How the identity verification process works
- What standards or certifications the provider holds

Q12. When you last used a digital identity service, did it explain what personal information they would collect from you?

Type: Single select

Q13. Did the service explain why they would collect this information from you?

Type: Single select

Q14. When you last used a digital identity service, did you understand how the digital identity service would use the information you provided to verify your identity?

Type: Single select

Q15. When you last used a digital identity service, did you feel confident that the information you provided was kept as private as possible?

Type: Single select

Q15a. Thinking about the last time you used a digital identity service, did the service you used provide options for you to control or limit how your personal information would be shared with third parties?

Type: Single select

Section I: Attitudes and Preferences

Q16. Digital identity services allow you to prove who you are online or in person using your mobile phone or other digital device. These services verify your identity by checking information from documents like passports or driving licences. To what extent do you agree or disagree with the following statements?

Type: Multi-item grid (agreement scale for each)

Note: *Approximately six attitudinal statements were presented.*

Q17. If both government and private sector digital identity options were available, which would you prefer?

Type: Single select

Q18. How important are the following factors if/when using a digital identity provider?

Type: Multi-item grid (importance scale for each)

- Security of my personal data
- Privacy – my data will not be shared with third parties beyond the identity check
- Ease of use
- Adheres to government or independent standards
- Cost (free vs paid services)
- How widely accepted it is by other services
- Quality of customer support
- Transparency about how my data is used
- Ability to control what information is shared
- Speed of verification process

Section J: Benefits, Challenges and Concerns

Q19. What do you think are the benefits of using a digital identity service compared to physical IDs like a passport or a driving licence? Please select all that apply.

Type: Multi-select

- It would be a quicker process to prove my identity
- It would be a more convenient way to prove my identity
- I would be able to re-use a digital identity across multiple services
- It allows me to prove my identity without carrying physical documents
- It would allow me to verify my identity from anywhere
- I would be able to get support if I had issues verifying my identity
- The information I provide about myself would be more secure
- I would not have to share more personal data than is necessary
- The service would protect me against fraud or identity theft
- It could save me time or money
- Other (please explain)
- I do not perceive there to be any benefits
- Don't know

Q20. What do you think are the challenges of using a digital identity service compared to physical IDs like a passport or a driving licence?

Type: Multi-select

Note: *Includes open-text follow-ups for accessibility, trust and other.*

- The service would be too complicated to use
- I would not feel confident using a technology I do not know
- I would find it difficult to complete the selfie/video process
- I would not find the services accessible (please explain why)
- I would not be sure how my privacy was being protected
- I would not be sure how data about me would be used, shared or stored
- I would not trust the digital identity provider (please explain why)
- I would not have the right technology to access the service
- I'm wary of what happens if the technology or device fails
- I do not have the right identity documents to make use of the service
- Other (please explain)
- I do not perceive there to be any challenges or downsides

- Don’t know

Q21. For each of the following situations, please indicate your preference.

Type: Multi-item grid (physical/digital/no preference for each)

Note: *Preference for physical versus digital identity verification by use case.*

- Proving my age in person (e.g. in a bar, restaurant or cinema)
- Making age-restricted purchases online
- Making age-restricted purchases in shops
- Opening a bank account or financial product
- Renting or purchasing property
- Applying for jobs and undertaking right to work checks
- Accessing government or NHS services
- Healthcare appointments
- Travelling outside of the UK or Ireland

Q22. What concerns, if any, do you have about digital identity services? Please select all that apply.

Type: Multi-select

- Security breaches or hacking
- Government surveillance
- Commercial use of my data
- Identity theft
- Loss of privacy
- Technical failures or service outages
- Exclusion of people without smartphones
- Being required to use them instead of physical ID
- Cost
- Lack of trust in providers
- Don’t understand how they work
- Other (please specify)
- No concerns

Section K: Overall Outlook

Q23. Overall, how do you view the development of digital identity services in the UK?

Type: Single select (scale)

Q24. How important do you think digital identity services will be in the next five years?

Type: Single select (scale)

Q25. Is there anything else you'd like to tell us about your views or experiences on using digital identity services?

Type: Open text