**<head> What are the biggest challenges in digital payments today?**

**<standfirst> Digital payment services are revolutionising e-commerce in the UK – but there are obstacles to overcome before they deliver their full potential. Here we run through the key challenges facing the sector, and the role digital identity providers can help overcome them.**

In a few short years, digital payments have gone from a novel innovation to becoming central to how the UK does business. The sector is increasingly diverse, involves a huge range of stakeholders from almost every industry, and is still growing rapidly. Total transaction value is expected to reach just under £360 bn GBP in 2023, and is set to grow to £633 bn GBP by 2027[[1]](#footnote-1).

These are staggering numbers, but there are still obstacles along the way to full consumer adoption, barriers that can prevent banks and retailers from capturing the full revenues the digital payment opportunity offers.

Chief among these is the need for a reliable and secure method for verifying a customer’s identity that can overcome the anonymity inherent to remotely-accessed digital services; let’s break down some of the challenges this capability would overcome.

**<subhead> Security concerns in the round**

The simple fact is that many people do not feel safe online.

Verifying a customer is who they say they are sounds like a simple process, but the difficulties in the process open up gaps that malicious actors can exploit.

From phishing attacks to intercepting data transfers to full-blown identity theft, fraudsters have various methods for stealing sensitive information via weak links or vulnerabilities in the system that they can then use to make unauthorised purchases. Hackers can gain access to the databases of banks, retailers and payment providers, putting customer data at risk.

These incidents can be rare, but along with the obvious financial threat, even mild occurrences carry substantial brand risk and can seriously dent consumer trust not only in the impacted institution, but in the digital payments space in general. The problem is huge, and growing: in the UK there were more than 226,000 individual cases of identity theft, overwhelmingly online, in 2021 alone – an increase of 22% on the year before[[2]](#footnote-2).

Digital ID services can play a crucial role in addressing these risks by providing a safe, reliable way for individual users to confirm they are who they say they are. They can allow providers to securely store and manage personal data, reducing the risk of breaches and building consumer faith in the system as a whole.

**<subhead> Complexity turns off consumers**

Not every consumer is at the cutting edge of technology, and even the most digitally-savvy is not necessarily patient. Inconvenience and complexity can discourage customers with better things to do than laboriously proving they are who they say they are. In the era of e-commerce, requiring ID documents is not only anachronistic, but places an undue burden on a customer for the privilege of wanting to complete a transaction.

Existing digital ID providers take an average of almost two minutes to complete an ID verification check, with some taking up to five minutes.

All this added time and extra clicks are to the detriment of any provider’s user experience, and ultimately detract from the engagement and loyalty they want to build with their customers. Ultimately, the damage is to revenues – the bottom line.

And the damage can be serious: digital banks in the US have reported abandonment rates of 55% for new account origination, with 43% of these abandonments occurring specifically thanks to unwieldy ID verification procedures[[3]](#footnote-3). Global e-commerce retailers, meanwhile, report average cart abandonment rates of as high as 69%.

The opportunity for providers who solve these issues is clear, not only in retained transactions but in brand value: 81% of customers say that a positive experience improves their perception of a brand[[4]](#footnote-4), while 76% say they would stop engaging with a company after only one poor online experience[[5]](#footnote-5).

In offering simple, straightforward and most important fast identity verification, and in doing so at a minimum of clicks and friction, digital ID services streamline the transaction pipeline. Personal data beyond financial information, such as shipping addresses, sizes and other preferences, can be stored and used to deliver bespoke experiences that will both make transactions easier, and encourage customer loyalty and retention.

**<subhead> Costs for providers**

Administering digital infrastructure is not necessarily automated, and manual human intervention can be required in even the most sophisticated solutions. All the infrastructure and the people who manage it need to be paid for, meaning that digital identity checks in the UK now cost an average of approximately £1.92 per transaction. Extrapolate this out across the entire economy, and we are seeing a enormous amount of value squandered unnecessarily.

On a macro scale, we can add to these costs the billions banks and other institutions spend developing and maintaining security processes and systems. Additionally, following up with customers after abandoned or failed transactions to encourage them to complete to deliver a refund, whether through digital marketing or manual intervention, incurs substantial costs in both money, time and other resources.

Digital ID services, however, offer the opportunity to automate processes, cutting down on the need for expensive human intervention.

**<subhead> Compliance hurdles**

KYC (Know Your Customer) and AML (Anti-Money Laundering) protocols are vital compliance requirements for banks and other financial institutions as they fight financial crime. The pressures are significant: final liability for customer due diligence lies with the financial services provider.

In providing secure, accurate and reliable ways to verify their customers’ identities that can reinforce the integrity of the financial system, digital ID services can streamline these processes at the same time as reducing their cost.

Not only that, but in delivering these services that are transferable to other contexts and use cases, financial institutions can open a path toward unlocking potential value from processes that were once a part of routine regulatory compliance.

**<subhead> How bank-assured digital ID can help overcome these challenges**

Given they already hold a wide range of their customers’ sensitive personal information and financial data, it makes sense to centre a digital ID verification platform around bank data.

Doing so delivers the highest possible level of privacy protection. No new information in the shape of forms, documents or photos needs to be uploaded, meaning data remains ring-fenced within the bank’s ecosystem and the number of insertion points for malicious actors is dramatically reduced. Compliance, AML and KYC are, of course, already taken care of

Reducing the need to upload information also streamlines the customer experience and can serve to replace a process that can require dozens of clicks or the downloading of separate apps into a smooth, frictionless journey that requires as few as three clicks.

**<CTA> If you’d like to learn more about how OneID can help your organisation fully benefit from the digital payments opportunity, click here.**

1. https://www.statista.com/outlook/dmo/fintech/digital-payments/united-kingdom [↑](#footnote-ref-1)
2. https://www.cifas.org.uk/insight/reports-trends/fraudscape-2021 [↑](#footnote-ref-2)
3. https://www.onespan.com/resources/cornerstone-digital-identity-verification-report [↑](#footnote-ref-3)
4. https://www.experian.co.uk/blogs/latest-thinking/data-insights-and-analytics/global-insights-report-april-2022/ [↑](#footnote-ref-4)
5. https://venturebeat.com/ai/report-76-of-consumers-would-stop-doing-business-with-a-company-after-just-one-bad-customer-experience/ [↑](#footnote-ref-5)