SERVE LEGAL
Empowering businesses to operate with confidence

Digital ID for Age-Restricted Sales

This report highlights the views of frontline Digital ID users, drawing on exclusive Serve Legal data, alongside our recommendations for effective Digital ID implementation and our ongoing commitment to supporting trusted, practical, privacy-first age assurance.

CONTENTS

Foreword

Serve Legal operates at the intersection between businesses and government regulation. They are the leading provider of ID, compliance and safety perception testing, dedicated to strengthening public safety through ensuring government and regulatory policy compliance across hospitality, retail venues and town centres. Serve Legal's highly trained cohort of 10,000 auditors carry out 250,000 tests a year across the UK's hospitality and retail sectors in a range of compliance areas including alcohol, vaping, and women's safety. Serve Legal therefore does not provide a digital ID product, but rather is well placed to provide sandbox testing and auditing of its implementation amongst its retailer clients including Tesco, Waitrose, and high street bars and restaurants.

1. Introduction

Digital identity is moving from concept to reality. From age checks in shops and bars to right-to-work, financial services and online safety, the question is no longer *if* Digital ID will be part of everyday life, but *how* it will work in practice – and whether people will trust it.

In November 2025, Serve Legal conducted a survey to understand the perspectives of two groups at the frontline of age-restricted sales and compliance: young consumers (through our nationwide auditor community) and retailers across supermarkets, convenience, betting, hospitality and online marketplaces.

With a database of over 10,000 highly engaged auditors, many aged 16–24, Serve Legal is uniquely placed to capture the views of the demographic most affected by Digital ID systems, particularly for alcohol, vaping and other age-restricted products. Our auditors are not only regular users of these environments; many also work in them. Alongside this, our clients include some of the UK and Ireland's largest supermarkets, hospitality businesses and leisure operators, giving us direct insight into operational realities and compliance pressures that digital ID will pose.

This report brings together the results of those surveys and our wider engagement in the Digital ID debate, including our involvement in the Westminster Policy Forum and evidence to the Home Affairs Committee inquiry on digital ID.

It focuses on key themes:

- Current usage, trust and privacy,
- Offline functionality, perceived benefits and implementation barriers,
- The conditions required for Digital ID to succeed.

Digital ID is not just a technical solution. It is a live question about operational reality, consumer trust and regulatory clarity.

2. Executive summary

Digital identity is moving from concept to operational reality across age checks, right-to-work, financial services and online safety. For age-restricted sales, the central question is no longer whether Digital ID will be used, but whether it will be trusted by young people and workable for retailers in real-world conditions. Serve Legal's November 2025 surveys of young auditors and retailers show clear potential benefits alongside firm requirements for success.

Auditors' views

Adoption remains low: only 7% of auditors currently use Digital ID for age verification. Views are divided on where it should be accepted, with a significant proportion opposed or undecided. Privacy is the dominant barrier (78%), and expectations for data minimisation are strong: 85% rate "proof-only" disclosure as significantly important. Trust is most likely to sit with government-issued solutions (56%), not private providers. Security confidence remains weak, and concern about losing access via phone loss is high. Practicality matters: 78% want offline functionality and 78% would only use Digital ID if it is free.

Retailers' views

Retailers see Digital ID as a possible enhancement to existing compliance frameworks, with potential to speed age checks, reduce fake ID and strengthen audit trails. But adoption is constrained by risk. Privacy concerns are widespread (59%), alongside anxiety about liability if systems fail or are spoofed (53%) and the impact of downtime (47%). Interoperability is non-negotiable (100%), and most also want clear government guidance and recognition. Offline resilience is viewed as essential by the majority.

What must be true for success

The data points to six conditions for confident rollout:

1. Proof-only, privacy-first design by default.
2. Reliable offline capability.
3. Clear, simple recovery processes.
4. Mandated interoperability.
5. Upfront clarity on liability and enforcement recognition.
6. Protection of digital inclusion with physical-ID fallbacks.

Serve Legal

Serve Legal works where policy meets frontline reality. With over 10,000 nationwide auditors - many aged 16–24 - and clients across major UK and Ireland retail, hospitality, betting and leisure operators, we provide real-world evidence on how age verification operates at checkouts, bars, doors and online. We support the development and testing of Digital ID through audits, pilots and advisory work, ensuring both operational practicality and young people's trust are reflected in implementation.

3. Young people's views: cautious, conditional and privacy-first

3.1 Current usage and overall sentiment

Despite being highly digital-native, only a very small proportion of auditors currently use a Digital ID for age verification – 7% reported doing so. Views on where Digital ID should be accepted are mixed. Nearly a third of respondents are comfortable with Digital ID being accepted everywhere that physical ID is used; 22% favour limited or context-specific use; and a notable 47% are opposed to Digital ID altogether or undecided.

This is not a rejection of technology. Rather, it reflects unresolved questions about who controls Digital ID, how data is handled and what happens if something goes wrong.

3.2 Trust, privacy and "proof-only" disclosure

Privacy emerged as the single most important barrier to adoption. When asked about obstacles to using Digital ID, 78% of auditors cited privacy concerns. Linked to this is a clear preference for data minimisation: 85% said that "proof-only" disclosure – where only proof of age is shared, and not wider personal details – is significantly important when using Digital ID in a store or venue.

Taken together, these findings show that young people are not prepared to accept a digital equivalent of a passport being handed over in full. They expect systems that share only what is strictly necessary, make that process transparent and give them control over how their identity data is used.

3.3 Who they trust to issue Digital ID

Contrary to some public debate, government involvement is not the main sticking point. When asked who they would trust most to issue a Digital ID, 56% of auditors chose a government-issued solution. Fewer than 5% said they would most trust a private provider, and 34% said they would not use a Digital ID at all.

Young people are therefore more comfortable with government-issued identity than with commercial schemes, but this trust is conditional. The concern is less about the idea of government involvement and more about safeguards, governance and the scope of use. There is also clear resistance among a significant minority who are uncomfortable with Digital ID in principle.

3.4 Security confidence and fear of losing access

Security is a major concern. Only 20% of auditors rated the security of Digital IDs highly, while 55% expressed low confidence. A related anxiety is what happens if access is lost: 57% said they were concerned about losing their Digital ID if they lost their phone.

These figures highlight the need for robust and clearly communicated security measures, as well as simple, trusted recovery processes in the event of device loss or compromise. For young people to adopt Digital ID, they must be confident that their identity is not only secure, but recoverable.

3.5 Offline functionality and cost

The expectation that Digital ID should work in real-life conditions came through strongly. A significant 78% of auditors said they wanted Digital IDs that can function offline. This reflects the reality of patchy mobile signal, limited data allowances and venues with unreliable connectivity. If Digital ID is pledging to offer a reliable solution, offline functionality must be considered.

Cost is another decisive factor, with 78% of auditors saying they would only use a Digital ID if it were free of charge and only 1% indicated they would be willing to pay. Any model that proposes to charge young people for basic identity functionality should therefore expect very low uptake.

3.6 Perceived benefits

Despite their concerns, auditors recognise meaningful benefits if Digital ID is designed and implemented well. The most frequently cited advantages were a reduced risk of losing physical documents such as passports and driving licences (identified by 67%), the convenience of having ID always available on their phone (60%), and faster checkouts or smoother access where Digital ID is accepted (44%).

In other words, the potential upside is clear: convenience, safety and a reduction in hassle. But these will not be enough on their own to overcome deep anxieties about privacy, security and loss of control.

3.7 Co-creation, not imposition

As Serve Legal CEO Kate Rand commented:

“Digital ID can’t be something we build in isolation and then try to sell to young people afterwards. It has to be co-created with them, with privacy and agency designed in from the start. Otherwise we will spend years trying to repair trust that we could have earned by involving them on day one. Serve Legal works to bridge the gap between the users, retailers and developers so a solution can be found that benefits all parties and ensures robust, compliant and efficient age verification moving into the future.”

Education will play a role, but auditors are clear that communication must be a two-way dialogue, not a one-way campaign once decisions have already been made.

4. Retailers’ views: opportunity tempered by risk

4.1 Compliance today

Retail respondents demonstrated a strong existing commitment to age-restricted sales compliance. 88% percent reported using training and refresher courses for staff, and 82% operate challenge policies such as Challenge 25. Digital ID is therefore being considered in the context of existing compliance frameworks, not as a substitute for them.

4.2 Perceived operational benefits

Retailers and operators see clear potential for Digital ID to help them manage risk and improve the customer experience. The most valued benefits include faster age checks, quicker service

at checkouts, bars and doors, a reduction in fake ID and fraud risk, and clearer audit trails that make it easier to evidence compliance.

These benefits align with broader industry trends towards streamlining compliance processes, reducing friction for customers and providing more robust documentation for regulators and enforcement bodies.

4.3 Concerns: privacy, liability and downtime

Alongside these advantages, retailers raised serious concerns about how Digital ID will work in practice. Privacy and data handling issues were the most commonly cited concerns, mentioned by 59% of respondents. Many businesses are wary of the responsibility and risk that might come with storing, processing or relying on sensitive identity data.

Liability is close behind. Just over half of retailers (53%) expressed concern about who would be responsible if the technology fails, is spoofed or produces an incorrect result. A further 47% highlighted the risk of technology faults or downtime affecting their ability to trade compliantly.

For retailers, these are not abstract worries. A failed system can mean a failed test purchase, a licensing breach, or a reputational hit that affects trust with customers and regulators. Until there is clarity about liability, redress and support, many will be cautious about relying on Digital ID.

4.4 Support needed for successful implementation

Retailers were clear about what they would need in order to adopt Digital ID with confidence. Interoperability emerged as a non-negotiable requirement: every respondent – 100% – agreed that systems must work together. No business wants to invest in a solution that proves incompatible with future standards or requires multiple overlapping systems at different sites.

Beyond interoperability, 81% said that clear government guidance and regulation would be essential, both to define acceptable use and to ensure that enforcement bodies recognise Digital ID as a legitimate means of age verification. 69% highlighted the importance of staff training, and 63% emphasised the need for ongoing technical support.

Offline functionality was once again prominent. 59% of retailers said offline capabilities were essential for their business, reflecting the reality of variable connectivity across stores, venues and geographic regions.

4.5 Who should bear the cost?

There is limited appetite among retailers for bearing the full cost of implementing Digital ID. When asked who should pay, 47% felt the responsibility should lie primarily with government or regulators. 29% favoured a shared responsibility between government and businesses. Only 18% thought businesses should cover the costs on their own.

This reflects a broader view that Digital ID is part of public and regulatory infrastructure, not simply a commercial tool. Retailers see it as something that delivers societal and regulatory benefits as well as operational ones, and expect funding models to reflect that.

5. Cross-cutting themes: what needs to be true for digital id to work

Bringing together the perspectives of young people and retailers, supported by Serve Legal's wider policy engagement, several common themes emerge.

5.1 Trust is the central issue

Both auditors and retailers see potential benefits in Digital ID, but trust is fragile. Young people worry about who controls their identity data, how it might be used and what happens when systems fail. Retailers worry about liability, enforcement and the impact of failures on their compliance and reputation.

Trust cannot be bolted on at the end through messaging campaigns. It has to be built into the design of systems, the governance frameworks around them and the enforcement model that underpins them.

5.2 Privacy and data minimisation must be designed in

The strong preference for "proof-only" disclosure and the dominance of privacy as a barrier demonstrate that minimal data sharing is not a "nice-to-have" feature; it is a foundational requirement. Systems that mimic the full data exposure of physical IDs in digital form are unlikely to secure broad support from younger users.

Design principles for Digital ID need to include strict data minimisation, clear transparency about what is being shared and why, and simple controls for users to manage their data. Retailers also need solutions that do not force them to store more personal data than necessary, given the associated regulatory and reputational risks.

5.3 Policy ambition must meet operational reality

Serve Legal's work on the high street and in hospitality environments shows that Digital ID will stand or fall on how well it works in real-world settings: at self-checkouts, in busy convenience stores, at nightclub doors, in betting shops and in online journeys that span multiple channels.

If systems are not designed with those environments in mind – including patchy connectivity, high footfall and varying levels of staff training – adoption will be uneven. Larger chains may invest early; independent retailers and smaller venues may hold back, creating an inconsistent and confusing experience for consumers.

5.4 Standardisation, recognition and enforcement

In evidence to the Home Affairs Committee and in discussions at the Westminster Policy Forum, Serve Legal has emphasised standardisation as a central advantage of Digital ID – but only if it is done well. A clear framework could reduce ambiguity across different forms of ID and make enforcement more straightforward. However, this requires recognition and backing from enforcement bodies such as Trading Standards and licensing authorities.

Local authorities and regulators will need sufficient time, resources and budget to oversee Digital ID solutions, verify their proper use and carry out audits. Introducing new tools without strengthening the enforcement ecosystem risks creating more confusion, not less.

5.5 Offline resilience, recovery and digital inclusion

Both groups in our surveys highlighted the importance of offline capability. In many parts of the UK and Ireland, connectivity cannot be taken for granted. Systems that fail without a signal will not be reliable enough for either customers or businesses.

Equally, recovery processes must be clear and accessible. Young people need to know what happens if a phone is lost or stolen, and how they can regain access to their Digital ID safely. Systems should also avoid deepening digital exclusion by assuming access to the latest devices, constant data connectivity or high digital literacy.

6. Implications for policy, industry and providers

Taken together, the findings point to three broad areas of action.

6.1 For government and regulators

Government must work with retailers, hospitality businesses, technology providers, young people and regulators from the outset. That means using real-world retail and hospitality environments as testbeds, and drawing on operational expertise before standards are finalised.

There is also a need for clarity on the legislative framework. Policymakers should set out how Digital ID interacts with licensing, age-restricted sales, right-to-work, money laundering regulations and online safety. Enforcement bodies must be equipped with the tools and budget to oversee the use of Digital ID and to enforce compliance fairly and consistently.

Finally, official recognition routes are crucial. Retailers and providers need to know which schemes meet the requirements for age verification and other regulated uses, and how recognition will be updated as technology evolves.

6.2 For retailers and hospitality operators

Businesses should engage early in pilots and trials to ensure that Digital ID solutions are tested in real conditions, rather than in controlled environments only. They should insist on interoperability and clarity about liability before committing significant resources.

Staff training will be critical. Frontline workers must understand not only how to use Digital ID technology but also how to explain it to customers and handle edge cases, such as system outages or customers who do not use Digital ID. At the same time, analogue fallbacks for those who rely on physical ID must remain in place. Staff need to be just as confident challenging both a Digital ID and a physical ID; audit programmes must be in place to manage the compliance of both.

6.3 For technology and Digital ID providers

Providers should treat privacy, “proof-only” disclosure and user control as core design requirements, not optional extras. Systems should be built to function reliably in offline or low-connectivity environments, and interfaces should be simple enough to use at pace, under pressure.

Security models and recovery processes must be transparent and communicated in plain language, especially for younger users and frontline staff. Providers should also expect to work

within a framework of recognised standards and independent assurance, rather than purely proprietary approaches.

7. Serve legal's role and ongoing commitment

Serve Legal operates where policy, business and everyday life collide: in shops, bars, restaurants and venues across the UK and Ireland, and increasingly in hybrid and online environments. Each year, our auditors complete hundreds of thousands of anonymous checks, giving us a unique view of how regulation is interpreted at the checkout, the bar and the door.

We are committed to three things:

- First, to providing high-quality, real-world data on how policy decisions play out in practice, and where Digital ID is helping or hindering compliance.
- Second, to supporting retailers and hospitality businesses as they test and refine Digital ID implementation through mystery shopping, audits and advisory work.
- Third, to amplifying the voice of young people – particularly around privacy, trust and usability – in policy discussions, standards development and product design.

Digital ID is not simply a technological upgrade. It is a reshaping of how identity, responsibility and safety are managed in public and commercial spaces. If it is built *with* the people who rely on it – young consumers, frontline staff, retailers, regulators and enforcement bodies – it can deliver genuine benefits for consumer safety, business efficiency and regulatory confidence.

Serve Legal is ready to be a partner in making that happen.

Terms of Reference:

Methodology and Respondent Profile

Young auditors: The auditor survey was completed by members of Serve Legal's nationwide network, the majority aged between 16 and 24. These respondents are frequent shoppers and regular users of age-restricted environments such as supermarkets, convenience stores, bars and leisure venues. A number also work in retail and hospitality, and are directly involved in carrying out age checks.

Questions covered current usage of Digital ID, attitudes to trust and security, expectations of privacy and "proof-only" disclosure, preferred issuers, offline functionality, perceived benefits and barriers to adoption.

Retailers and operators: The retailer survey included organisations from across our client portfolio. Just over half of respondents operated supermarkets or convenience stores, around a quarter came from betting shops or bookmakers, a further share from pubs, bars and nightclubs, and the remainder from online marketplaces.

All respondents operate in age-restricted contexts and are familiar with Trading Standards, licensing requirements and test purchasing. The survey explored perceived benefits and risks of Digital ID, implementation support needs, views on costs, and the importance of interoperability and offline resilience.