

DIGITAL IDENTITY IN **2025**: A TRENDS REPORT BY ONEID®

SIX TRENDS ACCELERATING DIGITAL
IDENTITY ADOPTION IN THE UK.

2025 – THE YEAR OF DIGITAL IDENTITY IN THE UK.

Digital has become the default to how we lead our lives. So many of our interactions and exchanges happen without meeting each other even once. High-value contracts are signed, people are hired, recurring payments are set up, goods and services are bought and sold, and much more is done with our screens as the primary interface.

This shift has undoubtedly made our lives more convenient. But the question always looms: **'Do we really know who is on the other side?'** This veil of screens is putting individuals and businesses at risk of fraud and harm. **Fraud and computer misuse account for 50% of all crimes.**

While businesses know the risks, many are concerned about the friction, complexity, and ineffectiveness of traditional verification measures in the digital age.

However, the trends and developments surrounding modern business indicate a shift in how user verification will be viewed. Digital identity solutions, purpose-built for the digital age, enable seamless experiences, deliver robust security, and are easy to integrate. But they go beyond verification.

Organisations are seeing the broader business case for integrating a digital identity solution, with its ability to speed up processes, minimise errors, and reduce costs.



SUMMARY

Digital Identity in 2025: A Trends Report by OneID® points to the six factors that will make digital identity a priority for businesses like yours in 2025.

1. The evolving nature of fraud and its rising cost:

AI-driven deepfakes and account takeovers have surged in cases and losses, making robust digital identity solutions essential for businesses.

2. Policy and regulation momentum:

New regulations like the Data (Usage and Access) Bill will pave the way for wider adoption of digital identity, while the Online Safety Act will make its implementation a compliance requirement.

3. Global standardisation and interoperability:

International initiatives focussed on creating solutions compatible with different digital identity solutions across borders will broaden its coverage.

4. A focus on privacy and convenience:

Customers' demand for secure, private, and frictionless digital experiences can only be answered by privacy-preserving digital identity solutions that put users in control.

5. Identity as a business enabler:

With their ability to unlock operational efficiencies and add measurable value, digital identity solutions are being viewed as a digital transformation tool.

6. SME-driven demand for lean solutions:

SMEs require simple, scalable digital identity solutions to address fraud and improve operations.

The tide has been welling for wider and faster adoption of digital identity verification in the UK. With emerging technologies, evolving regulations, and changing business needs, 2025 is set to be a pivotal year for digital identity.



1. FRAUD IS COSTING MORE AND IS HARDER TO IGNORE

With the increasing use of AI-powered deepfakes, rising cases of payment fraud, and revised regulations like the Payment System Regulator's reimbursement recommendations, businesses will no longer be able to dismiss losses due to fraud as the 'cost of doing business'.



Digital identity solutions can help businesses protect their bottom lines from fraudsters.

2137%

rise in deepfake fraud attempts in the last three years¹

Cifas members have raised concerns about difficulty in identifying forged documents because they are so well-produced. Easy access to advanced AI technology and the availability of social data on almost anyone will only make this challenge even harder.²

was stolen in payment fraud just in the first half of 2024.³

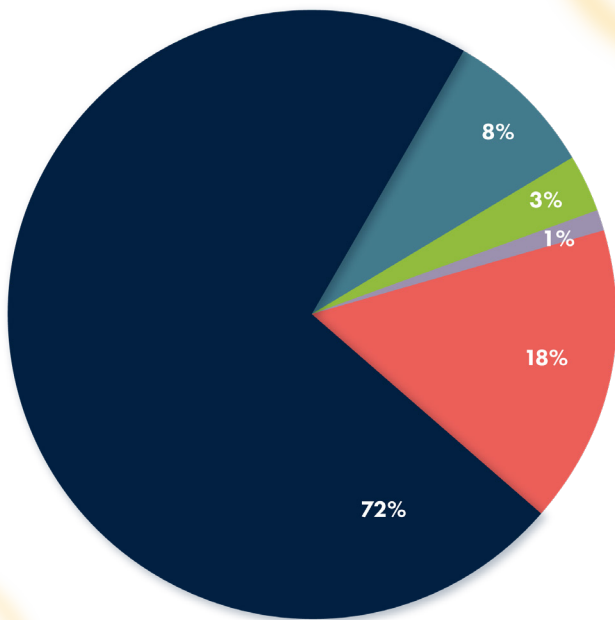
£570 MILLION

1-4%

turnover lost by businesses to fraud.⁴

1. [The Battle Against AI-driven Identity Fraud](#)
2. [Cifas Fraudscape 2024 – 6-Month Update](#)

3. [UK Finance 2024 Half-Year Report](#)
4. [BDO LLP Fraud Survey](#)



Online channels account for **72%** of cases of Authorised Push Payment (APP) Fraud.

- Online
- Telecom
- Email
- Other
- Unspecified

PSR'S REIMBURSEMENT REQUIREMENT WILL MAKE FRAUD MORE EXPENSIVE FOR BANKS.

Authorised Push Payment fraud happens when scammers trick people into authorising payments, believing they're legitimate. Until now, banks reimbursed victims under a Voluntary Code, often recovering costs from businesses.

From October 2024, new PSR rules require victims to be fully reimbursed. Even though APP fraud losses dropped by 11% in H1 2024 compared to 2023, PSR's new rules will increase businesses' costs. In H1 2024, £213.7 million was lost to APP fraud, with 59% (£126.7 million) reimbursed⁵. If similar losses occur in H2 and full reimbursement applies from October, the total cost to businesses could reach £296 million in 2024.

Reimbursement to victims of APP fraud in 2023 and 2024

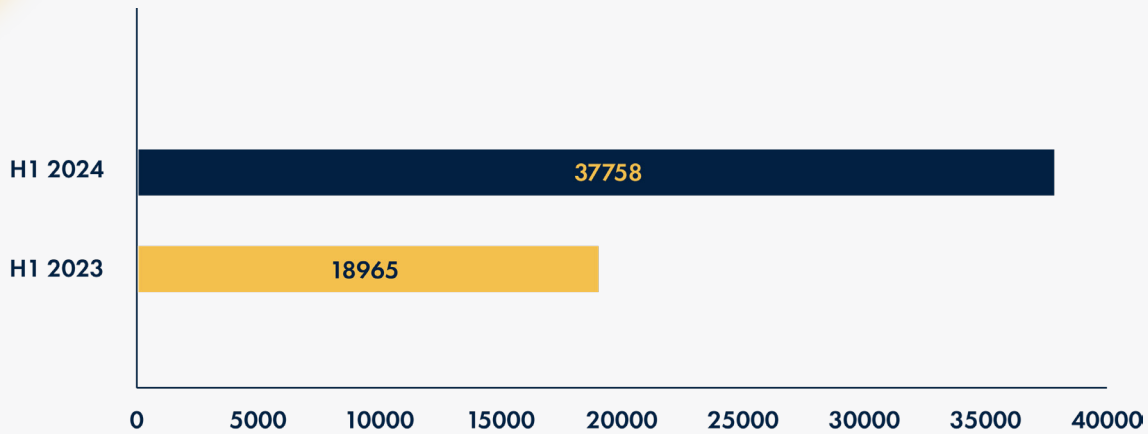
Year	H1	Jul-Sept	Oct-Dec	Total
2023	£152.8 mn	£134.5 mn		£287.3 mn
2024	£126.7mn	£63.04 mn ⁶	£106.85 mn ⁷	£296 mn

5. [The Battle Against AI-driven Identity Fraud](#)

6. Assuming the losses from fraud in H2 2024 were the same as H1 2024, and the reimbursement between Jul-Sept 2024 was 59% of the loss value.

7. Assuming the losses from fraud in H2 2024 were the same as H1 2024, and the reimbursement between Oct-Dec 2024 was 100% of the loss value as per PSR's requirements.

99% INCREASE IN ACCOUNT TAKEOVER FRAUD



Account or facilities takeover fraud is when a fraudster gains access to an account – by hacking the account or posing as someone who has lost access to the account – and makes unauthorised transactions. According to Cifas, over 37,000 account takeover cases were filed with the National Fraud Database in the first half of 2024, almost double the same time in 2023. 69% of these incidents were done using online channels.

HOW ONEID® CAN COUNTER THE FRAUD THREATS OF 2025.

The best way to prevent fraud is to be absolutely certain about who you're paying or who is paying you before the money exchanges hands. OneID® verifies an individual using identity data that has passed the banks' stringent KYC checks and is constantly monitored for money laundering activities or account compromises.

To know who an individual is, OneID® asks the individual to log in to their mobile banking app or online banking account. By using the bank's strong customer authentication measures and the identity data returned by the bank, OneID® helps businesses know for sure who they are dealing with.

£710 MILLION WORTH OF UNAUTHORISED FRAUD WAS PREVENTED BY THE BANKS

A document-free process eliminates the possibility of deepfakes, or AI-enabled identity document abuse.

Account verification, along with identity checks, remove the possibility of payment fraud or money mules.

Account servicing, using bank-based verification eliminates the risk of someone hacking into an account with socially available information.

Schedule a meeting with [Keith Mabbitt](#) to understand how OneID® can help you.

2. POLICY DEVELOPMENT AND IMPLEMENTATION FOR DIGITAL IDENTITY IS GAINING MOMENTUM

The UK government and its counterparts worldwide are developing policies to strengthen the digital identity framework and expand its usage in more sectors and everyday situations. These initiatives will enhance the trust, adoption, and interoperability of digital identity services, ultimately protecting businesses and individuals from online fraud and harm.

DATA (USAGE AND ACCESS) BILL

The bill, expected to be passed in Spring 2025, will give the UK's Digital Identity and Attributes Trust Framework (DIATF) a legal foundation. It will also pave the way for 'smart data' schemes, which will follow Open Banking's success in enabling secure data sharing.

With the bill, the Department for Science, Innovation, and Technology (DSIT) will be able to:



Certify digital identity providers.



Issue trust marks for compliant solutions.



Enable secure sharing of government-held data with certified third parties.

OFFICE FOR DIGITAL IDENTITIES AND ATTRIBUTES (OfDIA)

OfDIA will work to develop digital identity standards in the UK and oversee DIATF, driving the implementation of interoperable and secure systems.

OfDIA's work will focus on:

Creating
high-trust frameworks
for seamless identity
data exchange.

Expanding
use cases in finance,
e-commerce, and
public services.

Championing
privacy-by-design and data
minimisation

UK DIGITAL IDENTITY AND ATTRIBUTES TRUST FRAMEWORK (DIATF) GAMMA VERSION

In November 2024, the gamma version of UK DIATF was introduced, which lays the groundwork for innovative, interoperable and trusted digital identity services.

Along with the three existing roles – Identity Service Provider (IDSP), Attribute Service Provider (ASP) and Orchestration Service Provider, it introduces two new roles.

1. Holder service providers (HSPs) will enable users to store, manage and reuse their identity and attribute information using digital identity wallets like OneID® Wallet. Businesses will be able to elevate the onboarding experience they deliver with a user-centric identity management that meets privacy and security standards, and reduces friction.

2. Component service providers (CSPs) specialise in just part of the various identity verification or authentication processes, such as fraud checks or biometric face scans. This would enable businesses to leverage specialised services to improve accuracy, streamline operations, and reduce costs associated with in-house identity management.

CORPORATE IDENTITY WALLETS

The Centre for Finance, Innovation and Technology (CFIT) is working with certified identity providers like OneID® to build upon the certification of individuals to establish a 'corporate ID' model to reduce economic crime related to fraudulent companies.

The Corporate Identity Wallet will enable:

Verified data sharing
by businesses with banks, regulators and other stakeholders safely and instantly.

Fraud reduction
by using bank-verified data to ensure accuracy and reliability – tackling impersonation and fraudulent businesses.

Interoperability
by integrating seamlessly with DIATF, ensuring compatibility across sectors.

THE ONLINE SAFETY ACT (OSA)

The Online Safety Act continues to reshape the digital landscape in the UK, with significant milestones and compliance measures slated for 2025⁸. The Act puts greater accountability on online businesses to remove illegal and harmful content and prevent children from accessing it on their platforms.

Learn more at the OneID® [OSA Knowledge Hub](#).



AGE VERIFICATION FOR ALCOHOL PURCHASE USING DIGITAL ID

DSIT, after consulting with various parties, announced that digital identity could be used for age verification for the sale of alcohol. This will reduce the use of fraudulent IDs and eliminate the need to show a passport or driver's license to buy alcohol.

OneID® uses bank-verified data to establish with absolute certainty that **an individual is over 18** – taking out the possibility of errors that comes with facial age estimation.

ELECTRONIC IDENTIFICATION AND TRUST SERVICES (eIDAS) 2.0

The updated EU identity regulation, eIDAS 2.0, introduces the European Digital Identity Wallet—a secure, user-centric solution putting individuals in control of their personal data.

Users can now manage and share their identity data seamlessly across borders, ensuring secure and effortless access to public and private services throughout the EU.

eIDAS 2.0 will ensure:

Universal Access
Secure ID services for all
EU citizens.

Enhanced Security Supports
trusted services like diplomas,
professional certificates,
and electronic ledgers.

Interoperability:
Users can share data with any
eIDAS 2.0-certified
identity service

DRIVING LICENSES GO DIGITAL IN THE US, AUSTRALIA AND OTHER MARKETS.

The adoption of digital driving licences is gaining momentum, with countries like the US, Australia, and others leading the way. These digital licences provide a secure, convenient alternative to physical cards, enabling users to access their driving credentials via mobile devices.

The UK has an opportunity to accelerate its pace and align with faster-advancing global initiatives. By doing so, it can fully harness the potential of secure digital transformation as a driver of growth and innovation.

Contact Adrian Field

to learn more about
policy developments
around digital identity
and what it could mean
for your business.



3. THE GLOBAL MOVE TOWARDS STANDARDISING IDENTITY VERIFICATION SOLUTIONS

As businesses and individuals navigate an increasingly interconnected world, the push to standardise identity verification solutions is gathering momentum. This will become the cornerstone of a truly digital identity solution.



From centralised to decentralised models:

Established systems like Singpass, Aadhaar, and Estonia's eID are evolving alongside federated frameworks like OpenID Connect and eIDAS. The next frontier? Decentralised identity models powered by 'web3' technologies such as W3C Verifiable Credentials.



The UK already on course:

While the UK isn't part of eIDAS, the DIATF's Gamma version introduces the Holder Service Provider role, which lays the groundwork for interoperability and seamlessness among digital identity wallets and the adoption of VCs. Significant progress is anticipated in 2025¹⁰.



Paving the way for verifiable credentials and digital identity wallets:

This progress will fuel the adoption of Verifiable Credentials (VCs) – enabling individuals to easily store their identity, qualifications, and other verified attributes in a digital identity wallet and share it with anyone, globally, at the tap of a button.



Businesses and individuals set to gain:

Interoperable, standards-driven identity solutions will enable seamless global verification while aligning with local regulations like the UK's DIATF and Europe's eIDAS. This is an unparalleled opportunity to build trust, enhance user experiences, and unlock global opportunities.



Europe leading the charge on compatibility:

The European Digital Identity (EUDI) Wallet pilot is underway in 19 countries and Ukraine, with rollout expected by 2025. By the end of 2025, analysts predict 83 million wallets in use, doubling to 169 million by 2026. Nordic countries are poised to lead early adoption⁹.

9. [Important dates for Online Safety Compliance](#)

10. [Mlex/ Digital ID sector expects clarity in 2025 as UK framework tries to mirror EU's](#)

4. PRIVACY AND CONVENIENCE CONTINUE TO BE SUPREME

Gone are the days when users blindly clicked 'Log in with Facebook'. They are more conscious about who is accessing their data, how it is being used, and how it will be stored – and are asking if they need to do.

Processes that cause friction are processes that create dropouts. As people juggle more things than ever at any given moment, verification processes that fit right into what they are highly likely to be completed.



Data Minimisation:

Solutions that collect only the essential information are the future.



User Empowerment:

Giving users control over what they share and when builds trust and loyalty.



Anywhere Access:

Verification solutions must work anytime, anywhere—no specific lighting or location required.



Instant and Intuitive:

The faster and simpler the process, the more likely users will complete it.

[Schedule a meeting with John-Michael Eastman,](#)
to learn about OneID®'s privacy preserving and user-centric approach

5. BUSINESSES EXPECT MORE FROM THEIR VERIFICATION SOLUTION

At the same time they are looking to meet contrasting priorities of strict KYC compliant checks but without hampering the user experience. This is where traditional verification methods of scanning and uploading falter.

- **Remembering repeat visitors:**
Businesses want to delight digital natives by delivering a personalised experience even when they are not signed in.
- **Streamlining workflows:**
Solutions that cut out unnecessary steps like manually verifying documents or typing in forms are highly valued.
- **Onboarding without friction:**
Faster and easier customer onboarding and reduced time to serve will help improve satisfaction rates.
- **Reducing costs:**
The search is always on for solutions that minimise operational costs while optimising resource reduction.
- **Improving customer relationship management:**
Accurate and up-to-date data about customers can help build closer and stronger relationships with them.
- **Enhancing loyalty and satisfaction:**
Building trust and loyalty by delivering seamless, user friendly solutions is always a priority.

What else should you keep in mind when choosing a digital identity solution?

Our Digital Identity Buyer's Guide answers in detail.



6. SMEs WILL DRIVE THE DEMAND FOR LEAN SOLUTIONS

Small- and Medium-sized Enterprises that don't have the budget to spend or a team to monitor the digital identity verification solution dedicatedly will have to be approached in a completely different way. Solutions that can be integrated easily, scaled as per needs, and work on completely automated workflows with minimum human intervention will gain traction.

- **Efficiency is non-negotiable:**
With limited manpower, SMEs require easy-to-manage solutions. Manual verification is not an option and they need a process that doesn't require dedicated resources.
- **Fraud is a critical issue:**
Fraud hits SMEs harder than larger companies, which can afford to insure against it or price it in. For SMEs, robust fraud prevention is a top priority.
- **Seamless adoption:**
SMEs prefer no-code, web-based portals over complex integrations. SMEs want to avoid downtimes and prefer a solution that can be integrated and used immediately.
- **Agile and innovation-driven:**
SMEs are open to innovation and willing to adapt quickly.
- **Not limited by legacy systems:**
With no outdated systems to replace, SMEs are more flexible in adopting new solutions, free from the constraints of a historic IT infrastructure.
- **Government certification matters:**
While SMEs are pro-innovation, they rely heavily on government guidelines to ensure the safety and compliance of their identity service providers.

[Schedule a meeting with John-Michael Eastman](#) for a no-obligations chat.

○ About OneID®

OneID® is the only provider of truly digital, real-time identity services that create absolute certainty between a business and a customer, in the fastest, cheapest and safest way.

Our digital ID services use the most advanced counter-fraud measures to help protect banks, businesses and consumers from online identity fraud. By streamlining existing ID processes, including payments, direct debits, onboarding and more, we help businesses reduce operational costs, increase sales and improve customer engagement. As the only UK Identity Service with access to bank-verified data, nearly 50 million UK adults are already set up to use OneID®, for real-time verification.

OneID® is certified by the Age Check Certification Scheme (ACCS), which safeguards young people by preventing access to age-restricted products and services.

OneID® is certified as a Digital Identity Service Provider, authorised by HM Government's Department for Science, Innovation & Technology (DSIT), under their UK Digital Identity & Attributes Framework (DIATF). We were also the first Orchestration Service Provider to receive certification.

This allows OneID® to act as a hub to connect all of the UK's high street banks with providers and any online journey that needs customers to identify themselves.

Our certifications also include schemes such as Disclosure & Barring Service (DBS) checks for employee screening and Anti-Money Laundering (AML) compliant identity verification.

OneID® is regulated by the Financial Conduct Authority (FCA) to act as an Account Information Service Provider (AISP) under the Payment Services Regulations, 2017. This means OneID® is authorised, with customer consent, to use Open Banking infrastructure to capture personal data from banks and share it with selected parties in real time.

We are also a B Corp business.

To learn more visit www.oneid.uk



○ FOR MORE INFORMATION
Contact Keith Mabbitt,

keith@oneid.uk
07790 494 836